Power Systems

# *Установка и настройка консоли аппаратного обеспечения*

**Примечание**

Перед тем, как приступить к работе с этой информацией и описанным в ней продуктом, обязательно ознакомьтесь со сведениями, приведенными в документе “Примечания, касающиеся безопасности” на стр. v, “Замечания” на стр. 101 и в руководстве *IBM Systems - Информация по технике безопасности*, G229-9054, и *Руководстве пользователя и замечаниям по эксплуатации IBM*, Z125–5823.

Данное издание применимо к консоли аппаратного обеспечения IBM® Hardware Management Console версии 9 выпуска 2 уровня обслуживания 950 и ко всем последующим выпускам и модификациям данного продукта, если в новых изданиях не будет указано иное.

# Содержание

# Примечания, касающиеся безопасности

В настоящем руководстве используются следующие замечания по технике безопасности:

- **ОПАСНО** - это замечание касается ситуаций, создающих угрозу жизни или здоровью человека.
- **ОСТОРОЖНО** - это замечание касается потенциально опасных аварийных ситуаций.
- **Внимание** - это замечание касается ситуаций, создающих угрозу повреждения программы, устройства, системы или данных.

## Информация о безопасности международной торговли

В некоторых странах действует требование, согласно которому информация по технике безопасности, приводимая в документации к продукту, должна быть доступна на государственном языке данной страны. Если это требование применимо для вашей страны, пакет документов, поставляемый вместе с продуктом (например печатная документация, документация на диске DVD или в составе продукта), будет содержать документацию по технике безопасности. Эта документация содержит информацию о безопасности на государственном языке вашей страны со ссылками на источник на английском языке (США). Перед началом установки, использования или обслуживания данного продукта следует ознакомиться с информацией по технике безопасности, приведенной в этой документации. В случае возникновения каких-либо сомнений в отношении информации по технике безопасности, приведенной в английской документации, вы также можете обратиться к этой документации.

Для замены или получения дополнительных копий документации по технике безопасности обратитесь по телефону горячей линии IBM: 1-800-300-8751.

## Информация о безопасности для Германии

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

## Техника безопасности при работе с лазером

Серверы IBM могут использовать карты ввода-вывода или компоненты на основе оптоволоконных соединений, в которых применяются лазеры или светодиоды.

### Требования к лазерам

Серверы IBM можно устанавливать внутри стойки или за ее пределами.

**ОПАСНО:** При работе с системой или вблизи нее соблюдайте следующие меры предосторожности:

Ток электрических, телефонных и коммуникационных кабелей представляет опасность для человека. Во избежание поражения электрическим током, если в комплект поставки IBM входят кабели питания, для подключения данного блока используйте только кабель из комплекта поставки IBM. Не используйте эти кабели для других продуктов. Не открывайте и не пытайтесь ремонтировать блок питания. Не подключайте и не отключайте кабели и не проводите установку или обслуживание продукта при неполадках в электрической сети.

-  Этот продукт может быть оснащен несколькими кабелями питания. Во избежание поражения электрическим током отключайте все силовые кабели. В случае питания от сети переменного тока отключите все кабели питания от источника питания. Для стоек с панелью распределения питания (PDP) постоянного тока отключите источник питания, предоставляемый заказчиком, от PDP.

- При подключении питания к продукту убедитесь, что все кабели питания подсоединены правильным образом. Для стоек с питанием переменного тока все кабели питания включайте в правильно подсоединенные и заземленные электрические розетки. Убедитесь, что напряжение и чередование фаз розетки отвечает заданным требованиям. Для стоек с панелью распределения питания (PDP) постоянного тока подключите источник питания, предоставляемый заказчиком, к PDP. Проверьте полярность при подключении питания постоянного тока и проводов возврата питания.
- Устройства, которые соединены с этим продуктом, должны быть подключены к правильно установленным розеткам.
- При возможности отключение и подключение сигнальных кабелей следует производить одной рукой.
- Никогда не включайте оборудование при пожаре, наводнении и повреждении здания.
- Не пытайтесь включить систему до тех пор, пока не будут выполнены все требования техники безопасности.
- Во время проверки системы следует помнить об опасности поражения электрическим током. Выполните все проверки целостности, заземления и питания в ходе установки подсистемы, чтобы обеспечить соответствие системы всем требованиям техники безопасности. Нельзя включать питание системы, пока не будут выполнены все требования техники безопасности. Перед открытием крышек устройства, если обратное не указано в инструкциях по установке и настройке: отключите кабели питания переменного тока, выключите прерыватели, расположенные на панели распределения питания (PDP), и отключите все телекоммуникационные системы, сети и модемы.
- Подключение и отключение кабелей при установке, перемещении или снятии крышек продукта или подключенного к нему устройства должно проводиться в соответствии со следующими инструкциями.

  Для выключения: 1) Выключите все устройства (если в инструкциях не указано иное). 2) В случае питания от сети переменного тока отсоедините кабели питания из розеток. 3) Для стоек с панелью распределения питания (PDP) выключите прерыватели, расположенные на PDP, и отключите источник питания постоянного тока, предоставленный заказчиком. 4) Отключите от разъемов сигнальные кабели. 5) Отключите все кабели от устройств.

  Для подключения: 1) Выключите все устройства (если в инструкциях не указано иное). 2) Подключите все кабели к устройствам. 3) Подключите к разъемам сигнальные кабели. 4) В случае питания от сети переменного тока подсоедините кабели питания к розеткам. 5) Для стоек с панелью распределения питания (PDP) постоянного тока включите источник питания, предоставляемый заказчиком, и включите прерыватели, расположенные на PDP. 6) Включите устройства.
-  В системе или рядом с ней могут присутствовать острые края, углы и стыки. Проявляйте осторожность при перемещении оборудования, чтобы избежать порезов, царапин и прочих травм. (D005)

**(R001 - часть 1 из 2)**:

**ОПАСНО:** При работе возле системы ИТ-стоек или с самой системой соблюдайте следующие меры предосторожности:

- Тяжелое оборудование. Неправильное обращение может привести к получению травмы или повреждению оборудования.
- Всегда опускайте выравнивающие опоры стойки.
- Всегда устанавливайте стабилизирующие скобы стойки (если они предоставлены), если только не будет выполняться установка компонента защиты от землетрясений.
- Для обеспечения устойчивости стойки размещайте самые тяжелые устройства в нижней части стойки. Заполнение стойки устройствами всегда следует начинать снизу.

- Устройства для монтирования в стойке нельзя использовать в качестве полок или рабочего пространства. Не размещайте предметы на поверхности смонтированных в стойку устройств. Кроме того, не облокачивайтесь на смонтированные в стойке устройства и не используйте их для опоры (например, работая на лестнице).

- Риск потери устойчивости:
  - Стойка может опрокинутся и нанести тяжелые физические увечья.
  - Перед раскрытием стойки в монтажное положение ознакомьтесь с инструкциями по установке.
  - Не размещайте ничего тяжелого на оборудовании, смонтированном на выдвижных направляющих, в монтажном положении.
  - Не оставляйте оборудование, смонтированное на выдвижных направляющих, в монтажном положении.
- У устройств, монтируемых в стойке, может быть несколько силовых кабелей.
  - Если требуется отключить питание при обслуживании стойки, работающей от сети переменного тока, убедитесь, что отсоединены все кабели питания.
  - Для стоек с панелью распределения питания (PDP) постоянного тока выключите прерыватель цепи питания системных блоков или отключите источник питания, предоставляемый заказчиком, если обслуживание предусматривает отключение питания.
- Все устройства, монтируемые в стойке, должны быть подключены к устройствам питания этой же стойки. Не подключайте устройства из одной стойки к источнику питания из другой стойки.
- При подключении устройства к неправильно установленной электрической розетке на металлические части устройства может быть подан ток опасного напряжения. Потребитель должен убедиться, что розетка установлена и заземлена должным образом. (R001 часть 1 из 2)

**(R001 - часть 2 из 2)**:

**ОСТОРОЖНО:**

- Нельзя устанавливать блок в стойку, температура внутри которой превышает рекомендованную производителем рабочую температуру для монтируемых в стойке устройств.
- Нельзя устанавливать блок в стойку с нарушенной вентиляцией. Убедитесь, что воздух может беспрепятственно охлаждать устанавливаемый блок.
- При подключении оборудования к сети электропитания следует учитывать мощность цепи питания, чтобы перегрузка не привела к повреждению проводки или срабатыванию токовой защиты. Для вычисления требований к мощности цепи питания стойки обратитесь к сведениям о параметрах энергопотребления, указанным на этикетках, прикрепленных к установленному в стойке оборудованию.
- *(Для выдвижных ящиков.)* Не выдвигайте ящики и не монтируйте в стойке устройства, если на стойке не установлены стабилизирующие скобы или если стойка не прикреплена к полу. Выдвигайте блоки по одному. Если одновременно выдвинуть несколько ящиков, то стойка может потерять устойчивость.

- *(Для закрепленных ящиков.)* Этот ящик является закрепленным и не может выдвигаться для обслуживания, если это не указано производителем. Попытка полностью или частично выдвинуть такой ящик может нарушить равновесие стойки или привести к выпадению ящика. (R001 часть 2 из 2)

**ОСТОРОЖНО:** Чем ниже находится центр тяжести стойки, тем она устойчивее. При перемещении заполненной стойки в пределах помещения или здания выполняйте следующие общие указания.

- Удалите устройства из верхней части стойки, чтобы уменьшить ее массу. При возможности оставьте в ней только те компоненты, которые она содержала изначально. Если эти компоненты неизвестны, соблюдайте следующие меры предосторожности:
  - Удалите все устройства, расположенные выше 1422 мм.
  - Убедитесь, что самые тяжелые устройства находятся в нижней части стойки.
  - Убедитесь, что стойка не содержит пустых отсеков, расположенных ниже уровня 32U, если это не разрешено полученной конфигурацией.
- Если стойка прикреплена к другим стойкам, отсоедините ее.
- Если перемещаемая стойка оснащена съемными боковыми опорами, то их необходимо установить перед перемещением стойки.
- Расчистите предполагаемый путь.
- Убедитесь, что предполагаемый путь пригоден для массы стойки. Масса стойки приведена в документации по ней.
- Убедитесь, что размер дверных проемов не меньше 760 x 2083 мм (30 x 82 дюйма).
- Убедитесь, что все устройства, полки, блоки накопителей и кабели закреплены.
- Убедитесь, что выравнивающие опоры находятся в наивысшем положении.
- Убедитесь, что скоба стабилизатора извлечена из стойки.
- Не наклоняйте стойку более чем на десять градусов.
- Переместив стойку, выполните следующие действия:
  - Опустите выравнивающие опоры.
  - Установите скобу стабилизатора в стойку или в компонент для защиты от землетрясений и прикрутите стойку к полу.
  - Если перед перемещением вы извлекали устройства из стойки, установите их снова, начиная с нижней части стойки.
- Если требуется перемещение стойки на большое расстояние, восстановите первоначальное состояние стойки. Поместите стойку в исходный упаковочный материал или аналогичный ему. Опустите выравнивающие опоры, чтобы поставить поддон на ролики и прикрепить стойку к поддону.

(R002)

**(L001)**

**ОПАСНО:** Эта метка указывает на компоненты с опасным напряжением или током. Не открывайте крышки, на которых размещена эта метка. (L001)

**(L002)**

**ОПАСНО:** Устройства для монтирования в стойке нельзя использовать в качестве полок или рабочего пространства. Не размещайте предметы на поверхности смонтированных в стойку устройств. Кроме того, не облокачивайтесь на смонтированные в стойке устройства и не используйте их для опоры (например, работая на лестнице). Риск потери устойчивости:

- Стойка может опрокинутся и нанести тяжелые физические увечья.
- Перед раскрытием стойки в монтажное положение ознакомьтесь с инструкциями по установке.
- Не размещайте ничего тяжелого на оборудовании, смонтированном на выдвижных направляющих, в монтажном положении.
- Не оставляйте оборудование, смонтированное на выдвижных направляющих, в монтажном положении.

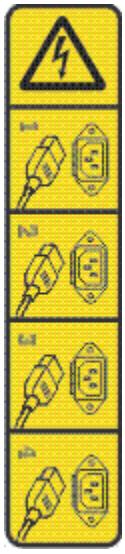
(L002)

**(L003)**

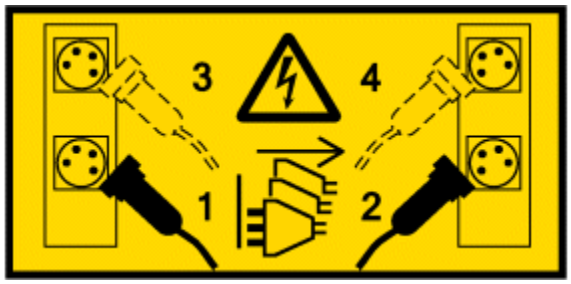

или

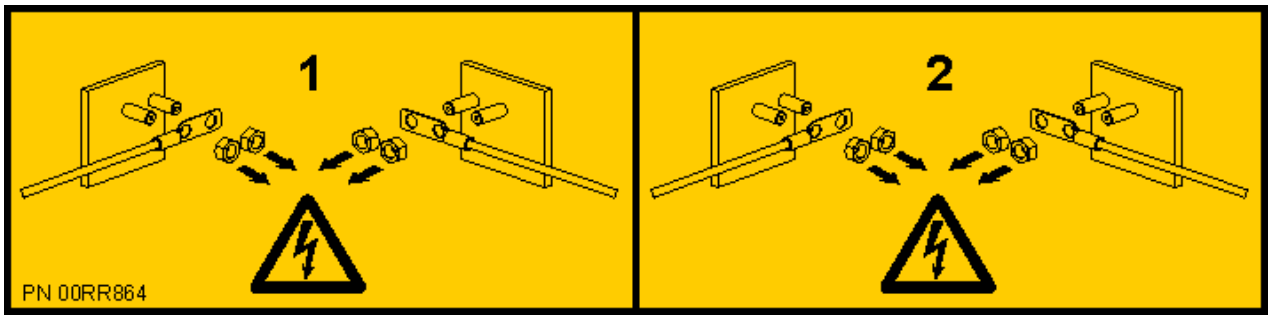

или


или




или




**ОПАСНО:** Несколько кабелей питания. Продукт может быть оснащено несколькими кабелями питания переменного и постоянного тока. Для обеспечения отсутствия опасных напряжений отсоединяйте все кабели питания. (L003)

**(L007)**

**ОСТОРОЖНО:** Горячая поверхность рядом. (L007)

**(L008)**

**ОСТОРОЖНО:** Опасные подвижные детали. (L008)

Все лазеры сертифицированы в США как продукты класса 1 и подчиняются требованиям, перечисленным в Постановлении 21 CFR, Подраздел J, Департамента здравоохранения и медицинских услуг (DHHS). В других странах они сертифицированы как продукты класса 1 и подчиняются требованиям, перечисленным в Стандарте 60825 Международной электротехнической комиссии (IEC). Все компоненты имеют маркировку, содержащую сертификационный номер лазера и контрольную информацию.

**ОСТОРОЖНО:** Продукт может содержать одно или несколько из следующих устройств: дисковод CD-ROM, дисковод DVD-ROM, дисковод DVD-RAM или лазерный модуль. Эти устройства относятся к лазерным продуктам класса 1. Учтите следующее:

- Не снимайте крышки. В результате снятия крышек с лазерных продуктов возникает угроза лазерного излучения. Устройство не содержит компонентов, которые может обслуживать пользователь.
- Использование сторонних приспособлений или нарушение указанных инструкций может привести к опасному радиационному облучению.

(C026)

**ОСТОРОЖНО:** Система обработки данных содержит оборудование, соединенное с лазерными устройствами класса уровня мощности выше 1. Запрещается заглядывать в волоконно-оптический кабель и открывать гнезда. Несмотря на то, что волоконно-оптический кабель можно проверить, подсветив его с одной стороны и заглянув с другой, такая процедура может быть опасной для глаз. Таким образом, такой способ проверки волоконно-оптических кабелей не рекомендуется. Для проверки волоконно-оптического кабеля следует использовать источник света и измеритель мощности. (C027)

**ОСТОРОЖНО:** Продукт содержит лазер класса 1M. Не следует рассматривать его с помощью оптических устройств. (C028)

**ОСТОРОЖНО:** В некоторые лазерные устройства встроен лазерный диод класса 3A или 3B. Учтите следующее:

- При открытии корпуса распространяется лазерное излучение.
- Не допускайте попадания луча в глаз, не рассматривайте луч с помощью оптических устройств и избегайте прямого контакта с лучом. (C030)

(C030)

**ОСТОРОЖНО:** Батареи содержат литий. Во избежание взрыва, батарею запрещается нагревать или перезаряжать.

*Запрещается:*

- Погружать или выбрасывать в воду
- Нагревать до температуры выше 100 C (212 F)
- Ремонтировать или разбирать батарею

Замена батарей допускается только на батареи разрешенного фирмой IBM типа. Уничтожение или переработка батарей должны производиться в соответствии с местными правилами. В США существует сеть отделений фирмы IBM, занимающихся сбором отслуживших свой срок батарей. Дополнительную информацию вы можете узнать по телефону 1-800-426-4333. При этом сообщите номер изделия, указанный на корпусе батареи. (C003)

**ОСТОРОЖНО:** Предупреждение относительно предоставленного IBM подъемника производителя:

- Работа с ПОДЪЕМНИКОМ разрешена только специальному персоналу.
- Подъемный инструмент предназначен для работы с верхними отсеками стоек (подъем, установка и удаление блоков (нагрузки)). Он не должен использоваться под нагрузкой при транспортировке по главным пандусам, а также в качестве замены таким инструментам как подъемные транспортные платформы, вилочные погрузчики и другие средства для подобных операций. Когда это не осуществимо, необходимо использовать специально обученных лиц (например, такелажники или переносчики).
- Перед началом работы необходимо прочитать руководство оператора подъемного инструмента. Если не прочитать, не понять, не соблюдать правила безопасности и не следовать инструкциям, что это может привести повреждению имущества и/или собственной травме. При наличии вопросов обратитесь в службу поддержки производителя. Бумажная копия руководства должна находиться вместе с системой в выделенной для этого области. Последнее издание руководства доступно на веб-сайте производителя.
- Проверяйте функционирование тормоза стабилизатора перед каждым использованием. Не перенагружайте движущийся или вращающийся ПОДЪЕМНИК тормозом стабилизатора.
- Не поднимайте, не опускайте и не перемещайте плоскость загрузки платформы при незадействованном стабилизаторе (педали тормоза). Стабилизатор должен быть зайдействован всегда, когда устройство не перемещается.
- Не перемещайте подъемный инструмент с поднятой платформой за исключением незначительных смещений при позиционировании.
- Не превышайте номинальную грузоподъемность. В Таблице грузоподъемности приведены максимальные нагрузки на центр и на край расширенной платформы.
- Выполняйте подъем только при правильном центрировании на платформе. Не размещайте более 200 фунтов (91 кг) на краю скользящего выступа платформы, учитывая также центр тяжести (CoG) нагрузки.
- Избегайте угловой нагрузки на платформы, наклонную подставку, приспособление для изменения угла наклона и другие подобные элементы. Перед использованием закрепите такие платформы, как наклонная подставка, приспособление изменения угла наклона и т. п. на главной плоскости во всех четырех точках крепления (или другом имеющемся числе точек) только с помощью предоставленных деталей. Грузы должны сдвигаться на ровные платформы и с них без существенного усилия, поэтому не следует давить или наклонять. Держите приспособление для изменения угла наклона платформы (систему регулировки угла наклона) ровно во всех случаях, кроме окончательной незначительной корректировки.
- Не стойте под нависающим грузом.
- Не работайте на неровной поверхности (с наклоном), такой как пандусы.
- Не складывайте грузы друг на друга.

- Не работайте под действием алкоголя или наркотиков.
- Не опирайте лестницу на ПОДЪЕМНИК (за исключением специальных случаев высотных работ после выполнения соответствующих процедур).
- Есть риск опрокидывания. Не давите на грузы и не наклоняйте их при поднятой платформе.
- Не используйте в качестве лифта или ступеньки для себя. Не ездите на нем.
- Не становитесь ни на какую часть подъемника.
- Не лезьте на мачту.
- Не работайте с поврежденным или неисправным ПОДЪЕМНИКОМ.
- Существует риск защемления под платформой. Опускайте груз только в области, свободные от персонала и препятствий. Держите руки и ноги открытыми в процессе выполнения операций.
- Никаких вилочных устройств. Никогда не поднимайте и не перемещайте пустой ПОДЪЕМНИК с помощью тележки с поддонами, домкрата или вилочного погрузчика.
- Мачта возвышается над платформой. Учитывайте высоту потолка, кабельные лотки, противопожарные спринклеры, осветительные приборы и другие объекты наверху.
- Не оставляйте ПОДЪЕМНИК с поднятым грузом без присмотра.
- Наблюдайте и сохраняйте руки, пальцы и одежду открытыми при движении оборудования.
- Поворачивайте ворот только с помощью ручного привода. Если рукоятку ворота не получается легко повернуть одной рукой, значит она перегружена. Не продолжайте поворачивать ворот после перемещения платформы в нижнее или верхнее положение. Чрезмерное раскручивание приведет к отсоединению рукоятки или повреждению кабеля. Всегда придерживайте рукоятку при опускании, раскручивании. Всегда убеждайтесь в том, что ворот удерживает груз, перед тем как отпустить рукоятку.
- Авария ворота может вызвать серьезную травму. Он не предназначен для перемещения людей. При подъеме оборудования должен ясно слышаться звук щелчков. Перед тем как отпустить рукоятку, убедитесь в том, что ворот заблокирован. Перед работой с этим воротом прочитайте инструкции. Никогда не допускайте свободного раскручивания. Свободное вращение вызовет неравномерное наматывание кабеля вокруг барабана ворота, повреждение кабеля и может привести к серьезным травмам.
- Использование ПОДЪЕМНИКА может осуществляться персоналом службы поддержки IBM только в случае его правильного обслуживания. Перед началом работ сотрудники IBM обязаны проверить состояние оборудования и историю его обслуживания. Персонал имеет право отказаться от использования ПОДЪЕМНИКА в случае несоблюдения указанных требований. (C048)

## Информация по электропитанию и кабельному соединению для NEBS (Network Equipment-Building System) GR-1089-CORE

Следующие комментарии относятся к серверам IBM, официально соответствующим требованиям NEBS (Network Equipment-Building System) GR-1089-CORE:

Оборудование пригодно для установки в следующих частях:

- оборудование сетевой телекоммуникации
- места расположения, соответствующие правилам NEC (National Electrical Code)

Предназначенные для работы внутри помещений порты данного оборудования пригодны только для соединения с расположенными в помещениях (или укрытиях) проводами или кабелями. Эти предназначенные для работы внутри помещений порты данного оборудования *не должны* быть подсоединены металлическим способом к интерфейсам, соединенным с внешней установкой OSP или с ее проводами. Эти интерфейсы предназначены для использования только внутри помещений (порты типа 2 и типа 4, согласно описанию в GR-1089-CORE) и должны быть изолированы от открытых кабелей внешней установки OSP. Дополнительная установка основных фильтров не

является достаточной защитой при подключении этих интерфейсов к проводке OSP металлическим способом.

**Прим.:** Все кабели Ethernet должны быть экранированы и заземлены с обоих концов.

Если система работает на переменном токе, использовать внешний фильтр защиты от перенапряжения (SPD) нет необходимости.

Система, работающая на постоянном токе, задействует механизм изолированного обратного провода (DC-I). Возвратная клемма аккумулятора постоянного тока *не должна* соединяться с проводом заземления корпуса или каркаса.

Если система работает на постоянном токе, то ее следует установить в сети с общим заземлением (CBN) (см. GR-1089-CORE).

# Установка и настройка Консоль аппаратного обеспечения

Описание установки аппаратного обеспечения HMC (Консоль аппаратного обеспечения), подключения к управляемой системе и настройки для использования. Рассмотренные задачи можно выполнить самостоятельно или обратиться за помощью в сервисный центр. В последнем случае услуга может оказаться платной.

## Новое в книге Установка и настройка HMC

Описание новой и значительно измененной с момента предыдущей публикации информации по установке и настройке консоли аппаратного обеспечения.

### Апрель 2021 года

- Добавлены следующие разделы:
  - “Установка IBM Power Systems HMC (7063-CR2) в стойку” на стр. 4
  - “Предварительные требования для установки монтируемой в стойке системы 7063-CR2” на стр. 4
  - “Инвентаризация системы” на стр. 5
  - “Определение расположения в стойке и его маркировка для системы 7063-CR2” на стр. 5
  - “Присоединение регулируемых направляющих к шасси системы и стойке” на стр. 6
  - “Присоединение фиксированных направляющих к шасси системы и стойке” на стр. 8
  - “Установка системы в стойку, подключение и прокладка кабелей питания” на стр. 10
  - “Подключение смонтированной в стойке HMC 7063-CR2” на стр. 10
  - “Настройка HMC 7063-CR2” на стр. 12

### Ноябрь 2020 года

- Обновлены следующие разделы:
  - “Задачи установки и настройки” на стр. 2
  - “Обеспечение безопасности HMC” на стр. 89
  - “Расположения портов HMC” на стр. 97

### Июль 2020 года

- Обновлены следующие разделы:
  - “Установка Виртуальное устройство HMC ” на стр. 25
  - “Расположения портов HMC” на стр. 97

### Октябрь 2019 года

- Обновлены следующие разделы:
  - “Установка Виртуальное устройство HMC ” на стр. 25
  - “Обеспечение безопасности HMC” на стр. 89

### Февраль 2019 года

- Добавлены следующие разделы:
  - “Обеспечение безопасности HMC” на стр. 89
  - “Улучшенная стратегия управления паролями” на стр. 91
  - “Решение распространенных проблем с безопасностью HMC” на стр. 94
  - “Профили безопасности: Общеевропейский регламент о защите персональных данных (GDPR) и Стандарт безопасности данных в сфере платежных карт (PCI-DSS) ” на стр. 92

### Август 2018 г.

- Обновлены следующие разделы:
  - “Настройка HMC 7063-CR1” на стр. 21
  - “Расположения портов HMC” на стр. 97

### Декабрь 2017 года

- Добавлена информация для серверов IBM Power Systems с процессором POWER9.

# Задачи установки и настройки

Описание задач, связанных с установкой и настройкой HMC.

Здесь приведено общее описание задач, выполняемых в ходе установки и настройки HMC. HMC можно устанавливать и настраивать разными способами. Выберите задачу, наиболее подходящую конкретной ситуации.

**Заметки:**

- Для управления серверами с процессорами POWER9 требуется HMC версии 9.1.0 или выше. См. раздел “Определение версии и выпуска машинного кода HMC” на стр. 78.
- Консоль аппаратного обеспечения (HMC) версии 9.2.950 и более поздних версий не поддерживается в HMC с типом системы 7042. Дополнительную информацию о версиях HMC, допустимых для HMC 7042, можно найти в информации о выпуске HMC, которая доступна на веб-сайте Fix Central.

## Установка и настройка новой консоли HMC с новым сервером

Общее описание задач, выполняемых в случае установки и настройки новой HMC с новым сервером.

*Таблица 1. Задачи, выполняемые в случае установки и настройки новой HMC с новым сервером*

| **Задача** | **Где искать связанную информацию** |
|---|---|
| 1. Соберите информацию и заполните справочную таблицу по подготовке к установке. | “Форма настройки HMC перед установкой” на стр. 48<br>“Подготовка к настройке HMC” на стр. 47 |
| 2. Извлеките аппаратное обеспечение из упаковки. | |
| 3. Подсоедините к HMC необходимые кабели. | “Подключение смонтированной в стойке HMC 7063-CR1” на стр. 20 |
| 4. Включите HMC, нажав кнопку питания. | |
| 5. Войдите в HMC и запустите веб-приложение. | |

| *Таблица 1. Задачи, выполняемые в случае установки и настройки новой HMC с новым сервером (продолжение)* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 6. Настройте HMC с помощью меню или мастера пошаговой настройки. | “Настройка HMC с помощью быстрого выполнения мастера пошаговой настройки” на стр. 55<br>“Настройка HMC с помощью меню ” на стр. 56 |
| 7. Подключите сервер к HMC. | |

## Обновление или модернизация кода HMC

Общее описание задач, выполняемых в случае обновления или модернизации кода HMC.

В ходе обновления или модернизации кода существующей HMC необходимо выполнить следующие задачи:

| *Таблица 2. Задачи, выполняемые в случае обновления или модернизации кода HMC* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 1. Получите обновление. | “Модернизация программного обеспечения HMC” на стр. 83 |
| 2. Просмотрите текущий уровень машинного кода HMC. | |
| 3. Создайте резервную копию данных профайла управляемой системы. | |
| 4. Создайте резервную копию данных HMC. | |
| 5. Запишите информацию о текущей конфигурации HMC. | |
| 6. Запишите состояние удаленной команды. | |
| 7. Сохраните данные модернизации. | |
| 8. Обновите программное обеспечение HMC. | |
| 9. Проверьте правильность установки модернизации машинного кода HMC | |

## Добавление второй HMC в существующую конфигурацию

Общее описание задач, выполняемых в случае добавления второй HMC в конфигурацию управляемой системы.

В случае добавления второй HMC в существующую конфигурацию необходимо выполнить следующие действия:

| *Таблица 3. Задачи, выполняемые в случае добавления второй HMC в существующую конфигурацию* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 1. Убедитесь, что аппаратное обеспечение HMC поддерживает код HMC версии 7. | |
| 2. Соберите информацию и заполните справочную таблицу по подготовке к установке. | “Форма настройки HMC перед установкой” на стр. 48 |
| 3. Извлеките аппаратное обеспечение из упаковки. | |

| *Таблица 3. Задачи, выполняемые в случае добавления второй HMC в существующую конфигурацию (продолжение)* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 4. Подсоедините к HMC необходимые кабели. | “Подключение смонтированной в стойке HMC 7063-CR1” на стр. 20 |
| 5. Включите HMC, нажав кнопку питания. | |
| 6. Войдите в систему HMC. | |
| 7. Уровни версий HMC должны совпадать. Измените уровень одной HMC, чтобы он соответствовал уровню другой. | “Определение версии и выпуска машинного кода HMC” на стр. 78<br>“Модернизация программного обеспечения HMC” на стр. 83 |
| 8. Настройте HMC с помощью меню или мастера пошаговой настройки. | “Настройка HMC с помощью меню ” на стр. 56 |
| 9. Настройте HMC для обслуживания с помощью мастера Настройка вызова сервисного центра. | “Настройка HMC для соединения со службой поддержки с помощью мастера настройки вызова сервисного центра” на стр. 70 |
| 10. Подключите сервер к HMC. | |

# Установка HMC

Перед настройкой программного обеспечения HMC необходимо установить аппаратное обеспечение HMC. Здесь описывается установка панельной HMC или устанавливаемой в стойку HMC.

## Установка IBM Power Systems HMC (7063-CR2) в стойку

Приведены инструкции по установке IBM Power Systems HMC (7063-CR2) в стойку.

Документация по установке доступна в электронном виде и в формате PDF для вывода на печать. Для просмотра или вывода на печать документации в формате PDF перейдите по ссылке Установка и настройка консоли аппаратного обеспечения.

### Предварительные требования для установки монтируемой в стойке системы 7063-CR2

Рассмотрены предварительные требования для установки системы.

#### Об этой задаче

**ОСТОРОЖНО:** Это тяжелый компонент, но вес его не превышает 18 кг. Соблюдайте осторожность при извлечении и установке этого блока. (C008)

Перед тем как приступить к установке сервера, рекомендуется ознакомиться со следующими документами:

- Последняя версия этого документа доступна на веб-странице Установка 7063-CR2 в стойку (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm).
- Инструкции по планированию установки сервера приведены в разделе Планирование помещения и аппаратного обеспечения.

### Процедура

1. Перед тем как приступить к установке, подготовьте следующие компоненты:
   - Крестовая отвертка 2-го размера
   - Плоская отвертка.
   - Отвертка T25
   - Канцелярский нож
   - Браслет заземления
   - Стойка со свободным отсеком высотой 1U EIA (Electronic Industries Association).

   **Заметки:**

   - Если стойка не установлена, установите ее. Соответствующие инструкции приведены в разделе Стойки и компоненты стоек (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).
   - Характеристики блока питания: 100 - 127 В~, 9 А (x2), 200 - 240 В~, 4,5 А (x2); 50 или 60 Гц.
2. Перейдите к “Инвентаризация системы” на стр. 5.

## Инвентаризация системы

Приведены инструкции по инвентаризации системы.

### Процедура

1. Убедитесь, что получены все заказанные коробки.
2. Распакуйте компоненты сервера.
3. Перед установкой каждого компонента сервера проведите инвентаризацию и убедитесь, что все заказанные детали получены.

   **Прим.:**

   Информация о заказе поставляется вместе с продуктом. Информацию о заказе можно получить от торгового представителя или делового партнера IBM.

   Если часть компонентов не соответствует заказу, отсутствует или повреждена, обратитесь по любому из следующих адресов:

   - Торговый посредник IBM.
   - Автоматизированная информационная линия производителя IBM Rochester: 1-800-300-8751 (только США).
   - Каталог контактной информации (http://www.ibm.com/planetwide). Выберите свое расположение, чтобы просмотреть контактную информацию службы поддержки.
4. Перейдите к “Определение расположения в стойке и его маркировка для системы 7063-CR2” на стр. 5.

## Определение расположения в стойке и его маркировка для системы 7063-CR2

Вам может потребоваться определить расположение для установки системного блока в стойке.

### Процедура

1. Ознакомьтесь с разделом Техника безопасности при работе со стойкой (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Выберите место для размещения системного блока в стойке. В процессе планирования установки системного блока в стойке рекомендуется учитывать следующую информацию:

- Самые большие и тяжелые блоки следует размещать внизу стойки.
- Сначала устанавливайте системные блоки в нижней части стойки.
- Укажите в плане отсеки в единицах EIA (Electronic Industries Alliance).

3. При необходимости снимите заглушки для доступа внутрь стойки в том месте, где планируется установить блок (см. Рисунок 1 на стр. 6).

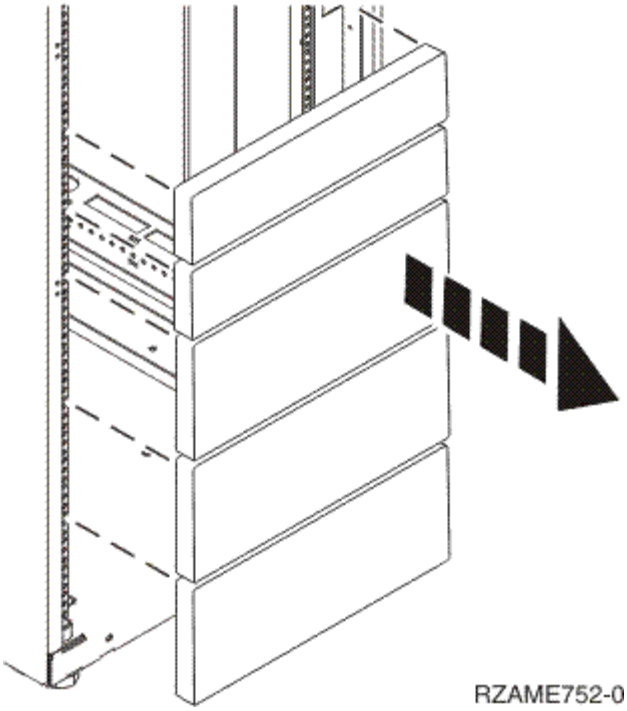



*Рисунок 1. Снятие заглушек*

4. Выберите место для размещения системы в стойке. Запишите расположение EIA.
5. Став лицом к стойке и работая с правой стороны стойки, с помощью скотча, маркера или карандаша отметьте нижнее отверстие каждого модуля EIA.
6. Повторите шаг “5” на стр. 6 для соответствующих отверстий, расположенных с левой стороны стойки.
7. Зайдите в тыл стойки.
8. На правой стороне найдите единицу EIA, соотносящуюся с нижней помеченной единицей EIA спереди стойки.
9. Отметьте нижний модуль EIA.
10. Пометьте соответствующие отверстия на левой стороне стойки.
11. Прикрепите регулируемые направляющие (см. раздел “Присоединение регулируемых направляющих к шасси системы и стойке” на стр. 6) или фиксированные направляющие (см. раздел “Присоединение фиксированных направляющих к шасси системы и стойке” на стр. 8).

## Присоединение регулируемых направляющих к шасси системы и стойке

Направляющие необходимо установить на шасси и в стойку. Используйте эту процедуру для выполнения этой задачи.

### Об этой задаче

**Внимание:** Для того чтобы избежать неправильной установки направляющих, травм и повреждения блока, убедитесь, что для стойки подготовлены подходящие направляющие и крепежные элементы. Направляющие и крепежные элементы должны соответствовать отверстиям в опорных фланцах (квадратные отверстия или отверстия с резьбой). Не

устанавливайте неподходящее оборудование с помощью шайб или вставок. Если комплект направляющих и крепежных элементов отсутствует, обратитесь к реселлеру IBM.

**Прим.:** 1 ячейка EIA в стойках измеряется в единицах высоты по 44,45 мм (1,75 дюйма) каждая. Одна единица EIA соответствует высоте 44,45 мм (1,75 дюйма). В некоторых странах эта единица имеет обозначение "U".

**Прим.:** Для установки системы требуется свободный отсек высотой 1 EIA (1U).

Проверьте наличие необходимых элементов для установки направляющих. В комплект направляющих входят следующие элементы:

- 4 - винты с крестовыми шлицами 6,35 мм (0,25 дюйма)
- 2 - направляющие и опорные скобы
- 2 - опорные скобы HMC
- 10 - гайки с зажимами для квадратных отверстий EIA
- 10 - гайки с зажимами для круглых отверстий EIA
- 10 - винты фланца M5

## Процедура

1. Извлеките все элементы из упаковки и положите их на рабочую поверхность.
2. Найдите в стойке HMC отсек высотой 1U.
3. Для того чтобы прикрепить опорные скобы к HMC, выполните следующие действия:
   a. Найдите правую скобу.
   b. Совместите отверстия на правой скобе со штырями на скобе, расположенными с правой стороны HMC. Убедитесь, что все штыри выровнены с отверстиями в скобе.
   c. До конца задвиньте скобу HMC в заднюю часть HMC.
   d. Прикрепите правую скобу к правой части рабочей станции HMC, установив два винта со шлицем для крестовой отвертки 6,35 мм (0,25 дюйма) в отверстия.
   e. Повторите шаги “3.a” на стр. 7 - “3.d” на стр. 7 для установки левой скобы в левую часть рабочей станции HMC.
4. Перейдите к передней стороне стойки.
   a. С левой левой стороны установите три гайки с зажимами в три отверстия на переднем краю стойки в отсек 1U, предназначенный для HMC.

      **Прим.:** В комплект направляющих входят гайки с зажимами для квадратных и круглых отверстий. Убедитесь, что применяемые гайки с зажимами соответствуют отверстиям в стойке.
   b. Повторите шаг “4.a” на стр. 7 с правой стороны стойки.
5. Перейдите к задней части стойки.
   a. С левой левой стороны установите две гайки с зажимами в два отверстия на переднем краю стойки в отсек 1U, предназначенный для HMC.

      **Прим.:** Среднее отверстие остается пустым.
   b. Повторите шаг “5.a” на стр. 7 с правой стороны стойки.
6. Для установки направляющих HMC в стойку выполните следующие действия:
   a. Измерьте глубину стойки. Глубина должна лежать в диапазоне от 558,8 мм (22 дюйма) до 863,6 мм (34 дюйма).
   b. Поместите направляющие HMC на плоской поверхности и найдите предварительно установленные винты.

      **Прим.:** В направляющих есть четыре отверстия для винтов.

c. Ослабьте предварительно установленные винты на направляющих, чтобы направляющие можно было легко перемещать.

d. С учетом глубины стойки, измеренной на шаге “6.a” на стр. 7, выберите положение винтов на направляющих.

i) Если глубина стойки лежит в диапазоне от 558,8 мм (22 дюйма) до 698,5 мм (27,5 дюйма), установите винты в первое и третье отверстия.

ii) Если глубина стойки лежит в диапазоне от 698,5 мм (27,5 дюйма) до 863,6 мм (34 дюйма), установите винты во второе и четвертое отверстия.

**Примечания:**

- Первое отверстия расположено ближе всего к концу направляющей. Третье и четвертое отверстия расположены рядом друг с другом.
- Убедитесь, что винты достаточно ослаблены, чтобы можно было легко изменять длину направляющей в ходе установки в стойку.

7. Установите направляющие HMC в переднюю часть стойки. Для этого выполните следующие действия:

a. Найдите левую выдвижную направляющую.

b. Разверните направляющую таким образом, чтобы конец с самым ближним отверстием (первое отверстие) первым заходил в стойку. Убедитесь, что головки винтов направлены внутрь стойки. Открытая прорезь в направляющей должна быть расположена ближе к передней части стойки.

c. С левой стороны стойки соедините фланец на конце направляющей с передним краем стойки с помощью двух винтов M5, оставив среднее отверстие пустым. Убедитесь, что направляющая немного ослаблена в передней части стойки, чтобы обеспечить возможность вставки HMC.

8. Справа с задней стороны стойки потяните конец направляющей назад и прикрепите фланец направляющей к стойке с помощью двух винтов M5, оставив среднее отверстие пустым.

9. Повторите шаги “7” на стр. 8 и “8” на стр. 8 для установки правой направляющей с правой стороны стойки.

10. Установите рабочую станцию HMC в переднюю часть стойки. Для этого выполните следующие действия:

a. Удерживая рабочую станцию HMC горизонтально, вставьте опорные скобы в направляющие HMC, установленные на предыдущем шаге. Задвиньте HMC вперед, чтобы совместить фланцы в передней части HMC с пустыми отверстиями для винтов в передней части стойки.

b. Прикрепите HMC с левой стороны стойки с помощью одного винта M5. Повторите этот шаг с правой стороны стойки.

11. Перейдите к “Установка системы в стойку, подключение и прокладка кабелей питания” на стр. 10.

## Присоединение фиксированных направляющих к шасси системы и стойке

Направляющие необходимо установить на шасси и в стойку. Используйте эту процедуру для выполнения этой задачи.

### Об этой задаче

**Внимание:** Для того чтобы избежать неправильной установки направляющих, травм и повреждения блока, убедитесь, что для стойки подготовлены подходящие направляющие и крепежные элементы. Направляющие и крепежные элементы должны соответствовать отверстиям в опорных фланцах (квадратные отверстия или отверстия с резьбой). Не устанавливайте неподходящее оборудование с помощью шайб или вставок. Если комплект направляющих и крепежных элементов отсутствует, обратитесь к реселлеру IBM.

**Прим.:** 1 ячейка EIA в стойках измеряется в единицах высоты по 44,45 мм (1,75 дюйма) каждая. Одна единица EIA соответствует высоте 44,45 мм (1,75 дюйма). В некоторых странах эта единица имеет обозначение "U".

**Прим.:** Для установки системы требуется свободный отсек высотой 1 EIA (1U).

Проверьте наличие необходимых элементов для установки направляющих. В комплект направляющих входят следующие элементы:

- 4 - Винты с крестовыми шлицами 6,35 мм (0,25 дюйма)
- 2 - Внутренние направляющие
- 2 - направляющие HMC
- 2 - Гайки с зажимами для квадратных отверстий EIA
- 2 - Гайки с зажимами для круглых отверстий EIA
- 8 - Винты фланца M5

## Процедура

1. Извлеките все элементы из упаковки и положите их на рабочую поверхность.
2. Найдите в стойке HMC отсек высотой 1U.
3. Для того чтобы прикрепить внутренние направляющие к HMC, выполните следующие действия:
   a. Найдите правую внутреннюю направляющую.
   b. Совместите отверстия на правой внутренней направляющей со штырями, расположенными с правой стороны HMC. Убедитесь, что все штыри выровнены с отверстиями во внутренней направляющей.
   c. До конца задвиньте внутреннюю направляющую HMC в заднюю часть HMC.
   d. Прикрепите правую внутреннюю направляющую к правой части рабочей станции HMC, установив два винта со шлицем для крестовой отвертки 6,35 мм (0,25 дюйма) в отверстия.
   e. Повторите шаги 3.a - “3.d” на стр. 9 для установки левой внутренней направляющей в левую часть рабочей станции HMC.
4. Перейдите к передней стороне стойки. С левой левой стороны установите одну гайку с зажимом в отверстие на переднем краю стойки в отсек 1U, предназначенный для HMC.

   **Прим.:** В комплект направляющих входят гайки с зажимами для квадратных и круглых отверстий. Убедитесь, что применяемые гайки с зажимами соответствуют отверстиям в стойке.
5. Перейдите к задней части стойки. С левой левой стороны установите одну гайку с зажимом в среднее отверстие на переднем краю стойки в отсек 1U, предназначенный для HMC.
6. Установите направляющие HMC в переднюю часть стойки. Для этого выполните следующие действия:
   a. Разместите штыри на направляющих выше и ниже гайки с зажимом, установленной на предыдущем шаге.
   b. С правой стороны стойки соедините фланец на конце направляющей с передним краем стойки, установив два винта M5 в верхнее и нижнее отверстия, оставив среднее отверстие пустым. Убедитесь, что направляющая немного ослаблена в передней части стойки, чтобы обеспечить возможность вставки HMC.
7. Справа с задней стороны стойки потяните конец направляющей назад и прикрепите фланец направляющей к стойке с помощью двух винтов M5, оставив среднее отверстие пустым.
8. Повторите шаги “6” на стр. 9 и “7” на стр. 9 для установки левой направляющей с левой стороны стойки.
9. Установите рабочую станцию HMC в переднюю часть стойки. Для этого выполните следующие действия:

a. Удерживая рабочую станцию HMC горизонтально, вставьте внутренние направляющие в направляющие HMC, установленные на предыдущем шаге. Задвиньте HMC вперед, чтобы совместить фланцы в передней части HMC с пустыми отверстиями для винтов в передней части стойки.

b. Прикрепите HMC с левой стороны стойки с помощью одного винта M5. Повторите этот шаг с правой стороны стойки.

**Прим.:** Удалите оранжевые транспортировочные скобы, установленные в задней части системы, и установите винт на место.

10. Перейдите к “Установка системы в стойку, подключение и прокладка кабелей питания” на стр. 10.

## Установка системы в стойку, подключение и прокладка кабелей питания

Установка системы на направляющие, подключение и прокладка кабелей питания.

### Об этой задаче

**ОСТОРОЖНО:** Это тяжелый компонент, но вес его не превышает 18 кг. Соблюдайте осторожность при извлечении и установке этого блока. (C008)

### Процедура

1. Снимите защитную пластиковую пленку с верхней части шасси системы.
2. Вставьте кабели питания в источники питания.

   **Прим.:** Пока не подключайте другой конец кабеля питания к источнику питания.

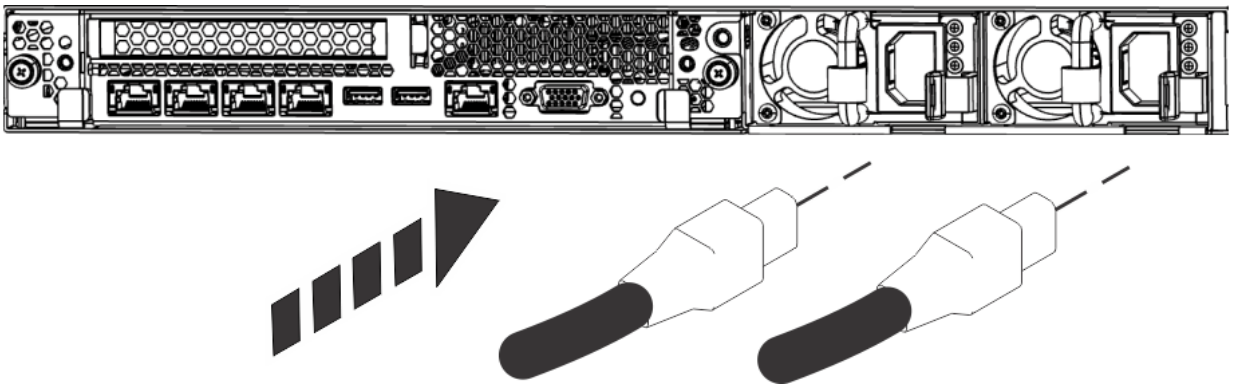


*Рисунок 2. Подключение кабелей питания к источникам питания*

3. Закрепите кабели питания с помощью фиксаторов на липучке.
4. Перейдите к “Подключение смонтированной в стойке HMC 7063-CR2” на стр. 10.

## Подключение смонтированной в стойке HMC 7063-CR2

Приведены инструкции по физической установке консоли аппаратного обеспечения (HMC).

### Процедура

1. Убедитесь в том, что консоль HMC установлена в стойке, а шнуры питания подключены к блокам питания. За дополнительной информацией обратитесь к разделу “Установка системы в стойку, подключение и прокладка кабелей питания” на стр. 10. После установки HMC в стойке перейдите к следующему шагу.
2. Подключите клавиатуру, монитор и мышь.

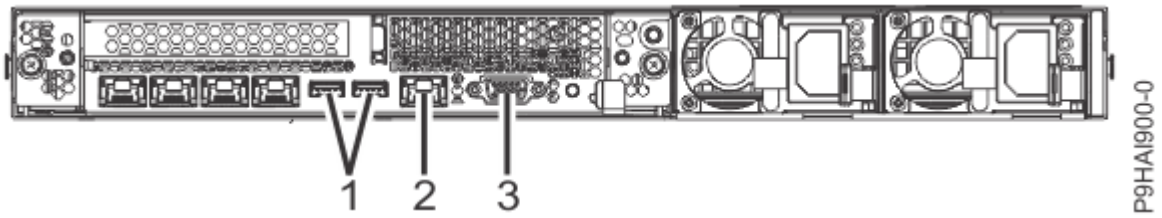



*Рисунок 3. Задние порты*

| *Таблица 4. Входные и выходные порты* | |
|---|---|
| **Идентификатор** | **Описание** |
| 1 | USB 2.0 применяется для подключения клавиатуры и мыши |
| 2 | IPMI (интерфейс интеллектуального управления платформой) Ethernet |
| 3 | Для подключения монитора применяется режим Video Graphics Array (VGA). Поддерживается только режим VGA 1024 x 768 с частотой 60 Гц. Длина кабеля не может превышать 3 метра. |

**Прим.:** На передней стороне системы есть 2 порта USB, которые можно использовать.

3. Подключите порт IPMI (интерфейс интеллектуального управления платформой) к сети.

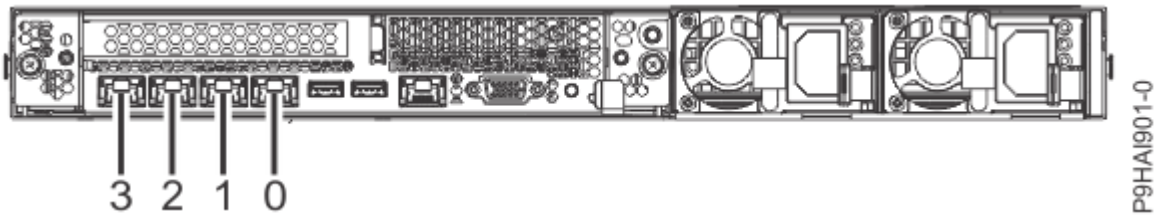



*Рисунок 4. Порты Ethernet*

| *Таблица 5. Порты Ethernet* | |
|---|---|
| **Идентификатор** | **Описание** |
| 0 | Общее сетевое соединение IPMI (интерфейс интеллектуального управления платформой) и HMC |
| 1, 2 и 3 | Сетевое соединение HMC |

**Прим.:** Это соединение необходимо для подключения к контроллеру управления платформой (BMC) в HMC. Доступ к BMC требуется для выполнения задач обслуживания и обновления встроенного программного обеспечения HMC. За дополнительной информацией обратитесь к разделу “Типы сетевых соединений HMC” на стр. 39.

**Предупреждение:** Этот продукт может быть не сертифицирован в вашей стране для подключения любыми средствами к интерфейсам общедоступных телекоммуникационных сетей. Может потребоваться дополнительная сертификация перед установкой такого подключения. Обратитесь в IBM для получения дополнительной информации.

4. Подключите кабель Ethernet, предназначенный для подключения к управляемой системе или системам.

**Заметки:**

- Если применяется общее соединение для IPMI и HMC, один кабель, подключаемый к порту 0 (см. рис. 2), соответствует требованиям IPMI и HMC.
- Дополнительная информация о сетевых соединениях HMC приведена в разделе “Сетевые соединения HMC” на стр. 38.

5. Если управляемая система уже установлена, можно проверить, активно ли кабельное подключение Ethernet: в процессе установки нужно смотреть на зеленые лампочки состояния и на HMC, и на портах Ethernet управляемой системы.
6. Подключите кабели питания системы и других устройств к источнику переменного тока (AC).
7. Проверьте состояние питания по индикаторам блока питания. См. раздел Индикаторы в системе 7063-CR2Индикаторы в системе 7063-CR2.
8. Нажмите кнопку питания, чтобы запустить систему. Индикатор питания перестает мигать и не гаснет; это означает, что питание включено.

### Результаты

Далее следует установить и настроить программное обеспечение HMC. Перейдите к “Настройка HMC 7063-CR2” на стр. 12.

## Настройка HMC 7063-CR2

Приведены инструкции по установке и настройке консоли аппаратного обеспечения (HMC).

Проверьте версию ПО HMC, полученную с консолью HMC. Сведения о просмотре версии системного кода HMC и выпуска приведены в разделе Проверка версии HMC, поставляемой вместе с HMC. Последнюю версию ПО HMC можно загрузить с веб-сайта Fix Central. С помощью съемного носителя (такого как диск DVD или накопитель USB) создайте загрузочный файл ISO на основе пакета HMC (образ ISO).

**Прим.:** Следующая таблица содержит предопределенную (используемую по умолчанию) информацию для входа в интерфейсы HMC и BMC.

*Таблица 6.*

| **Консоль или интерфейс** | **ИД по умолчанию** | **Пароль по умолчанию** | **Описание** |
|---|---|---|---|
| BMC (OpenBMC) | `root` | `0penBmc` | ИД и пароль пользователя root используются для первого входа в BMC. |
| HMC | `hscroot` | `abc123` | ИД пользователя hscroot и его пароль применяются для первого входа в систему. Они вводятся с учетом регистра и могут применяться только в роли главного администратора. |

*Таблица 6. (продолжение)*

| Консоль или интерфейс | ИД по умолчанию | Пароль по умолчанию | Описание |
|---|---|---|---|
| HMC | `root` | `passw0rd` | ИД пользователя root и его пароль применяются сотрудниками сервисного центра для выполнения процедур обслуживания. Эти значения нельзя использовать для входа в систему HMC. |

**Прим.:** Следующие варианты установки приведены в качестве примеров.

## Установка HMC с помощью флэш-накопителя USB

Для того чтобы установить HMC с помощью флэш-накопителя в системе Linux®, выполните следующие действия:

**Прим.:** Примеры для различных операционных систем:

- Windows: Установочный флэш-накопитель USB (Windows)
- Mac: Установочный флэш-накопитель USB (macOS)

1. Загрузите требуемую версию HMC можно на веб-сайте Fix Central.
2. Выполните следующую команду: **`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync`** (где **sdx** - это имя накопителя USB).

   **Прим.:** Имя подключенного накопителя USB можно узнать с помощью следующей команды Linux: `lsblk`.
3. Вставьте накопитель USB и включите систему.

   **Прим.:** Размер накопителя USB должен быть не менее 8 ГБ. Некоторые накопители USB могут быть слишком широкими и не помещаться в порт USB на задней стороне системы. Проверьте габариты накопителя USB, перед тем как продолжать.
4. Когда появится меню Petitboot, выберите пункт **Установить консоль аппаратного обеспечения**, который находится под пунктом **USB**.

## Установка HMC с помощью виртуального носителя из BMC

Для того чтобы установить HMC с помощью виртуального носителя из BMC, выполните следующие действия:

1. Откройте поддерживаемый браузер. В строке адреса укажите IP-адрес BMC, к которому следует подключиться, в формате `https://<IP-адрес-BMC`.
2. В окне **Вход в OpenBMC** заполните поля **Хост**, **Имя пользователя** и **Пароль**.

   **Прим.:** Имя пользователя по умолчанию - `root`, а пароль по умолчанию - `0penBmc`.

   В случае применения встроенного программного обеспечения версии OP940.01 и выше пароль пользователя root по умолчанию считается просроченным. Пароль по умолчанию необходимо изменить, чтобы получить доступ к BMC. Дополнительная информация об изменении пароля по умолчанию приведена в разделе Указание пароля.

   Если вы забыли пароль, вы можете сбросить систему до заводских значений, чтобы восстановить пароль по умолчанию. Инструкции по сбросу системы приведены в разделе Сброс до заводских значений.

3. Выберите **Вход**.
4. Выберите **Управление сервером**.
5. Выберите **Виртуальные носители**.
6. Выберите **Выбрать файл**.
7. Выберите файл ISO носителя восстановления HMC и нажмите кнопку **Открыть**.
8. Выберите **Запустить**.
9. Включите систему.
10. Когда появится меню Petitboot, выберите пункт **Установить консоль аппаратного обеспечения**, который находится под пунктом **USB**.

### Установка HMC с помощью внешнего накопителя DVD, подключаемого через USB

Для установки HMC с помощью внешнего накопителя DVD, подключаемого через USB, выполните следующие действия:

1. Загрузите требуемую версию восстановления HMC с веб-сайта Центр доставки исправлений.
2. Запишите образ DVD восстановления HMC на носитель DVD-R DL в режиме образа.
3. Выключите питание HMC.
4. Подключите внешний накопитель DVD через USB к HMC и вставьте DVD восстановления HMC.

   **Прим.:** Может потребоваться подключить накопитель DVD к внешнему источнику питания или использовать Y-кабель USB для подключения к дополнительному порту USB, чтобы обеспечить достаточную мощность питания для накопителя DVD.
5. Включите питание HMC.

   **Прим.:** Во время запуска на мониторе может показываться сообщение об отсутствии сигнала. Этот процесс занимает 2-3 минуты, и только после этого на монитор будет выведена какая-либо информация.
6. Когда запустится загрузчик Petitboot, отмените автоматическую загрузку.

   **Прим.:** Действует 10-секундный тайм-аут. Если в течение 10 секунд никаких действий не предпринимается, система начинает загрузку с жесткого диска.
7. Подождите, пока в меню Petitboot появится устройство **CD/DVD**.

   **Прим.:** Этот процесс может занять около минуты.
8. Выберите пункт **Установить консоль аппаратного обеспечения**, который находится под пунктом **CD/DVD**.

## Установка 7063-CR1 в стойку

Процедура установки консоли аппаратного обеспечения (HMC) 7063-CR1 в стойку.

Документация по установке доступна в электронном виде и в формате PDF для вывода на печать. Для просмотра или вывода на печать документации в формате PDF перейдите по ссылке Установка и настройка консоли аппаратного обеспечения.

### Предварительные требования для установки монтируемой в стойке системы 7063-CR1

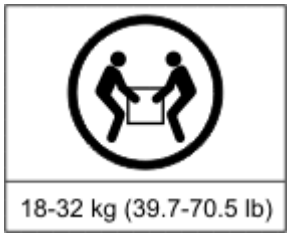
Рассмотрены предварительные требования для установки системы.

## Об этой задаче

**ОСТОРОЖНО:**

или


или




Вес данного компонента или блока составляет от 18 до 32 кг. Поднимать его следует только вдвоем. (C009)

Перед тем как приступить к установке сервера, рекомендуется ознакомиться со следующими документами:

- Последняя версия этого документа доступна на веб-странице Установка 7063-CR1 в стойку (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm).
- Инструкции по планированию установки сервера приведены в разделе Планирование помещения и аппаратного обеспечения.

## Процедура

Перед тем как приступить к установке, подготовьте следующие компоненты:

- Крестовая отвертка 2-го размера
- Плоская отвертка.
- Канцелярский нож
- Браслет заземления
- Стойка со свободным отсеком высотой 1U EIA (Electronic Industries Association).

**Прим.:** Если стойка не установлена, установите ее. Соответствующие инструкции приведены в разделе Стойки и компоненты стоек (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).

# Инвентаризация системы

Приведены инструкции по инвентаризации системы.

## Процедура

1. Убедитесь, что получены все заказанные коробки.
2. Распакуйте компоненты сервера.
3. Перед установкой каждого компонента сервера проведите инвентаризацию и убедитесь, что все заказанные детали получены.

   **Прим.:**

   Информация о заказе поставляется вместе с продуктом. Информацию о заказе можно получить от торгового представителя или делового партнера IBM.

   Если часть компонентов не соответствует заказу, отсутствует или повреждена, обратитесь по любому из следующих адресов:

   - Торговый посредник IBM.
   - Автоматизированная информационная линия производителя IBM Rochester: 1-800-300-8751 (только США).

- Каталог контактной информации (http://www.ibm.com/planetwide). Выберите свое расположение, чтобы просмотреть контактную информацию службы поддержки.

## Определение расположения в стойке и его маркировка для системы 7063-CR1

Вам может потребоваться определить расположение для установки системного блока в стойке.

### Процедура

1. Ознакомьтесь с разделом Техника безопасности при работе со стойкой (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Выберите место для размещения системного блока в стойке. В процессе планирования установки системного блока в стойке рекомендуется учитывать следующую информацию:
   - Самые большие и тяжелые блоки следует размещать внизу стойки.
   - Сначала устанавливайте системные блоки в нижней части стойки.
   - Укажите в плане отсеки в единицах EIA (Electronic Industries Alliance).
3. При необходимости снимите заглушки для доступа внутрь стойки в том месте, где планируется установить блок (см. Рисунок 5 на стр. 16).

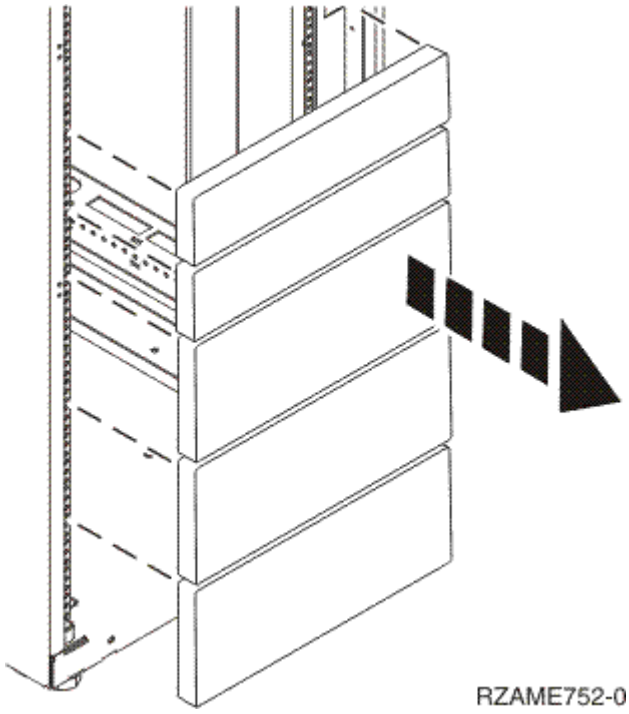



*Рисунок 5. Снятие заглушек*

4. Выберите место для размещения системы в стойке. Запишите расположение EIA.
5. Став лицом к стойке и работая с правой стороны стойки, с помощью скотча, маркера или карандаша отметьте нижнее отверстие каждого модуля EIA.
6. Повторите шаг “5” на стр. 16 для соответствующих отверстий, расположенных с левой стороны стойки.
7. Зайдите в тыл стойки.
8. На правой стороне найдите единицу EIA, соотносящуюся с нижней помеченной единицей EIA спереди стойки.
9. Отметьте нижний модуль EIA.
10. Пометьте соответствующие отверстия на левой стороне стойки.

## Присоединение фиксированных направляющих к шасси системы и стойке

Направляющие необходимо установить на шасси и в стойку. Используйте эту процедуру для выполнения этой задачи.

### Об этой задаче

**Внимание:** Для того чтобы избежать неправильной установки направляющих, травм и повреждения блока, убедитесь, что для стойки подготовлены подходящие направляющие и крепежные элементы. Направляющие и крепежные элементы должны соответствовать отверстиям в опорных фланцах (квадратные отверстия или отверстия с резьбой). Не устанавливайте неподходящее оборудование с помощью шайб или вставок. Если комплект направляющих и крепежных элементов отсутствует, обратитесь к реселлеру IBM.

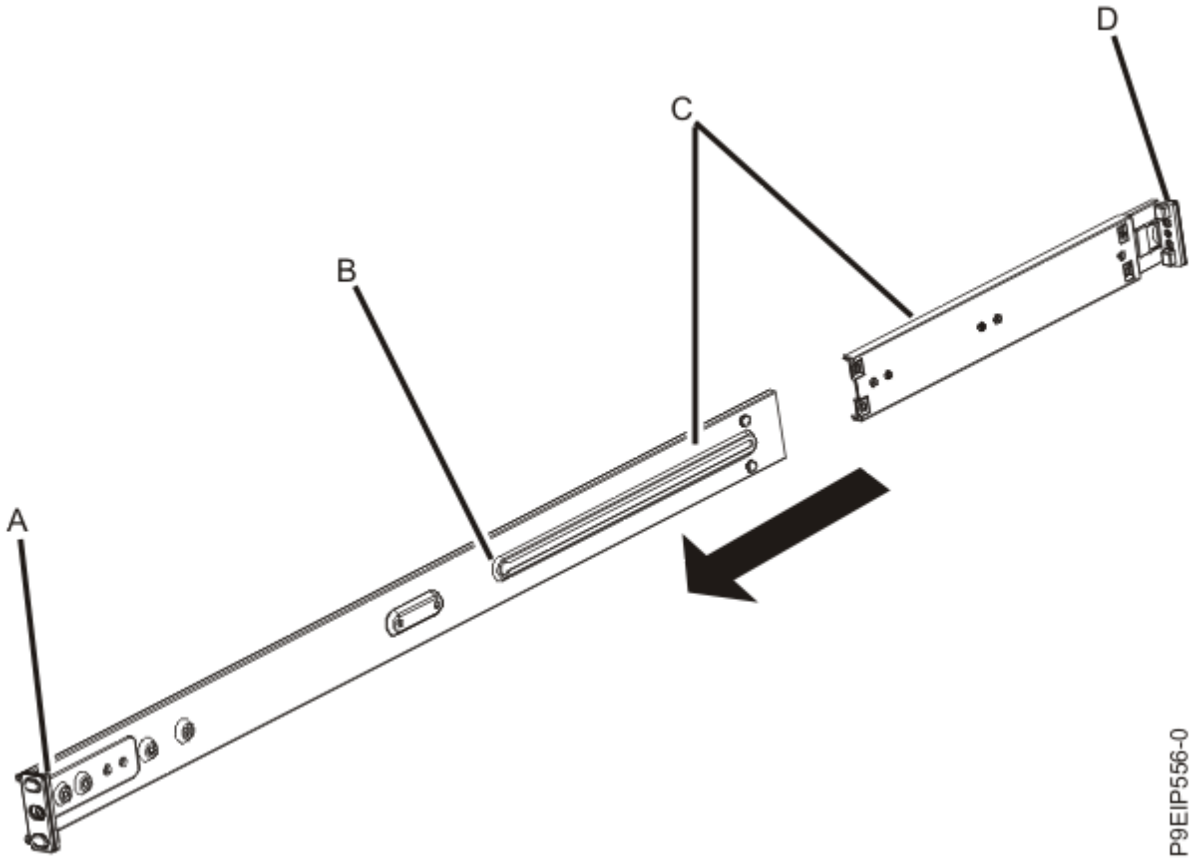
**Прим.:** Для установки системы требуется свободный отсек высотой 1 EIA (1U).

Проверьте наличие необходимых элементов для установки направляющих. В комплект направляющих входят следующие элементы:

- Винты направляющих, применяемые для прикрепления двух компонентов каждой направляющей
- Винты, применяемые для прикрепления направляющих к стойке
- Направляющие
- Винты 10 - 32 x 0,635 см (0,25 дюйма), применяемые для прикрепления направляющих к шасси системы

### Процедура

1. Извлеките все элементы из упаковки и положите их на рабочую поверхность.
2. Поменяйте штифты стоечных направляющих (**A**) и (**D**) квадратного сечения на штифты круглого сечения.
3. Соедините две части каждой направляющей. Для соединения двух частей каждой направляющей выполните следующие задачи:
   a. Определите две части левой направляющей. Выровняйте короткую и длинную части (**C**). Штифты направляющей должны быть направлены в одну сторону (**A**) и (**D**).




b. Короткая часть направляющей имеет металлический штифт. Вставьте штифт в отверстие в длинной части направляющей (**B**). Задвиньте короткую часть направляющей в длинную часть.

c. Совместите отверстия в двух частях направляющей. С помощью крестовой отвертки нетуго вверните винты в отверстия.

**Прим.:** Не затягивайте винты направляющей.

d. Повторите эти шаги для правой направляющей.

4. Установите направляющие в стойку.

a. Перейдите к передней стороне стойки.

b. Выберите левую направляющую и найдите ранее отмеченный блок EIA. На каждой направляющей находится метка **Back**, соответствующая задней части стойки. Убедитесь, что вы держите переднюю часть направляющей.

c. Раздвиньте направляющую из передней в заднюю часть стойки и совместите штифты на направляющей с ранее отмеченными отверстиями на фланце стойки.

d. Вставьте штифты в задний фланец стойки до щелчка.

e. Потяните переднюю часть направляющей в сторону переднего фланца стойки. Совместите штифты на направляющей с отверстиями на фланце стойки, затем вставьте их до щелчка.

f. С помощью отвертки затяните винты, установленные на шаге 2.

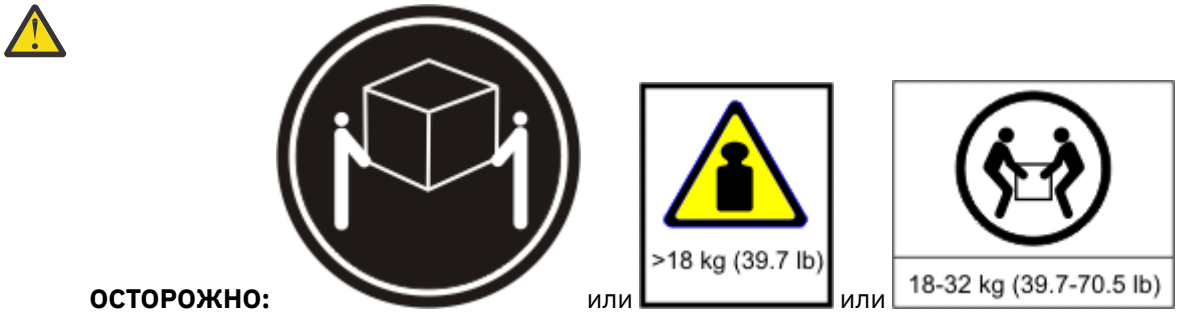
**Прим.:** Для затягивания винтов направляющей может потребоваться пространство высотой 2U.

g. Повторите шаги 4a - 4f для правой направляющей.

## Установка системы в стойку, подключение и прокладка кабелей питания

Установка системы на направляющие, подключение и прокладка кабелей питания.

## Об этой задаче




**ОСТОРОЖНО:** или или

Вес данного компонента или блока составляет от 18 до 32 кг. Поднимать его следует только вдвоем. (C009)

## Процедура

1. Снимите защитную пластиковую пленку с верхней части шасси системы.
2. Перейдите к передней стороне стойки.
3. Вдвоем, каждый со своей стороны, поднимите систему и выровняйте направляющие на шасси системы с направляющими, установленными в стойке.
4. Осторожно задвиньте систему в стойку.
5. Закрепите систему в стойке, ввернув винты через ручки с обеих сторон шасси системы.

   **Прим.:** На винты должны быть надеты шайбы. Наденьте шайбу на каждый из двух длинных винтов (1,5 см (0,59 дюйма)), из комплекта направляющих. Вверните винты с шайбой через левый и правый бока системы с передней стороны.
6. Вставьте кабели питания в источники питания.

   **Прим.:** Пока не подключайте другой конец кабеля питания к источнику питания.

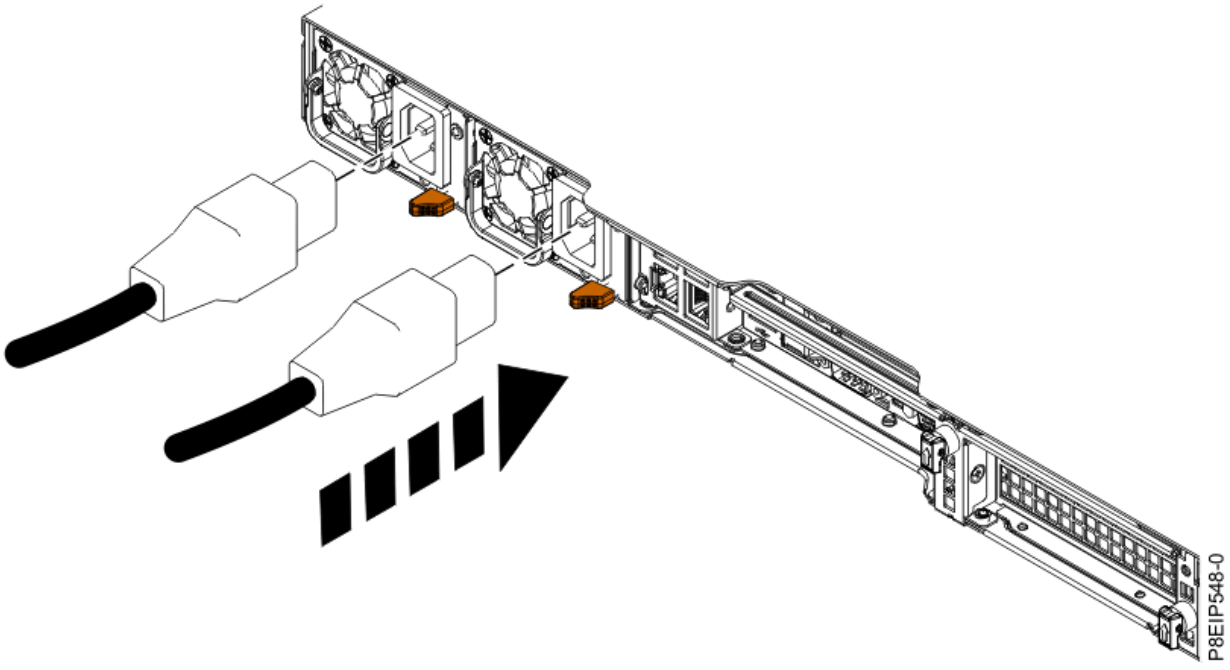



*Рисунок 6. Подключение кабелей питания к источникам питания*

7. Перейдите к “Подключение смонтированной в стойке HMC 7063-CR1” на стр. 20.

## Подключение смонтированной в стойке HMC 7063-CR1

Приведены инструкции по физической установке консоли аппаратного обеспечения (HMC).

### Процедура

1. Убедитесь в том, что консоль HMC установлена в стойке, а шнуры питания подключены к блокам питания. За дополнительной информацией обратитесь к разделу “Установка системы в стойку, подключение и прокладка кабелей питания” на стр. 18. После установки HMC в стойке перейдите к следующему шагу.

   **Прим.:** Если требуемый порт на задней стороне системы закрыт заглушкой, снимите ее и выбросьте. Заглушки нужны для напоминания о необходимости сбросить пароль администратора в управляемой системе после IPL системы.
2. Подключите клавиатуру, монитор и мышь.

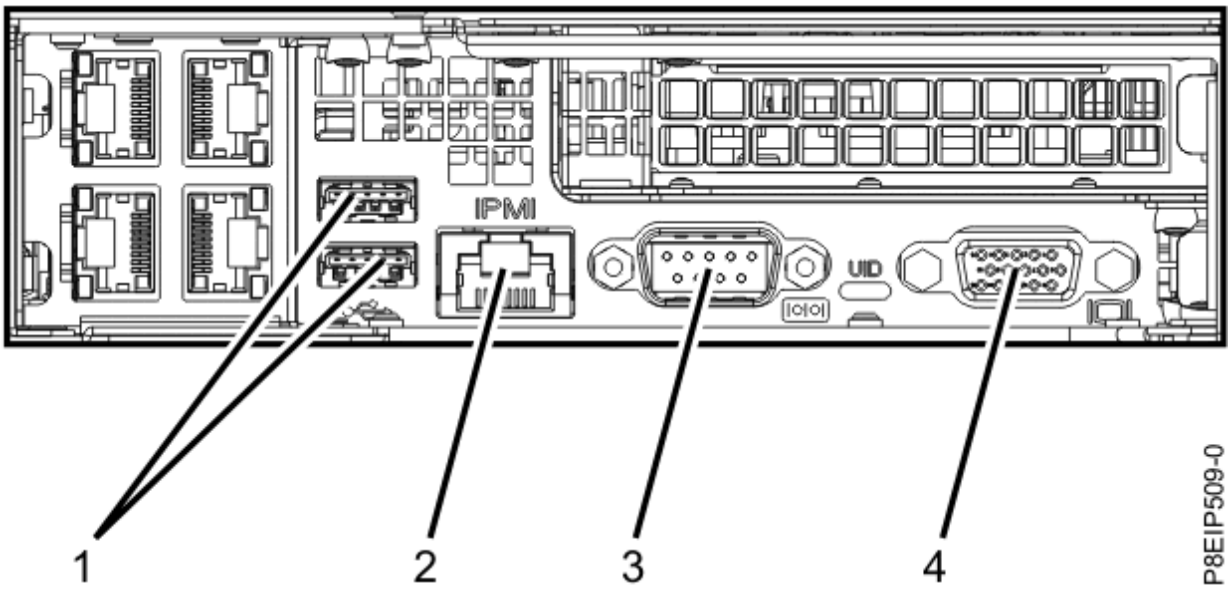



*Рисунок 7. Задние порты*

| *Таблица 7. Входные и выходные порты* | |
|---|---|
| **Идентификатор** | **Описание** |
| 1 | USB 2.0 применяется для подключения клавиатуры и мыши |
| 61 см | IPMI (интерфейс интеллектуального управления платформой) Ethernet |
| 3 | Последовательный IPMI |
| 4 | Для подключения монитора применяется режим Video Graphics Array (VGA). Поддерживается только режим VGA 1024 x 768 с частотой 60 Гц. Длина кабеля не может превышать 3 метра. |

   **Прим.:** На передней стороне системы есть 2 порта USB, которые можно использовать. Последовательный порт на передней стороне не работает.
3. Подключите кабель Ethernet, предназначенный для подключения к управляемой системе или системам.

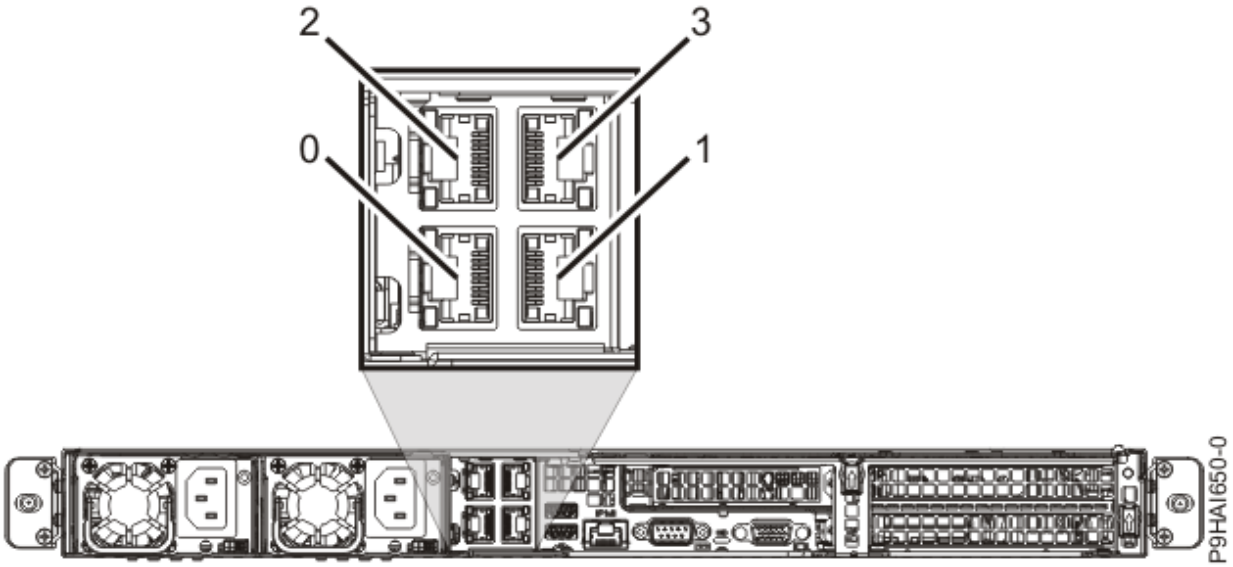



*Рисунок 8. Порты Ethernet*

**Прим.:** Дополнительная информация о сетевых соединениях HMC приведена в разделе “Сетевые соединения HMC” на стр. 38.

4. Если управляемая система уже установлена, можно проверить, активно ли кабельное подключение Ethernet: в процессе установки нужно смотреть на зеленые лампочки состояния и на HMC, и на портах Ethernet управляемой системы.
5. Подключите порт IPMI (интерфейс интеллектуального управления платформой) к сети.

   **Прим.:** Это соединение необходимо для подключения к контроллеру управления платформой (BMC) в HMC. Доступ к BMC требуется для выполнения задач обслуживания и обновления встроенного программного обеспечения HMC. За дополнительной информацией обратитесь к разделу “Типы сетевых соединений HMC” на стр. 39.

6. Подключите кабели питания системы и других устройств к источнику переменного тока (AC).
7. Проверьте состояние питания по индикаторам блока питания. См. раздел Индикаторы в системе 7063-CR1Индикаторы в системе 7063-CR1.

### Результаты

Далее следует установить и настроить программное обеспечение HMC. Перейдите к “Настройка HMC 7063-CR1” на стр. 21.

## Настройка HMC 7063-CR1

Приведены инструкции по установке и настройке консоли аппаратного обеспечения (HMC).

Проверьте версию ПО HMC, полученную с консолью HMC. Последнюю версию ПО HMC можно загрузить с веб-сайта Fix Central. С помощью съемного носителя (такого как диск DVD или накопитель USB) создайте загрузочный файл ISO на основе пакета HMC (образ ISO).

**Прим.:** Следующая таблица содержит предопределенную (используемую по умолчанию) информацию для входа в интерфейсы HMC и BMC.

| *Таблица 8.* | | | |
|---|---|---|---|
| **Консоль или интерфейс** | **ИД по умолчанию** | **Пароль по умолчанию** | **Описание** |
| BMC | `ADMIN` | `ADMIN` | ИД и пароль пользователя ADMIN используются для первого входа в BMC. |
| HMC | `hscroot` | `abc123` | ИД пользователя hscroot и его пароль применяются для первого входа в систему. Они вводятся с учетом регистра и могут применяться только в роли главного администратора. |
| HMC | `root` | `passw0rd` | ИД пользователя root и его пароль применяются сотрудниками сервисного центра для выполнения процедур обслуживания. Эти значения нельзя использовать для входа в систему HMC. |

**Прим.:** Следующие варианты установки приведены в качестве примеров.

## Установка HMC с помощью флэш-накопителя USB

Для того чтобы установить HMC с помощью флэш-накопителя в системе Linux, выполните следующие действия:

**Прим.:** Примеры для различных операционных систем:

- Windows: Установочный флэш-накопитель USB (Windows)
- Mac: Установочный флэш-накопитель USB (macOS)

1. Загрузите требуемую версию HMC можно на веб-сайте Fix Central.
2. Выполните следующую команду: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (где **sdx** - это имя накопителя USB).

   **Прим.:** Имя подключенного накопителя USB можно узнать с помощью следующей команды Linux: `lsblk`.
3. Вставьте накопитель USB и включите систему.

   **Прим.:** Размер накопителя USB должен быть не менее 4 ГБ. Некоторые накопители USB могут быть слишком широкими и не помещаться в порт USB на задней стороне системы. Проверьте габариты накопителя USB, перед тем как продолжать.
4. Когда появится меню Petitboot, выберите пункт **Установить консоль аппаратного обеспечения**, который находится под пунктом **USB**.

## Установка HMC с помощью удаленного носителя из программы просмотра консоли

Для того чтобы установить с помощью удаленного носителя из программы просмотра консоли, выполните следующие действия:

1. Войдите в веб-интерфейс BMC (`http://<bmc-ip>`).
2. Выберите **Удаленное управление**.
3. Выберите **Перенаправление консоли**.
4. Выберите **Запустить консоль**.
5. В программе iKVM Viewer Java™ выберите **Виртуальные носители** > **Виртуальная память**.
6. В разделе **Тип логического накопителя** выберите **Файл ISO**.
7. Выберите **Открыть образ** и найдите файл ISO в системе.
8. Нажмите кнопку **Подключить**, чтобы смонтировать файл ISO.
9. Включите систему.
10. Когда появится меню Petitboot, выберите пункт **Установить консоль аппаратного обеспечения**, который находится под пунктом **CD/DVD**.

## Установка HMC с помощью внешнего накопителя DVD, подключаемого через USB

Для установки HMC с помощью внешнего накопителя DVD, подключаемого через USB, выполните следующие действия:

1. Загрузите требуемую версию восстановления HMC с веб-сайта Центр доставки исправлений.
2. Запишите образ DVD восстановления HMC на носитель DVD-R в режиме образа. Можно также заказать готовый DVD восстановления.
3. Выключите питание HMC.
4. Подключите внешний накопитель DVD через USB к HMC и вставьте DVD восстановления HMC.

   **Прим.:** Может потребоваться подключить накопитель DVD к внешнему источнику питания или использовать Y-кабель USB для подключения к дополнительному порту USB, чтобы обеспечить достаточную мощность питания для накопителя DVD.
5. Включите питание HMC.

   **Прим.:** Во время запуска на мониторе может показываться сообщение об отсутствии сигнала. Этот процесс занимает 2-3 минуты, и только после этого на монитор будет выведена какая-либо информация.
6. Когда запустится загрузчик Petitboot, отмените автоматическую загрузку.

   **Прим.:** Действует 10-секундный тайм-аут. Если в течение 10 секунд никаких действий не предпринимается, система начинает загрузку с жесткого диска.
7. Подождите, пока в меню Petitboot появится устройство **CD/DVD**.

   **Прим.:** Этот процесс может занять около минуты.
8. Выберите пункт **Установить консоль аппаратного обеспечения**, который находится под пунктом **CD/DVD**.

## Установка HMC с помощью удаленного носителя, находящегося на файловом сервере SMB

Для установки HMC с помощью удаленного носителя, находящегося на файловом сервере SMB, выполните следующие действия:

1. Скопируйте файл ISO восстановления на общий хост на файловом сервере с поддержкой SMB.

**Прим.:** Server Message Block версии 3 (SMBv3) не поддерживается.

2. Войдите в веб-интерфейс BMC (`http://<bmc-ip>`).
3. Выберите **Виртуальные носители**.
4. Выберите **Образ компакт-диска**.
5. Введите следующую информацию:

   **Общий хост**

   IP-адрес хоста SMB. Если применяется имя хоста, проверьте правильность конфигурации DNS в BMC.

   **Путь к образу**

   Путь SMB к системе. Пример: `/<имя общего диска>/<остальной путь>/<имя образа>.iso`

   **Пользователь (необязательно)**

   Имя пользователя для входа в систему хоста SMB.

   **Пароль (необязательно)**

   Пароль пользователя.

6. Нажмите **Сохранить**.
7. Выберите **Смонтировать**.
8. Теперь в устройстве 1 отображается следующее сообщение: **Смонтирован файл iso.**

   **Прим.:** Если сообщение не показано, снова проверьте информацию и повторите шаги 6 - 8.

9. Включите систему.
10. Когда появится меню Petitboot, выберите пункт **Установить консоль аппаратного обеспечения**, который находится под пунктом **CD/DVD**.

## Необязательно: обновите уровень встроенного ПО HMC с помощью прилагаемого флэш-накопителя (USB-ключа)

**Прим.:** Если к вашей конфигурации прилагается обновление встроенного ПО HMC на флэш-накопителе, то выполните следующие действия, чтобы обновить уровень встроенного ПО консоли.

Для обновления встроенного ПО HMC с помощью прилагаемого USB-ключа выполните следующие действия:

1. Вставьте флэш-накопитель в USB-порт на задней стороне системы.
2. Включите питание системы и войдите в консоль аппаратного обеспечения.
3. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
4. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
5. Следуйте инструкциям в окне Установка исправления HMC.

Далее следует настроить программное обеспечение HMC. Соответствующие инструкции приведены в разделе “Настройка HMC” на стр. 38.

**Понятия, связанные с данным**

Настройка связи BMC
Можно настроить или просмотреть сетевые параметры BMC для консоли управления.

# Установка Виртуальное устройство HMC

Рассмотрена процедура установки Виртуальное устройство консоли аппаратного обеспечения (HMC).

Виртуальное устройство HMC можно установить в существующей виртуализованной инфраструктуре x86 или POWER. Виртуальное устройство HMC поддерживает следующие гипервизоры виртуализации x86:

- Виртуальная машина на основе ядра (KVM)
- Xen
- VMware

Виртуальное устройство HMC поддерживает следующие гипервизоры виртуализации POWER:

- PowerVM

Минимальные требования для запуска Виртуальное устройство HMC:

- 16 ГБ оперативной памяти
- 4 виртуальных процессора
- 2 сетевых интерфейса (максимум 4)
- 1 дисковый накопитель с 500 ГБ свободного места

**Примечания:**

- Виртуальное устройство HMC можно установить в системе на основе процессора с аппаратной поддержкой виртуализации Intel VT-x или AMD-V.
- Диски DVD Виртуальное устройство HMC не являются загрузочными. Необходимо сначала смонтировать носитель, а затем скопировать файл `.tgz`. Способ монтирования диска DVD может зависеть от применяемой операционной системы.
- Синтаксис команд, применяемых в следующих примерах, может зависеть от операционной системы.
- Гипервизор виртуализации PowerVM требует 160 ГБ дискового пространства. Рекомендуется 500 ГБ.
- Для процессора PowerVM требуется как минимум 1 логический процессор и 4 общих виртуальных процессора в режиме совместного использования с ограничениями. Не рекомендуется использовать выделенные процессоры. Процессору PowerVM также требуется 16 ГБ памяти.

**Информация, связанная с данной**

HMC V8 - образы для сетевой установки и инструкции по установке

## Установка Виртуальное устройство HMC в среде x86

Рассмотрена процедура установки Виртуальное устройство консоли аппаратного обеспечения (HMC) в среде x86.

### *Установка Виртуальное устройство HMC с помощью гипервизора KVM*

Рассмотрена установка Виртуальное устройство консоли аппаратного обеспечения (HMC) с помощью гипервизора KVM.

Для установки Виртуальное устройство HMC в KVM выполните следующие действия:

**Прим.:** В следующей процедуре используется интерфейс командной строки и требуются права пользователя root. Синтаксис команды может зависеть от операционной системы.

1. Убедитесь, что пакеты виртуализации установлены в системах с Red Hat Enterprise Linux (RHEL) версии 7.0 и выше.
2. Загрузите файл `<установочный файл vHMC KVM>.tar.gz` в систему хоста.

3. Выполните следующую команду: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Выполните следующую команду: `cd /var/lib/libvirt/images/vHMC`.
5. Для извлечения образов виртуальных дисков выполните следующую команду: `tar -zxvf <установочный файл vHMC KVM>.tgz`

   **Прим.:** В этой команде укажите полный путь к файлу .tar Виртуальное устройство HMC.
6. Файл **domain.xml** входит в состав файла `<установочный файл vHMC KVM>.tar.gz`. Выполните следующие действия:
   a. Откройте файл **domain.xml** в редакторе и проверьте правильность пути к дискам. Этот файл содержит строку **DISK_PATH**.
   b. Укажите `virtio` в качестве значения шины дискового устройства.
   c. Можно указать другое имя VM. Имя по умолчанию в файле **domain.xml**: **vHMC**.
   d. Убедитесь, что в файле **domain.xml** указан MAC-адрес. Этот файл содержит строку **MAC_ADDRESS**.

      **Прим.:** Удалите эту строку, если MAC-адрес следует создавать в автоматическом режиме.
   e. Убедитесь, что мосты соответствуют устройствам Ethernet. В файле **domain.xml** по умолчанию указано одно устройство Ethernet.
   f. Если используется служба активации, поменяйте **AEDISK** на имя образа виртуального диска службы активации. В противном случае удалите элемент disk.
7. Для того чтобы создать VM, выполните следующую команду: `virsh define <домен>.xml`.
8. Для проверки добавления виртуальной HMC в список виртуальных машин выполните следующую команду: `virsh list --all`.
9. Для того чтобы запустить VM, выполните следующую команду: `virsh start vHMC`.
10. Для того чтобы определить номер дисплея Virtual Network Computing (VNC) для консоли выполните следующую команду: `virsh vncdisplay vHMC`.
11. Для того чтобы подключиться к консоли с помощью программы просмотра VNC, выполните следующую команду: `vncviewer HOSTNAME:ID`(где ID - это номер дисплея, например `0`).

    **Прим.:** Если требуется удаленный доступ, то необходимо выключить брандмауэр или открыть в нем порт 5900.

### *Установка Виртуальное устройство HMC с помощью гипервизора Xen*

Рассмотрена установка Виртуальное устройство консоли аппаратного обеспечения (HMC) с помощью гипервизора Xen.

Виртуальное устройство HMC поддерживает Xen версии 4.2 и выше.

Для установки Виртуальное устройство HMC с помощью гипервизора Xen выполните следующие действия:

**Прим.:** В следующей процедуре используется интерфейс командной строки и требуются права пользователя root. Синтаксис команды может зависеть от операционной системы.

1. Убедитесь, что пакеты виртуализации установлены в системах с Red Hat Enterprise Linux (RHEL) версии 6.4 и выше.
2. Загрузите файл `<установочный файл vHMC XEN>.tar.gz` в систему хоста.
3. Выполните следующую команду: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Выполните следующую команду: `cd /var/lib/libvirt/images/vHMC`.
5. Для извлечения образов виртуальных дисков выполните следующую команду: `tar -zxvf <установочный файл vHMC XEN>.tgz`

   **Прим.:** В этой команде укажите полный путь к файлу .tar Виртуальное устройство HMC.
6. Файл **vhmc.cfg** входит в состав файла `<установочный файл vHMC XEN>.tar.gz`. Откройте файл **vhmc.cfg** в текстовом редакторе и измените следующие значения:

a. Измените имя виртуальной HMC (необязательно): откройте файл **vhmc.cfg** в редакторе и проверьте правильность пути к дискам. Этот файл содержит строку **DISK_PATH**.

b. Замените строку **DISK_PATH** на путь к `disk1.img`:

```
disk = [ 'file:DISKPATH,hda,w' ]
```

c. Замените строку **ethernet adapter** и добавьте MAC-адрес (необязательно):

```
vif = [ 'type=virtio, model=e1000, bridge=eth0' ]
```

Необязательный MAC-адрес:

```
vif = [ 'type=virtio, mac=MACADDRESS, model=e1000, bridge=eth0' ]
```

**Прим.:** В ходе перезапуска виртуальной HMC гипервизор Xen автоматически заново создает MAC-адрес. Для устранения неполадки можно добавить дополнительный MAC-адрес.

d. Замените строку **FLOPPYPATH** (если применяется служба активации):

```
device_model_args = [ "-fda", "FLOPPYPATH" ]
```

7. Для того чтобы создать и запустить виртуальную машину, выполните следующую команду: `xl create vHMC.cfg`.
8. Убедитесь, что виртуальная машина добавлена в список существующих виртуальных машин. Для этого выполните следующую команду: `xl list`.
9. Для того чтобы открыть локальную консоль виртуальной машины, выполните следующую команду: `vncviewer localhost 0`.

### *Установка Виртуальное устройство HMC с помощью VMware ESXi*

Рассмотрена установка Виртуальное устройство консоли аппаратного обеспечения (HMC) с помощью VMware ESXi.

Виртуальное устройство HMC можно установить в VMware ESXi с помощью графического пользовательского интерфейса клиента vSphere путем развертывания шаблона Open Virtualization Format (OVF).

**Прим.:** Виртуальное устройство HMC можно установить в VMware ESXi версии 6.0 и выше.

Для установки Виртуальное устройство HMC в VMware ESXi с помощью клиента vSphere выполните следующие действия:

**Прим.:** Синтаксис команды может зависеть от операционной системы.

1. Получите файл архива Tar: `<имя установочного файла vHMC VMware>.tgz`.
2. С помощью команды `tar` извлеките файл OVA из архива Tar.
3. Запустите клиент vSphere и войдите в систему хоста ESXi.
4. В меню **Файл** выберите **Развернуть шаблон OVF**.
5. Нажмите кнопку **Обзор** и выберите файл OVA.
6. Нажмите кнопку **Далее**.
7. После завершения развертывания нажмите кнопку **Закрыть** и щелкните на значке Виртуальное устройство HMC, чтобы включить Виртуальное устройство HMC.

## Установка Виртуальное устройство HMC в среду POWER

Процедура установки Виртуальное устройство консоли аппаратного обеспечения (HMC) в виртуализированную среду POWER.

### *Установка Виртуальное устройство HMC в PowerVM (логический раздел)*

Процедура установки Виртуальное устройство консоли аппаратного обеспечения (HMC) в среде PowerVM.

Виртуальное устройство HMC поддерживает серверы POWER9 с уровнем встроенного ПО не ниже FW910. См. документ Поддерживаемые варианты Linux для POWER8 и POWER9 Linux в системах Power (https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm).

**Примечания:**

1. Сервером с Виртуальное устройство HMC нельзя управлять.
2. В качестве управляемого нельзя добавить сервер с другой Виртуальное устройство HMC, которая управляет сервером с данной Виртуальное устройство HMC.

   Например, Виртуальное устройство HMC A работает на сервере A, а Виртуальное устройство HMC B работает на сервере B. Ситуация, в которой Виртуальное устройство HMC A управляет сервером B и одновременно с этим Виртуальное устройство HMC B управляет сервером A недопустима. Любая Виртуальное устройство HMC может управлять другим сервером, но обе Виртуальное устройство HMC не могут делать это одновременно.

.

## Создание образа для автоматической установки HMC (необязательно)

Для мастера **Установка HMC** можно создать установочный образ HMC, позволяющий устанавливать Виртуальное устройство HMC автоматически, без участия человека.

**Прим.:** Виртуальное устройство HMC в PowerVM не поддерживает графические адаптеры, присвоенные разделу. В качестве альтернативы можно подключиться к HMC через веб-браузер для доступа к пользовательскому интерфейсу.

Для того чтобы создать образ для автоматической установки HMC, выполните следующие действия:

1. Создайте два каталога следующими командами: `mkdir -p oldiso` и `mkdir -p newiso`.
2. Смонтируйте установочный образ HMC в каталоге **oldiso** следующей командой: `sudo mount -o loop <путь-к-образу> oldiso`.
3. Скопируйте содержимое каталога **oldiso** в каталог **newiso** следующей командой: `cp -r oldiso/* newiso`.
4. Настройте автоматическую установку в файле Grub следующей командой: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Сделайте файл Grub доступным только для чтения следующей командой: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Создайте новый установочный ISO для HMC следующей командой: `mkisofs -o <имя-нового-ISO> -V <метка-ISO> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso` (где **метка-ISO** должна быть `HMC-<номер-версии-HMC>`, например `HMC-8.0.870.0`).

**Прим.:** Дополнительная информация о настройке службы активации и файла конфигурации приведена в разделе “Работа со службой активации для Виртуальное устройство HMC” на стр. 31.

## Настройка логического тома

Для настройки логического тома выполните следующие действия:

1. Выберите управляемую систему.
2. В меню **Действия системы** > **Power VM** > **Виртуальная память**.
3. Выберите **Управление VIOS системы** > **Действие** > **Управление виртуальной памятью**.
4. Откройте вкладку **Виртуальные диски**.
5. Выберите **Создать виртуальный диск** и введите следующую информацию:
   - **Имя виртуального диска** - имя виртуального диска.

- **Имя пула памяти** - имя пула памяти.
- **Размер виртуального диска** - размер виртуального диска.
- **Присвоенный раздел** - имя логического раздела.

**Прим.:** Требуется не менее 160 ГБ дискового пространств (рекомендуется 500 ГБ).

## Настройка установочного носителя - создание библиотеки носителей

Для создания библиотеки носителей выполните следующие действия:

1. Выберите управляемую систему.
2. В меню **Действия системы** > **Power VM** > **Виртуальная память**.
3. Выберите **Управление VIOS системы** > **Действие** > **Управление виртуальной памятью**.
4. Выберите вкладку **Оптические устройства**.
5. Выберите **Создать библиотеку** и введите следующую информацию:
   - **Пул памяти** - имя пула памяти.
   - **Размер библиотеки носителей** - размер библиотеки носителей.
6. Нажмите кнопку **OK**.

## Настройка установочного носителя - передача носителя в VIOS

Для передачи носителя в VIOS выполните следующие действия:

1. Войдите в VIOS.
2. В режиме пользователя root VIOS выполните следующую команду: `oem_setup_env`.
3. Разрешите соединение NFS следующей командой: `nfso -o nfs_use_reserved_ports=1`.
4. Смонтируйте NFS в локальном каталоге VIOS следующей командой: `mount <IP-адрес-сервера>:/Mountpoint <локальный-каталог>`.
5. Убедитесь, что в каталоге точки монтирования NFS есть установочный ISO HMC и образ конфигурации службы активации (необязательно), следующей командой: `ls`.

## Настройка установочного носителя - связывание носителя с библиотекой носителей

Для связывания носителя с библиотекой носителей выполните следующие действия:

1. Вернитесь в **Управление VIOS системы** > **Действие** > **Управление виртуальной памятью** и откройте вкладку **Оптические накопители**.
2. В разделе **Виртуальный оптический носитель** выберите **Добавить носитель** в меню **Действия**.
3. В окне **Добавить виртуальный носитель** выберите **Добавить существующий файл из файловой системы VIOS** и введите следующую информацию:
   - **Имя носителя** - имя носителя, например `HMCInstall` или `AEDrive`.
   - **Имя файла оптического носителя** - имя файла установочного ISO, например `01234567-ppc64ie.iso`.
4. Нажмите кнопку **OK**.
5. Если был создан образ конфигурации службы активации, повторите шаги 3 - 4, чтобы добавить его. В противном случае переходите к шагу 6.
6. Убедитесь, что оптический носитель передан в библиотеку носителей, найдя его имя в списке **Виртуальный оптический носитель**.

## Настройка логического раздела

Для настройки логического раздела выполните следующие действия:

1. Выберите управляемую систему.
2. В меню выберите **Действия системы** > **Разделы** > **Разделы**.
3. Выберите **Создать раздел** и введите следующую информацию:
   - **Имя раздела** - имя раздела.
   - **ИД раздела** - ИД раздела.
   - **Тип раздела** - выберите операционную систему (**AIX/Linux** или **IBM i**).
4. Нажмите кнопку **OK**.
5. Выделите процессоры и память для раздела.

   **Прим.:** Требуется не менее 4 виртуальных процессоров и 8 ГБ памяти.
6. В меню выберите **Операции раздела** > **Виртуальный ввод-вывод** > **Виртуальные сети**.
7. Выберите **Подключить виртуальную сеть** и включите переключатель **Показать и подключить новые виртуальные адаптеры Ethernet**. Выберите в таблице виртуальные сетевые адаптеры, которые требуется подключить к логическому разделу.

   **Прим.:** Поддерживается до 4 виртуальных сетевых адаптеров.
8. В меню выберите **Операции раздела** > **Виртуальный ввод-вывод** > **Виртуальная память**.
9. На вкладке **Виртуальный оптический накопитель** выберите **Добавить виртуальный оптический накопитель**.
10. Введите **Имя устройства**, например `HMCInstall` или `AEDrive`, и выберите требуемый VIOS в таблице.

    **Прим.:** Установка `AEDrive` необязательная.
11. Нажмите кнопку **OK**.
12. Убедитесь, что виртуальные оптические накопители, добавленные на шаге 10, теперь есть в таблице.
13. В меню **Действие** выберите **Загрузить**.
14. Выберите файл накопителя, который требуется присвоить логическому разделу, и нажмите кнопку **OK**.
15. Убедитесь, что виртуальные оптические накопители, загруженные на шаге 13, теперь есть в таблице.

## Запуск Виртуальное устройство HMC

**Прим.:** Если Виртуальное устройство HMC устанавливается в разделе с помощью файла образа ISO HMC, то не будет доступа к пользовательскому веб-интерфейсу из локальной графической консоли.

Для запуска Виртуальное устройство HMC в PowerVM выполните следующие действия:

1. Выберите управляемый раздел.
2. Откройте активное соединение с логическим разделом, выбрав **Действия** > **Консоль** > **Открыть терминал**.
3. Активируйте логический раздел, выбрав **Действия** > **Активировать**.
4. Выберите **Активировать (обычный режим)** и **Текущая конфигурация**.
5. Нажмите кнопку **Закончить**.
6. Переключитесь на окно терминала.
7. В меню **Загрузка** выберите **1 = Меню SMS**.
8. В меню **Главное** выберите **5 = Выбрать опции загрузки**.
9. В меню **Загрузка с выбором операционной системы** выберите **1 = Выбрать устройство установки и загрузки**.

10. В меню **Выбрать тип устройства** выберите **5 = Показать все устройства**.
11. Выберите устройство `HMCInstall` в зависимости от расположения устройства.
12. Выберите **2. Обычный режим загрузки**.
13. Выберите **1. Да** для подтверждения.
14. Следуйте инструкциям мастера **Установка HMC**.

    **Прим.:** Пропустите этот шаг в случае использования образа для автоматической установки HMC.
15. После завершения установки и запуска системы необходимо выбрать язык в окне **Выбор языка**.
16. Примите условия лицензионного соглашения.

    **Прим.:** Перед тем как приступить к выполнению команд, убедитесь, что контроллер команд готов к приему команд. Например, запускайте команду **`lshmc -V`** до тех пор, пока она не будет успешно выполнена.
17. Войдите в систему от имени пользователя `hscroot` и настройте сеть с помощью команды **`chhmc`**.

    В следующем примере показана последовательность команд **`chhmc`**, с помощью которых можно настроить сеть, а также включить ssh и удаленный доступ через веб-интерфейс, в HMC.

    ```
    chhmc -c network -s modify -i ethX -a <IP-адрес-HMC> -nm <маска-подсети-HMC> --lparcomm on
    chhmc -c network -s modify -h <имя хоста hmc> -d <имя домена hmc> -g <IP-адрес шлюза>
    chhmc -c network -s add -ns <сервер имен> -ds <домены для поиска>
    chhmc -c ssh -s enable
    chhmc -c ssh.name -s add -a <IP-адрес>
    chhmc -c SecureRemoteAccess.name -s add -a <IP-адрес>
    chhmc -c remotewebui -s enable -i ethX
    hmcshutdown -r -t now
    ```

    - **ethX** - имя настраиваемого сетевого интерфейса.
    - **IP-адрес hmc** - это IP-адрес HMC.
    - **маска сети hmc** - маска сети HMC.
    - **имя хоста hmc** - имя хоста HMC.
    - **имя домена hmc** - имя домена HMC.
    - **IP-адрес шлюза** - IP-адрес шлюза в сети.
    - **сервер имен** - адрес сервера имен в сети.
    - **домены для поиска** - имена доменов, в которых консоль HMC должна выполнять поиск.
    - Для того чтобы разрешить доступ со всех IP-адресов укажите **-a 0.0.0.0 -nm 0** вместо параметра **IP-адрес**.

    **Прим.:** При использовании нескольких виртуальных адаптеров Ethernet выполните команду **`cat /etc/sysconfig/network-scripts/ifcfg-ethX`** в Виртуальное устройство HMC на каждом интерфейсе. Сравните MAC-адрес с тем, что показывает HMC на панели адаптера для виртуальной сети раздела. Можно выбрать **Показать параметры виртуального адаптера Ethernet** для получения дополнительной информации о виртуальных адаптерах Ethernet. Этот шаг помогает определить правильный интерфейс.
18. Перезапустите систему.

## Работа со службой активации для Виртуальное устройство HMC

Рассмотрено применение службы активации для Виртуальное устройство консоли аппаратного обеспечения (HMC).

Служба активации обеспечивает настройку различных компонентов виртуальной машины в ходе запуска системы. Для применения службы активации необходимо настроить профайл конфигурации XML, обеспечивающий перевод Виртуальное устройство HMC в состояние

готовности к управлению при первом запуске. Дополнительная информация о настройке профайла конфигурации XML приведена в разделе “Настройка профайла конфигурации для службы активации” на стр. 32. В файле конфигурации можно настроить следующие параметры:

- Клавиатура по умолчанию (США)
- Локаль по умолчанию (США)
- Выключить настройку клавиатуры
- Выключить настройку дисплея
- Лицензионное соглашение и соглашение на машинный код
- Выключить мастер настройки
- Выключить мастер вызова сервисного центра
- Настроить до четырех сетевых карт
- Настроить параметры брандмауэра для каждого интерфейса
- Настроить сетевой интерфейс как сервер DHCP для IPv4
- Настроить частный и открытый интерфейсы
- Настроить устройство интерфейса шлюза по умолчанию

**Прим.:** Число адаптеров Ethernet, указанное в файле конфигурации **vHMC-Conf.xml**, должно соответствовать сетевым адаптерам в файле конфигурации **domain.xml**, **vHMC.cfg** или **VMWare**.

Службе активации требуется виртуальный диск с конфигурацией в формате XML. Файл **user_data** можно изменить в текстовом редакторе, используя следующий пример в качестве руководства по настройке.

Для создания образа виртуального диска ISO с конфигурацией службы активации в среде Linux выполните следующие действия:

1. Создайте каталог:

```
mkdir -p config-drive/openstack/latest
```

2. Скопируйте в него измененный файл **user_data**:

```
cp user_data config-drive/openstack/latest
```

3. Создайте образ виртуального диска с конфигурацией службы активации:

```
mkisofs -R -V config-2 -o AEdrive.iso config-drive
```

## *Настройка профайла конфигурации для службы активации*

В этом разделе приведены инструкции по настройке файла конфигурации службы активации с помощью тегов XML.

### Файл конфигурации

Пример файла конфигурации для знакомства с тегами XML.

```
<vHMC-Configuration>
   <ConfigurationVersion>2.0</ConfigurationVersion>
   <LicenseAgreement></LicenseAgreement>
   <AcceptLicense>Yes</AcceptLicense>
   <Locale>en_US.UTF-8</Locale>
   <SetupWizard>No</SetupWizard>
   <SetupCallHomeWizard>No</SetupCallHomeWizard>
   <SetupKeyboard>No</SetupKeyboard>
   <SetupDisplay>No</SetupDisplay>
   <Ethernet Enable='Yes' DefaultGatewayDevice='Yes' PrivateInterface='No'>
      <Hostname></Hostname>
      <Domain></Domain>
      <DNSServers></DNSServers>
      <IPV4Config>
```

```
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Netmask></Netmask>
         <Gateway></Gateway>
      </IPV4Config>
      <IPV6Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Gateway></Gateway>
      <IPV6Config>
      <Firewall>
         <PEGASUS>Enabled</PEGASUS>
         <RPD>Enabled</RPD>
         <FCS>Enabled</FCS>
         <I5250>Enabled</I5250>
         <PING>Enabled</PING>
         <L2TP>Disabled</L2TP>
         <SLP>Enabled</SLP>
         <RSCT>Enabled</RSCT>
         <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
         <SSH>Enabled</SSH>
         <NTP>Disabled</NTP>
         <SNMPTraps>Disabled</SNMPTraps>
         <SNMPAgents>Disabled</SNMPAgents>
      </Firewall>
   </Ethernet>
   <NTPServers>
      <ntpparam ntpserver="" ntpversion=""/>
   </NTPServers>
</vHMC-Configuration>
```

## Теги XML для файла конфигурации

Теги XML применяются в файле конфигурации службы активации для указания значений атрибутов. Эти значения можно вручную указать в файле конфигурации службы активации. В следующей таблице приведено описание каждого тега вместе с допустимыми значениями:

*Таблица 9. Теги XML*

| Теги | Описание | Допустимые значения | Примечания |
|---|---|---|---|
| ConfigurationVersion | Обязательный элемент, описывающий используемую версию конфигурации. | **2.0** | |
| LicenseAgreement | Обязательный элемент для отображения лицензионного соглашения Виртуальное устройство HMC. | | |
| AcceptLicense | Обязательный элемент для принятия лицензионного соглашения Виртуальное устройство HMC. | • **Yes** - принять лицензионное соглашение HMC.<br>• **No** - спросить у пользователя, следует ли принять лицензионное соглашение HMC | При вводе недопустимого значения служба активации использует значение по умолчанию - **No**. |
| Locale | Обязательный элемент, определяющий параметры локали. | **en_US.UTF-8** | При вводе недопустимого значения служба активации использует значение по умолчанию - **US**. |

*Таблица 9. Теги XML (продолжение)*

| Теги | Описание | Допустимые значения | Примечания |
|---|---|---|---|
| SetupWizard | Обязательный элемент для включения/выключения мастера **Настроить HMC**. | • **Yes** - показать мастер **Настроить HMC**.<br>• **No** - не показывать мастер **Настроить HMC**. | При вводе недопустимого значения служба активации использует значение по умолчанию - **Yes**. |
| SetupCallHomeWizard | Обязательный элемент для включения/выключения мастера **Вызов сервисного центра HMC**. | • **Yes** - показать мастер **Вызов сервисного центра HMC**.<br>• **No** - не показывать мастер **Вызов сервисного центра HMC**. | При вводе недопустимого значения служба активации использует значение по умолчанию - **Yes**. |
| SetupKeyboard | Обязательный элемент, определяющий конфигурацию клавиатуры. | • **Yes** - запросить у пользователя конфигурацию клавиатуры.<br>• **No** - принять конфигурацию клавиатуры по умолчанию (US). | При вводе недопустимого значения служба активации использует значение по умолчанию - **Yes**. |
| SetupDisplay | Обязательный элемент для включения/выключения настройки дисплея. | • **Yes** - запросить у пользователя конфигурацию дисплея.<br>• **No** - принять конфигурацию дисплея по умолчанию. | При вводе недопустимого значения служба активации использует значение по умолчанию - **Yes**. |
| Ethernet | Обязательный элемент, содержащий конфигурации адаптеров Ethernet. Можно настроить до 4 адаптеров Ethernet. | **Enable**:<br>• **Yes** - настроить этот адаптер.<br>• **No** - не настраивать этот адаптер.<br>**DefaultGatewayDevice**:<br>• **Yes** - настроить этот адаптер как основной сетевой адаптер.<br>• **No** - не настраивать этот адаптер как основной сетевой адаптер.<br>**PrivateInterface**:<br>• **Yes** - настроить этот адаптер как частный интерфейс. **Yes** - обязательное для настройки интерфейса как сервера DHCP для IPv4.<br>• **No** - не настраивать этот адаптер как частный интерфейс. **No** - обязательное для настройки статического интерфейса IPv4. | Служба активации выполняет настройку по умолчанию, если в разделе адаптеров Ethernet указаны недопустимые значения или если определено несколько **Устройств шлюза по умолчанию**. Необязательные элементы можно не указывать в конфигурации. Требуется хотя бы одна конфигурация IPV4 или IPV6. Если конфигурация IP не указана, служба активации использует конфигурацию по умолчанию. |

*Таблица 9. Теги XML (продолжение)*

| Теги | Описание | Допустимые значения | Примечания |
|---|---|---|---|
| HostName | Необязательный элемент, определяющий имя хоста. | Любое допустимое имя хоста. | Если элемент не указан, служба активации использует значение **HostName** локального хоста по умолчанию. |
| Domain | Необязательный элемент, определяющий домен. | Любое допустимое значение домена, например **example.us.com**. | Если элемент не указан, служба активации использует пустое значение **Domain**. |
| DNSServers | Необязательный элемент, определяющий серверы DNS. | Можно указать от одного до трех адресов IPv4 или IPv6 через запятую.<br>• Пример 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888<br>• Пример 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844<br>• Пример 3: IPv4: 8.3.2.1,8.5.4.1,8.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844, ::ffff:903:201 | Если элемент не определен, служба активации использует пустое значение **DNSServers**. |
| IP4Config | Необязательный элемент, определяющий параметры конфигурации IPv4. | **IPType** - обязательный элемент, определяющий тип конфигурации IPv4.<br>• **Static** - настроить этот адаптер для статической конфигурации.<br>• **DHCP** - настроить этот адаптер для конфигурации DHCP.<br>• **DHCPServer** - настроить этот адаптер как сервер DHCP IPv4 (в **PrivateInterface** должно быть указано значение **Yes**).<br>**IPAddress** - необязательный элемент, требуемый, только если выбрана конфигурация **Static** или **DHCPServer**.<br>• **Конфигурация Static** - любой допустимый адрес IPv4.<br>• **Конфигурация DHCPServer** - любой IP-адрес сервера DHCP в диапазоне IP-адресов.<br>**Netmask** - необязательный элемент, требуемый, только если выбрана конфигурация **Static**.<br>• Любое допустимое значение маски подсети IPv4.<br>**Gateway** - необязательный элемент, требуемый, только если выбрана конфигурация **Static**.<br>• Любое допустимое значение маски подсети IPv4. | |

*Таблица 9. Теги XML (продолжение)*

| Теги | Описание | Допустимые значения | Примечания |
|---|---|---|---|
| IP6Config | Необязательный элемент, определяющий параметры конфигурации IPv6. | **IPType** - обязательный элемент, определяющий тип конфигурации IPv6.<br>• **Static** - настроить этот адаптер для статической конфигурации.<br>• **DHCP** - настроить этот адаптер для конфигурации DHCP.<br>**IPAddress** - допустимы полная и краткая форма адреса IPv6 и полная и краткая форма префикса IPv6.<br>• Пример 1: IPv6: 2001:4860:4860:0000:0000:0000:0000:8888<br>• Пример 2: IPv6: 2001:4860:4860::8888<br>• Пример 3: IPv6: 2001:4860:4860::8888/128<br>Если префикс не указан, служба активации использует префикс по умолчанию /64.<br>**Gateway**:<br>• Любой допустимый адрес IPv6. | |

*Таблица 9. Теги XML (продолжение)*

| Теги | Описание | Допустимые значения | Примечания |
|---|---|---|---|
| Firewall | Необязательный элемент, определяющий параметры брандмауэра. | **PEGASUS**:<br>• **Enabled** - разрешить открытие портов PEGASUS.<br>• **Disabled** - выключить порты PEGASUS.<br>**RPD**:<br>• **Enabled** - разрешить открытие портов RMC.<br>• **Disabled** - выключить порты RMC.<br>**FCS**:<br>• **Enabled** - разрешить открытие портов FCS.<br>• **Disabled** - выключить порты FCS.<br>**I5250**:<br>• **Enabled** - разрешить открытие портов 5250.<br>• **Disabled** - выключить порты 5250.<br>**PING**:<br>• **Enabled** - разрешить открытие порта проверки связи.<br>• **Disabled** - выключить порт проверки связи.<br>**L2TP**:<br>• **Enabled** - разрешить открытие портов L2TP.<br>• **Disabled** - выключить порты L2TP.<br>**SLP**:<br>• **Enabled** - разрешить открытие портов SLP.<br>• **Disabled** - выключить порты SLP.<br>**RSCT**:<br>• **Enabled** - разрешить открытие портов RSCT.<br>• **Disabled** - выключить порты RSCT.<br>**SECUREREMOTEACCESS**:<br>• **Enabled** - разрешить открытие портов защищенного удаленного доступа.<br>• **Disabled** - выключить порты защищенного удаленного доступа.<br>**SSH**:<br>• **Enabled** - разрешить открытие порта SSH.<br>• **Disabled** - выключить порт SSH. | |

| *Таблица 9. Теги XML (продолжение)* | | | |
|---|---|---|---|
| **Теги** | **Описание** | **Допустимые значения** | **Примечания** |
| Firewall | Необязательный элемент, определяющий параметры брандмауэра. | **NTP**:<br>• **Enabled** - разрешить открытие портов NTP.<br>• **Disabled** - выключить порты NTP.<br>**SMNPTraps**:<br>• **Enabled** - разрешить открытие портов прерываний SMNP.<br>• **Disabled** - выключить порты прерываний SMNP.<br>**SMNPAgents**:<br>• **Enabled** - разрешить открытие портов агентов SMNP.<br>• **Disabled** - выключить порты агентов SMNP. | |
| NTPServers | Тег **NTPServers** нужен, если требуется настроить до 5 серверов NTP в Виртуальное устройство HMC. | **NTPServers** - содержит элементы `<ntpparam ntpserver="server" ntpversion="version"/>`<br>**ntpparam**:<br>• **ntpserver** - любой допустимый адрес IPv4 или IPv6 или любое допустимое имя хоста.<br>• **ntpversion** - число 1-4<br>Пример:<br>`<NTPServers>`<br>`  <ntpparam ntpserver= "test.austin.ibm.com" ntpversion="2"/>`<br>`  <ntpparam ntpserver="192.168.34.1"  ntpversion="4"/>`<br>`  <ntpparam ntpserver="::ffff:903:201"  ntpversion="3"/>`<br>`</NTPServers>` | |

# Настройка HMC

Описание настройки сетевых соединений, настройки HMC, действий после настройки и обновления HMC.

## Выбор параметров сети в HMC

Описание сетевых параметров, которые можно использовать в консоли аппаратного обеспечения (HMC).

### Сетевые соединения HMC

Информация по использованию консоли аппаратного обеспечения HMC в сети.

Для соединения HMC с управляемыми системами можно использовать разные типы сетевых соединений. Дополнительная информация о настройке HMC для подключения к сети приведена в разделе “Настройка HMC” на стр. 55. Дополнительная информация по использованию HMC в сети:

### *Типы сетевых соединений HMC*

Знакомит с использованием функций дистанционного управления HMC и служебных функций при помощи сети.

HMC поддерживает следующие типы логических связей:

**Соединение HMC с управляемой системой**
Используется для выполнения большинства функций управления аппаратными средствами; в нем HMC выдает запросы функции управления через служебный процессор управляемой системы. Другое название соединения между HMC и служебным процессором: *сеть обслуживания*. Оно требуется для работы с управляемой системой.

**Соединение HMC с логическим разделом**
Используется для получения информации, связанной с платформой (события при ошибках аппаратных средств, реестр аппаратных средств), от операционных систем, работающих в логических разделах, а также для координации определенных действий платформы (динамический LPAR, оперативный ремонт) с указанными операционными системами. Для работы с функциями обслуживания и извещений об ошибках используется именно этот тип соединения.

**HMC к BMC**

**Прим.:** Соединение с контроллером управления базовой платой (BMC) применимо только к HMC модели 7063-CR1.

Применяется для выполнения задач обслуживания. Соединение BMC используется для настройки и обслуживания встроенного программного обеспечения HMC в системе. Это соединение требуется для доступа к BMC в HMC.

**Соединение HMC с удаленными пользователями**
Обеспечивает удаленный доступ к функциям HMC. Удаленные пользователи могут получить доступ к HMC следующим образом:

- С помощью веб-браузера для удаленного доступа ко всем функциям графического пользовательского интерфейса HMC.
- С помощью протокола SSH для доступа к функциям командной строки HMC.
- Через сервер виртуального терминала - для удаленного доступа к виртуальным консолям логических разделов.

**Соединение HMC со службой сопровождения и поддержки**
Используется для обмена данными, такими как отчеты об ошибках аппаратных средств, реестровые данные и обновления микрокодов, с обслуживающей системой. С его помощью можно также осуществлять автоматические вызовы сервисного центра.

HMC может поддерживать до четырех отдельных физических интерфейсов Ethernet, в зависимости от модели. Автономная версия HMC поддерживает три физических интерфейса HMC, используя один встроенный адаптер Ethernet и один или два встраиваемых адаптера. Каждый из указанных интерфейсов используется следующим образом:

- Один сетевой интерфейс может использоваться только для связи между HMC и управляемой системой; это означает, что в такой сети могут присутствовать только HMC и служебные процессоры управляемых систем. Один или несколько сетевых интерфейсов могут использоваться только для связи между HMC и управляемой системой; это означает, что в такой сети могут присутствовать только HMC и служебные процессоры управляемых систем. Несмотря на то, что сетевые интерфейсы для связи со служебными процессорами зашифрованы по протоколу Secure Sockets Layer (SSL) и защищены паролем, выделенная сеть обеспечивает более высокую степень защиты таких интерфейсов.
- Интерфейс открытой сети используется обычно для сетевых соединений между HMC и логическими разделами управляемых систем, обеспечивая связь между HMC и логическими разделами. Кроме того, интерфейс открытой сети обеспечивает удаленное управление HMC.
- При необходимости можно настроить третий интерфейс для подключения к логическим разделам и удаленного управления HMC. Третий интерфейс можно также использовать для

отдельного соединения HMC с разными группами логических разделов. Например, можно создать отдельный сегмент локальной сети для задач администрирования, не связанный с общей локальной сетью, в которой выполняются деловые задачи. По этой сети администраторы смогут обращаться к HMC и другим управляемым компонентам. Иногда логические разделы размещаются в отдельных защищенных сегментах сети, возможно - за брандмауэром, и иногда требуются отдельные соединения HMC с этими сегментами сети.

## Требования к веб-браузерам для HMC

Консоль аппаратного обеспечения (HMC) версии 9.1.0 поддерживается следующими веб-браузерами: Google Chrome 57, Microsoft Internet Explorer (IE) 11.0, Mozilla Firefox 45 и 52 Extended Support Release (ESR), а также Safari 10.1.

Если браузер настроен для использования прокси-сервера, то в список исключений следует добавить локальные IP-адреса. За дополнительной информацией о списке исключений обратитесь к администратору сети. Если для подключения к HMC требуется использовать прокси-сервер, то включите переключатель Использовать HTTP 1.1 через прокси-соединения на вкладке Дополнительно в окне Свойства обозревателя.

Для работы Расширенного интерфейса управления системой (ASMI) при удаленном подключении к HMC необходимо включить cookie для текущего сеанса. В коде asm proxy сохраняется информация о сеансе, которая используется в дальнейшем. Выполните инструкции по включению cookie сеансов.

Включение cookie сеансов в Internet Explorer.

1. Выберите Сервис, затем выберите Свойства обозревателя.
2. Выберите Конфиденциальность и нажмите кнопку Дополнительно
3. Убедитесь, что переключатель Всегда разрешать сеансовые cookie включен. Если он выключен, то включите переключатели Перекрыть автоматическую обработку файлов cookie и Всегда разрешать сеансовые cookie.
4. Включите переключатель Запрашивать в списках Основные cookie и Сторонние cookie.
5. Нажмите кнопку OK.

Включение cookie сеансов в Firefox.

1. Выберите Инструменты, затем выберите Настройки.
2. Выберите Cookie
3. Включите переключатель Разрешить сайтам задавать cookie.
4. Выберите Исключения и добавьте HMC.
5. Нажмите кнопку OK.

*Частные и открытые сети в среде HMC*
Консоль аппаратного обеспечения (HMC) может быть настроена для использования открытых и частных сетей. Частная сеть позволяет пользоваться избранным диапазоном немаршрутизируемых IP-адресов. *Общедоступная* или "открытая" сеть представляет собой сетевое соединение между HMC и любыми логическими разделами, а также другими системами обычной сети.

## Частные сети

Из устройств в частной сети с HMC имеются только сама HMC и каждая из управляемых систем, к которым она подключена. HMC подключена к FSP (гибкому служебному процессору) каждой управляемой системы.

В большинстве систем FSP имеет два порта Ethernet с метками **HMC1** и **HMC2**. Можно подключить до двух HMC.

В некоторых системах предусмотрена такая возможность, как наличие двух FSP. В этой ситуации второй FSP выступает в роли избыточного резервного сервера. Основные требования установки системы с двумя FSP мало чем отличаются от требований к системе без второго FSP. HMC должна быть подключена к каждому FSP, поэтому при наличии дополнительного FSP или нескольких управляемых систем потребуется дополнительное сетевое оборудование (например, коммутатор или концентратор LAN).

**Прим.:** Каждый порт FSP управляемой системы должен быть подключен только к одной HMC.

## Общедоступные сети

Открытая сеть может быть соединена с брандмауэром или маршрутизатором для подключения к Интернету. Подключение к Интернету позволяет HMC вызывать сервисный центр в случае аппаратных сбоев, требующих уведомления.

HMC предоставляет собственный брандмауэр на каждом из своих сетевых интерфейсов. Основной брандмауэр настраивается автоматически при запуске мастера пошаговой настройки HMC, но по окончании начальной установки и настройки HMC необходимо настроить брандмауэра, задав собственные параметры с учетом своих требований.

*HMC в качестве сервера DHCP*
Консоль аппаратного обеспечения (HMC) можно использовать в качестве сервера DHCP.

Если первый сетевой интерфейс желательно настроить как частную сеть, можно выбирать IP-адреса для сервера DHCP, которые будут присвоены его клиентам. Диапазоны адресов, доступные для выбора, включают фрагменты стандартных диапазонов немаршрутизируемых IP-адресов.

Кроме стандартных диапазонов, для IP-адресов резервируется особый диапазон IP-адресов. Особый диапазон помогает избежать конфликтов в тех случаях, когда в подключенных к HMC открытых сетях используется один из диапазонов немаршрутизируемых адресов. В зависимости от выбранного диапазона, сетевому интерфейсу HMC частной сети автоматически присваивается первый IP-адрес данного диапазона, а служебным процессорам присваиваются оставшиеся IP-адреса диапазона.

Сервер DHCP в HMC использует автоматическое выделение. Это значит, что каждому уникальному интерфейсу Ethernet служебного процессора присваивается один и тот же IP-адрес во время запуска. Каждый интерфейс Ethernet имеет уникальный идентификатор, формируемый на основе встроенного MAC-адреса, который позволяет серверу DHCP каждый раз присваивать одинаковые параметры IP. Порты HMC **eth0** и **eth1** можно настроить для работы с адресами DHCP. Порты HMC **eth0** и **eth1** можно настроить для работы с адресами DHCP.

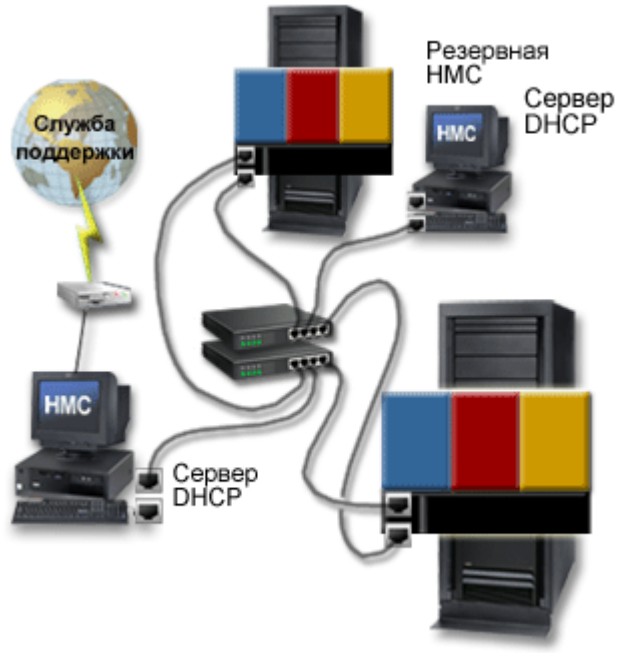
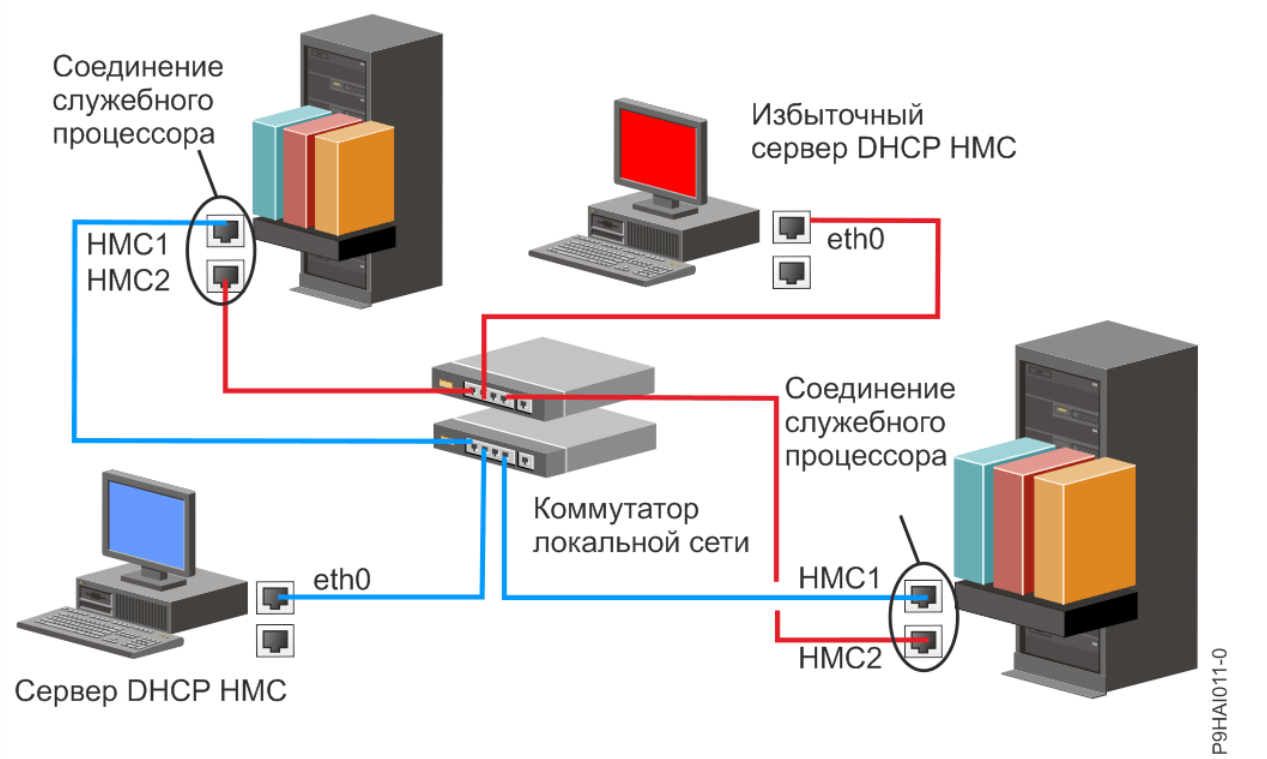



*Рисунок 9. Частная сеть с одной HMC в качестве сервера DHCP*

**Прим.:** При использовании IPv6 поиск необходимо выполнить вручную. Для IPv6 автоматический поиск не поддерживается.

Дополнительная информация о настройке HMC в качестве сервера DHCP приведена в разделе “Настройка HMC в качестве сервера DHCP” на стр. 64.



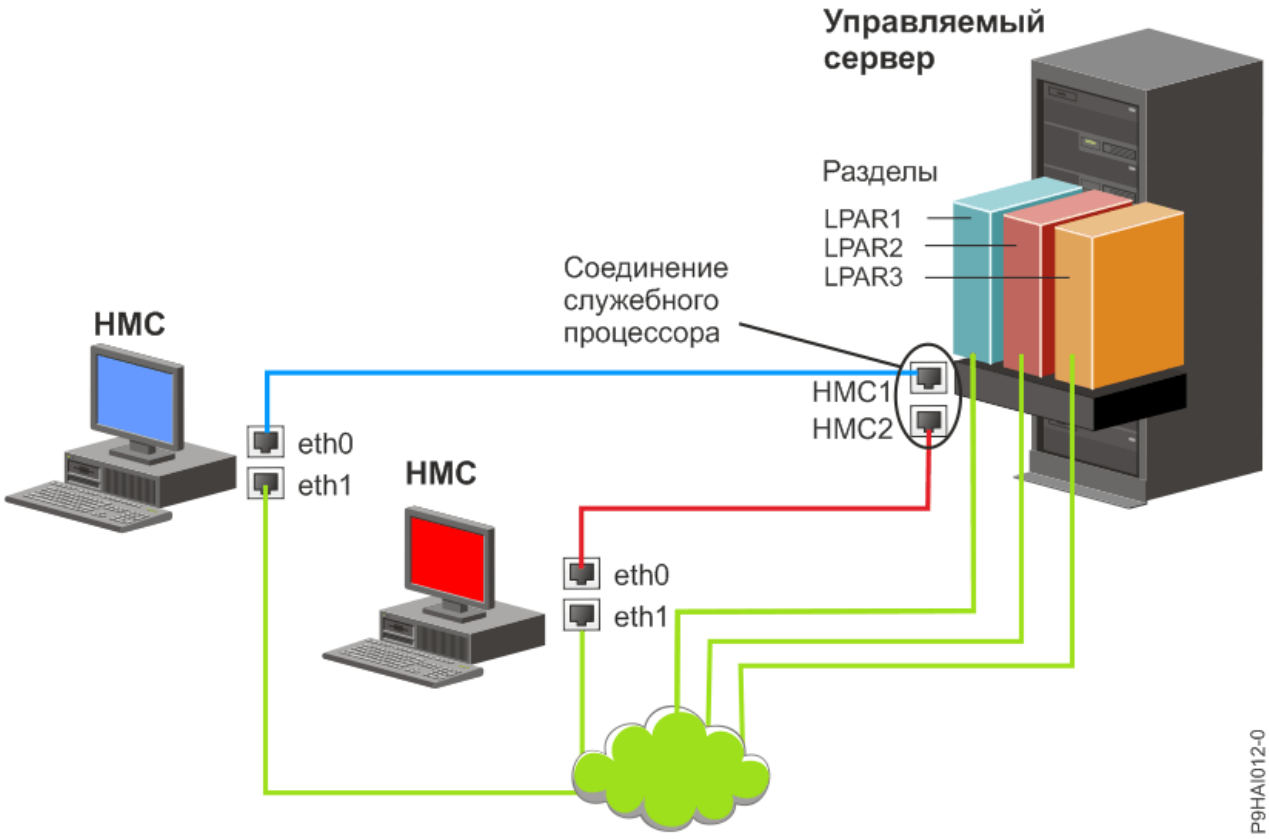

На рисунке показана среда дополнительной HMC с двумя управляемыми системами. Первая HMC подключена к первому порту на каждом FSP, дополнительная HMC - ко второму порту на каждой HMC. Каждая HMC настроена в качестве сервера DHCP с использованием отдельного диапазона IP-

адресов. Соединения выполняются в разных частных сетях. Исходя из этого, важно, чтобы каждый порт был подключен только к одной HMC.

Каждый порт FSP управляемой системы, подключенный к HMC, требует уникального IP-адреса. С этой целью воспользуйтесь встроенной функцией сервера DHCP консоли HMC. После обнаружения процессором FSP активной сетевой ссылки, он выдает оповещающий запрос для нахождения сервера DHCP. Если настройка выполнена правильно, HMC в ответ на этот запрос назначает один из выбранных диапазонов адресов.

При наличии нескольких FSP требуется отдельный коммутатор или концентратор LAN для подключения HMC к частной сети FSP. В альтернативном варианте этот частный сегмент может существовать в виде нескольких портов в частной *виртуальной LAN* (VLAN) на более крупном управляемом переключателе. Если частных сетей VLAN несколько, они должны быть изолированными друг от друга, и между ними не должно быть перекрестных потоков данных.

В среде с несколькими HMC необходимо, кроме того, подключить каждый HMC к логическим разделам и к остальным HMC в одной и той же открытой сети.




На рисунке представлены две консоли HMC, подключенные к одному управляемому серверу в частной сети и к трем логическим разделам в открытой сети. Для того чтобы пользоваться тремя сетевыми интерфейсами, можно добавить дополнительный адаптер Ethernet для HMC. Эту третью сеть можно использовать в качестве сети управления или можно подключить ее к серверу управления CSM (Cluster Systems Manager).

### *Выбор способа соединения для сервера вызова сервисного центра*

Дополнительные сведения об опциях соединения при использовании сервера вызова сервисного центра.

Консоль аппаратного обеспечения (HMC) можно настроить для передачи сервисной информации по аппаратному обеспечению в компанию IBM через интернет-соединение по LAN или коммутируемое соединение по модему.

При настройке интернет-соединения по LAN обмен данными можно организовать двумя способами. В первом варианте используется стандартный протокол защищенных сокетов (SSL). Связь по протоколу SSL можно разрешить для подключения к Интернету через прокси-сервер. SSL-соединение с большей вероятностью будет соответствовать корпоративным рекомендациям по обеспечению защиты.

**Прим.:** Если для открытого сетевого соединения интерфейса используется только IPv6, нельзя использовать VPN через Интернет для соединения со службой поддержки. Дополнительная информация о применяемых протоколах приведена в разделе “Выбор протокола соединения с Интернетом” на стр. 45.

К преимуществам использования интернет-соединения можно отнести:

- Более высокая скорость передачи данных
- Более низкие расходы пользователя (например, затраты на выделенную телефонную линию)
- Более высокая надежность

При любом способе соединения действуют следующие характеристики защиты:

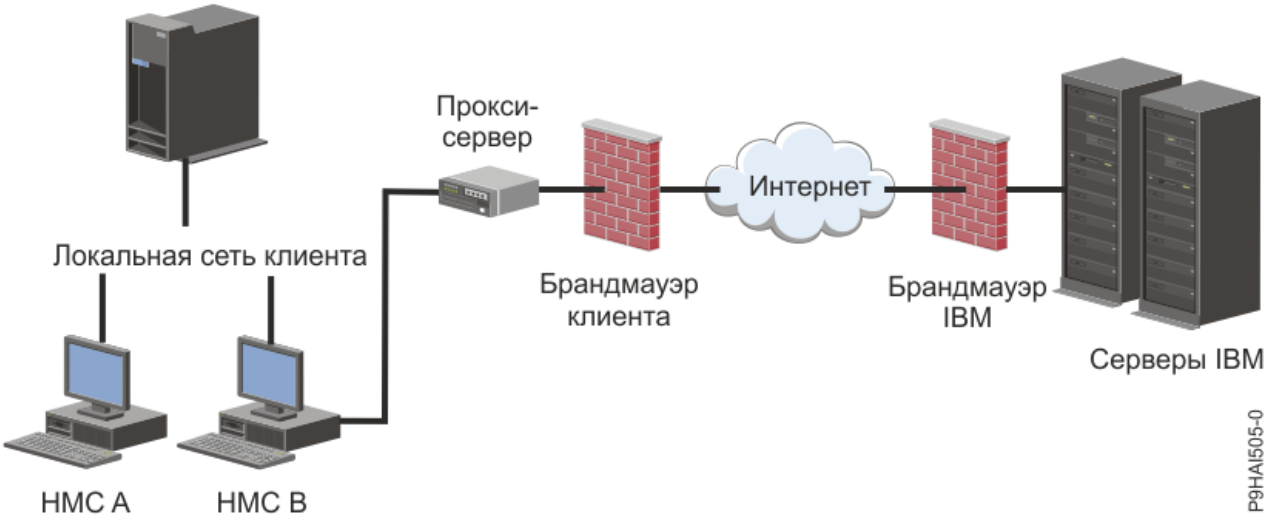
- Запросы Remote Support Facility всегда инициируются с HMC к IBM. Соединение для приема данных никогда не инициируется с системы сервисной поддержки IBM.
- Все данные, передаваемые между HMC и системой сервисной поддержки IBM, шифруются с помощью высококачественного шифрования. В зависимости от выбранного способа соединения, шифрование выполняется с помощью SSL или безопасного закрытия содержания по протоколу IPSec (ESP).
- При инициализации зашифрованного соединения HMC идентифицирует целевую систему как систему сервисной поддержки IBM.

Данные, отправляемые в систему сервисной поддержки IBM, состоят исключительно из сведений о неполадках аппаратных средств и данных конфигурации. Данные о прикладных программах и пользовательские данные в компанию IBM не передаются.

## Использование непрямого интернет-соединения через прокси-сервер

Если по требованиям установки HMC должна находиться в частной сети, то соединение с Интернетом может выполняться через SSL прокси-сервер, используемый для направления запросов в Интернет. Еще одно потенциальное преимущество использования SSL прокси-сервера состоит в том, что прокси-сервер может поддерживать средства регистрации и контроля.

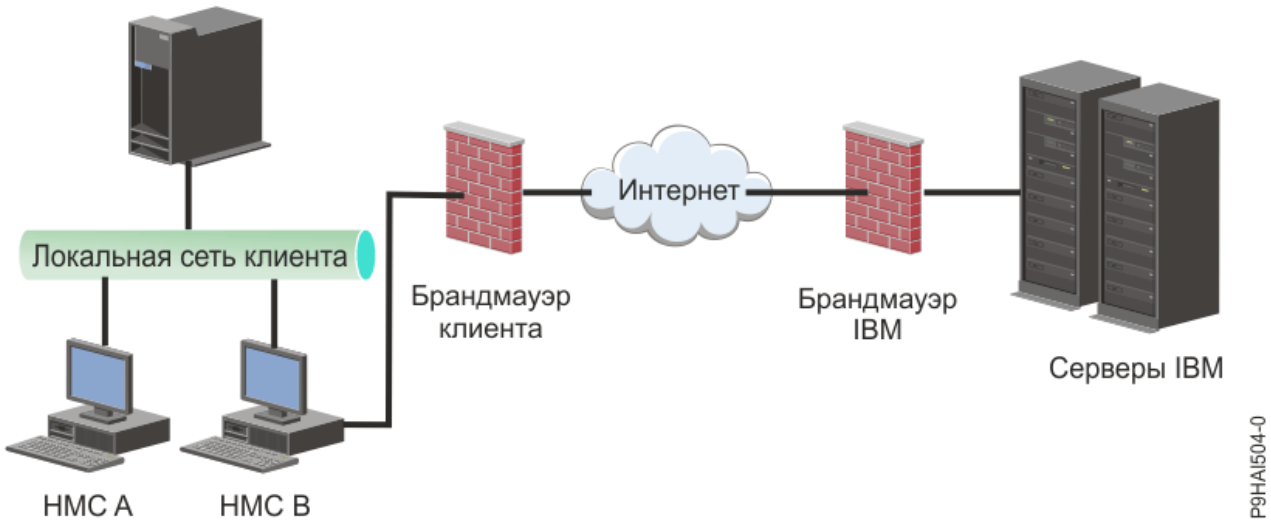
Для пересылки SSL сокетов прокси-сервер должен поддерживать основные функции заголовка прокси-сервера (см. RFC 2616) и метод CONNECT. По желанию можно настроить базовую идентификацию прокси-сервера (RFC 2617), чтобы HMC выполняла идентификацию перед пересылкой данных через прокси-сервер.



Для успешного обмена данными с HMC прокси-сервер клиента должен допускать соединение с портом 443. Можно настроить прокси-сервер таким образом, чтобы ограничить конкретные IP-адреса, с которыми HMC может устанавливать соединение. Список IP-адресов приведен в разделе “Списки адресов SSL для Интернета” на стр. 45.

## Использование прямого SSL-соединения с Интернетом

Если можно устанавливать соединение HMC с Интернетом, и внешний брандмауэр можно настроить для передачи установленных исходящих пакетов TCP получателям, описанным в “Списки адресов SSL для Интернета” на стр. 45, то можно использовать прямое соединение с Интернетом.




### *Использование интернет-соединения SSL для подключения к удаленному сервисному центру*

Вся передача данных обрабатывается через сокеты TCP, открываемые консолью аппаратного обеспечения (HMC). Передаваемые данные надежно шифруются с помощью SSL. Адреса TCP/IP получателей публикуются (см. “Списки адресов SSL для Интернета” на стр. 45), что позволяет настраивать внешние брандмауэры для разрешения таких соединений.

**Прим.:** Для всей передачи данных используется стандартный порт HTTPS 443.

HMC можно включать для соединения с Интернетом напрямую или для непрямого соединения с Интернетом через клиентский прокси-сервер. Выбор подходящего решения зависит от защиты и требований к сетевому взаимодействию конкретной организации. HMC, настроенная для работы с интернет-соединениями SSL, использует (прямо или через прокси-сервер SSL) следующие адреса.

### *Выбор протокола соединения с Интернетом*

Определите версию IP-адреса, использующуюся для подключения консоли аппаратного обеспечения (HMC) к провайдеру.

Большинство пользователей для связи с провайдером используют IPv4. Для доступа к Интернету адреса IPv4 имеют формат, состоящий из 4 байтов адреса IPv4, разделенных точками (например, 9.60.12.123). Также можно использовать IPv6. IPv6 часто используется администраторами сети для обеспечения уникального пространства адресов. Если неизвестно, какой протокол используется в вашей системе, обратитесь к администратору сети. Дополнительная информация об использовании каждой версии приведена в разделах “Установка IPv4-адреса” на стр. 65 и “Установка адреса IPv6” на стр. 65.

### *Списки адресов SSL для Интернета*

Информация об адресах, которые используются консолью аппаратного обеспечения (HMC) для связи по SSL через Интернет.

Для связи с сервисным центром IBM HMC, в которой настроена связь по SSL через Интернет, использует следующие адреса IPv4.

Следующие адреса IPv4 используются для всех регионов:

- 129.42.26.224
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216
- 170.225.15.41

Следующие адреса IPv4 используются для Северной и Южной Америк:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Следующие адреса IPv4 используются для всех регионов, за исключением Северной и Южной Америк:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

**Прим.:** При настройке брандмауэра, который должен разрешать соединение HMC с указанными серверами, требуются только IP-адреса, специфические для географического региона.

Для связи с сервисным центром IBM HMC, в которой настроена связь по SSL через Интернет, использует следующие адреса IPv6:

- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

### *Использование нескольких серверов вызова сервисного центра*

Информация для использования нескольких серверов вызова сервисного центра.

Во избежание возникновения единой точки отказа настройте консоль аппаратного обеспечения (HMC) для использования нескольких серверов вызова сервисного центра. Каждое сервисное событие будет обрабатываться первым доступным сервером вызова сервисного центра. Если произойдет сбой соединения или передачи с этого сервера, то попытка отправки запроса на обслуживание будет повторяться со следующих доступных серверов до тех пор, пока она не будет успешно завершена или пока не произойдет сбой на всех серверах.

Сообщение о неполадке отправляется подключенной HMC, которая была распознана при анализе неполадок как главная консоль анализа для данной управляемой системы. Главная консоль также отправляет копию отчета о неполадке вспомогательным HMC. Вспомогательная HMC должна быть распознана в сети главной HMC. Вспомогательная HMC распознается главной HMC как дополнительный сервер вызова сервисного центра, если:

- Главная HMC настроена для использования "обнаруженных" серверов вызова сервисного центра, и сервер либо находится в той же подсети, что и главная HMC, либо управляет той же системой.
- Сервер вызова сервисного центра вручную добавлен в список консолей серверов, доступных для установки исходящих соединений.

## Подготовка к настройке HMC

Информация о параметрах конфигурации, которые необходимы для настройки.

Для настройки HMC необходимо ознакомиться со связанными концепциями, принять ряд решений и подготовить требуемую информацию.

Необходимая информация для подключения HMC к следующим узлам:

- Служебные процессоры управляемых систем
- Логические разделы управляемых систем
- Удаленные рабочие станции
- Служба IBM для реализации функций вызова сервисного центра

Для подготовки конфигурации HMC выполните следующие действия:

1. Приобретите и установите самый новый уровень версии HMC, который вы хотите установить.
2. Определите физическое расположение HMC по отношению к управляемым ею серверам. Если расстояние между HMC и управляемой системой превышает 7,5 метров, то необходимо настроить доступ к HMC через веб-браузер.
3. Определите серверы, которыми управляет HMC.
4. Определите, используется частная или открытая сеть для управления серверами. В частной сети следует использовать сервер DHCP, если не применяется конфигурация Cluster Systems Management (CSM). CSM не поддерживает IPv6. Для доступа к CSM нужно иметь две сети. Дополнительная информация о CSM приведена в соответствующей документации. Дополнительная информация об открытых и частных сетях приведена в разделе “Выбор типа сети (частная, открытая)” на стр. 63.
5. Если используется открытая сеть, то адрес FSP следует указать вручную через меню расширенного интерфейса управления системой (ASMI). Рекомендуется использовать частную сеть без возможности маршрутизации.
6. Если у вас две HMC, назначьте главную и вспомогательную HMC. Главная HMC должна физически находиться ближе к системе и быть настроена для вызова сервисного центра.
7. Определите сетевые параметры, необходимые для подключения HMC к удаленным рабочим станциям, логическим разделам и сетевым устройствам.
8. Определите, как HMC должна вызывать сервисный центр. Можно выбрать исходящее интернет-соединение SSL, модемное соединение или VPN.
9. Определите пользователей HMC, пароли пользователей, а также выполняемые ими роли. Пользователи **hscroot** и **hscpe** должны быть с паролем.
10. Подготовьте следующую контактную информацию, необходимую для настройки вызова сервисного центра:
    - Имя компании
    - Имя администратора
    - Адрес электронной почты
    - Номера телефонов
    - Номера факсов
    - Адрес помещения, в котором предполагается установить HMC

11. Если планируется уведомлять операторов или администраторов об отправке информации в сервисный центр IBM, то укажите сервер SMTP и адреса электронной почты.
12. Необходимо задать следующие пароли:
    - Пароль доступа для идентификации HMC в FSP.
    - Пароль ASMI **администратора**.
    - Пароль ASMI **обычного** пользователя.

    Укажите пароли при первом подключении HMC к новому серверу. В случае применения резервной или второй консоли HMC необходимо получить пароль пользователя HMC и указать его при первом подключении к FSP управляемого сервера.

После завершения подготовки выполните инструкции раздела “Форма настройки HMC перед установкой” на стр. 48.

## Форма настройки HMC перед установкой

В этой справочной таблице приведена информация, необходимая для подготовки к установке.

### Улучшенная стратегия управления паролями для HMC

Необходимо задать новый пароль при первом использовании новой системы с HMC версии 9.940.0 или выше, а также после восстановления заводских параметров системы. Это изменение помогает исключить случай, когда у HMC остается всем известный пароль.

Начиная с версии HMC 9.940.0 пароль `hscroot` просрочен, и его необходимо поменять для доступа к функциям HMC. См. инструкции по изменению пароля в разделе https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm. При обновлении предыдущей версии HMC менять пароль необязательно.

### Параметры сети

Интерфейс LAN: выберите доступные адаптеры (например, eth0, eth1), с помощью которых HMC будет подключаться к управляемым системам, логическим разделам, сервисному центру или удаленным пользователям. За дополнительной информацией обратитесь к разделу “Сетевые соединения HMC” на стр. 38. Соединение с HMC может устанавливаться в частной или открытой сети.

**Пропускная способность и дуплексный режим адаптера Ethernet**

Введите требуемую пропускную способность и дуплексный режим адаптера Ethernet. Параметр автоматическое определение определяет оптимальный параметр для данных аппаратных средств. Стандартное значение = Автоматическое определение Пропускная способность задает пропускную способность в дуплексном режиме адаптера Ethernet. Выберите автоматическое определение, если не требуется указать конкретную пропускную способность. Любое устройство, подключенное к FSP (коммутаторы/HMC) должно работать в режиме Автоматически (быстродействие) / Автоматически (дуплексный), поскольку это режим FSP по умолчанию, который нельзя изменить.

*Таблица 10. Пропускная способность и дуплексный режим адаптера Ethernet*

| **Параметр** | **eth0** | **eth1** | **eth2** | **eth3** |
|---|---|---|---|---|
| **Выберите пропускную способность и дуплексный режим** | | | | |
| Пропускная способность (Автоматическое определение, 10/100/1000 дуплексный/ полудуплексный) | | | | |

Дополнительная информация об открытых и частных сетях приведена в разделе “Частные и открытые сети в среде HMC” на стр. 40.

| *Таблица 11. Частная или открытая сеть* | | | | |
|---|---|---|---|---|
| **Параметр** | **eth0** | **eth1** | **eth2** | **eth3** |
| Для каждого адаптера укажите **Частная** или **Открытая** сеть. | | | | |

Протокол динамической настройки хостов (DHCP) является автоматическим способом динамической настройки клиента. Данную HMC можно определить как сервер DHCP. Для первой или единственной HMC в частной сети разрешите HMC в качестве сервера DHCP. При настройке HMC в качестве сервера DHCP управляемые системы в сети автоматически настраиваются и обнаруживаются HMC.

Для адаптеров Ethernet, заданных как частные сети, заполните следующую таблицу:

| *Таблица 12. Сервер DHCP* | | |
|---|---|---|
| **Характеристики** | **eth0** | **eth1** |
| Определить эту HMC как сервер DHCP? (да/нет) | | |
| Если да, запишите диапазон IP-адресов, который будет использоваться. | | |

В случае применения HMC 7063-CR1 необходимо подключить порт **IPMI** Ethernet к сети, чтобы обеспечить доступ к контроллеру управления платформой (BMC) в HMC. За дополнительной информацией обратитесь к разделу “Настройка связи BMC” на стр. 64. Заполните следующую таблицу для соединения BMC.

| *Таблица 13. Соединение BMC* | |
|---|---|
| **Характеристики** | **IPMI** |
| Вы хотите настроить это соединение в режиме DHCP? (да/нет) | |
| Если "нет", введите указанные статические адреса ниже: | |
| IP-адрес: | |
| Маска подсети: | |
| Шлюз: | |

Для адаптеров Ethernet, заданных как *открытые* сети, заполните следующие таблицы. Более подробная информация о различных версиях протокола IP приведена в разделе “Настройка типов сетей HMC” на стр. 58.

**Применение IPv6**

Если вы используете IPv6, обсудите с администратором сети то, как необходимо получать IP-адреса. Затем заполните следующие таблицы:

| *Таблица 14. IPv6 (статический)* | | | | |
|---|---|---|---|---|
| **Параметр** | **eth0** | **eth1** | **eth2** | **eth3** |
| Используется статически заданный IP-адрес? Если да, то укажите его здесь. | | | | |

| *Таблица 15. IPv6 (сервер DHCP)* | | | | |
|---|---|---|---|---|
| **Параметр** | **eth0** | **eth1** | **eth2** | **eth3** |
| Получаете ли вы IP-адреса от сервера DHCP? (Да/Нет) | | | | |

| *Таблица 16. IPv6 (маршрутизатор IPv6)* | | | | |
|---|---|---|---|---|
| **Параметр** | **eth0** | **eth1** | **eth2** | **eth3** |
| Получаете ли вы IP-адреса от маршрутизатора IPv6? | | | | |

Дополнительная информация о настройке адресов IPv6 приведена в разделе “Установка адреса IPv6” на стр. 65. Дополнительная информация об использовании только адресов IPv6 приведена в разделе “Использование только адресов IPv6” на стр. 65.

**Применение IPv4**

Заполните следующие таблицы для адаптеров Ethernet, заданных как открытые сети с использованием IPv4.

| *Таблица 17. IPv4* | | | | |
|---|---|---|---|---|
| **Характеристики** | **eth0** | **eth1** | **eth2** | **eth3** |
| Получать IP-адреса автоматически? (да/нет) | | | | |
| Если "нет", введите указанный адрес ниже: | | | | |
| Адрес интерфейса TCP/IP: | | | | |
| Маска сети интерфейса TCP/IP: | | | | |
| Параметры брандмауэра: | | | | |
| Настроить параметры брандмауэра HMC? (да/нет) | | | | |

| *Таблица 17. IPv4 (продолжение)* | | | | |
|---|---|---|---|---|
| **Характеристики** | **eth0** | **eth1** | **eth2** | **eth3** |
| Если да, то перечислите приложения и IP-адреса, которые должны пропускаться через брандмауэр: | | | | |
| | | | | |

**Информация TCP/IP**

Уникальный адрес TCP/IP требуется для каждого узла, как для элемента поддержки (SE), так и для консоли аппаратного обеспечения (HMC). Заданная маска сети используется для создания уникального адреса (по умолчанию) для локальной частной LAN. Если узлы подключены к более крупной сети с устанавливаемым адресом TCP/IP, можно указать адрес этот TCP/IP. Стандартное значение генерируется системой.

**Параметры брандмауэра**

Параметры брандмауэра HMC создают защитный барьер, который разрешает или запрещает доступ к конкретным сетевым приложениям на HMC. Эти параметры управления можно устанавливать для каждого физического интерфейса сети отдельно; таким образом можно регулировать, через какую HMC будет предоставляться доступ к сетевым приложениям в каждой сети.

Если хотя бы один адаптер настроен как адаптер открытой сети, то для разрешения доступа к LAN с HMC потребуется следующая дополнительная информация:

| *Таблица 18. Адаптер открытой сети* | |
|---|---|
| **Информация о локальном хосте** | |
| Имя хоста HMC: | |
| Имя домена: | |
| Описание HMC: | |
| **Информация о шлюзе** | |
| Адрес шлюза: (nnn.nnn.nnn.nnn) | |
| Устройство шлюза: | |
| **Разрешение DNS** | |
| Использовать DNS? (да/нет) | |
| Если “да”, укажите очередность обращения к серверам DNS ниже: | |
| 1. | |
| 2. | |
| Порядок просмотра доменных суффиксов: | |
| 1. | |
| 2. | |

**Информация о локальном хосте**

Для того чтобы идентифицировать консоль аппаратного обеспечения (HMC) для сети, введите имя хоста и имя домена HMC. Введите полное имя хоста, кроме случаев, когда в сети используются только короткие имена. Пример имени домена: name.yourcompany.com

**Информация о шлюзе**
Для указания шлюза по умолчанию введите адрес TCP/IP, на который будут пересылаться пакеты IP. Адрес шлюза сообщает каждому компьютеру или сетевому устройству, когда пересылать данные, если целевая рабочая станция и отправитель находятся в разных подсетях.

**Включение DNS**
Система имен доменов (DNS) служит стандартным соглашением об именах для поиска компьютеров, использующих IP-протокол. Определив серверы DNS, можно вместо IP-адресов использовать имена хостов для идентификации серверов и консолей аппаратного обеспечения (HMC).

**Очередность обращения к серверам DNS**
Введите IP-адреса серверов DNS, которые нужно будет искать для преобразования имен хостов и IP-адресов. Очередность обращения доступна только тогда, когда DNS включен.

**Порядок просмотра доменных суффиксов**
Введите используемые доменные суффиксы. HMC использует доменные суффиксы, которые добавляются к неполным именам для обращений к DNS. Суффиксы просматриваются в порядке их следования в списке. Порядок просмотра доступен только тогда, когда DNS включен.

## Уведомление по электронной почте

Введите параметры электронной почты, если нужно получать уведомления об аппаратных неполадках в локальной системе по электронной почте.

*Таблица 19. Уведомление по электронной почте*

| **Характеристики** | **Поле ввода** |
|---|---|
| Адреса электронной почты: | |
| Сервер SMTP: | |
| Порт: | |
| **Уведомлять об ошибках:** | |
| Только события при неполадках для сервисного центра | |
| События при всех неполадках | |

**Сервер SMTP**
Введите адрес SMTP-сервера, который будет использоваться для отправки электронного сообщения. Пример имени сервера SMTP - `relay.us.ibm.com`.

SMTP - это протокол для отправки электронной почты. При использовании SMTP клиент отправляет сообщение и обменивается данными с сервером SMTP по протоколу SMTP.

Если вам не известен адрес SMTP сервера или нет уверенности в его правильности, обратитесь к администратору сети.

**Порт**
Введите номер порта сервера, который нужно оповещать о системном событии, или воспользуйтесь стандартным портом.

**Адреса электронной почты для получения уведомлений**
Введите настроенные адреса электронной почты для отправки сообщений о системных событиях.

- Для получения уведомлений о событиях, использующих функцию вызова сервисного центра, выберите **Только события, связанные с вызовом сервисного центра**.
- **События при всех неполадках** выбирают для получения извещения при наступлении любых событий.

## Контактная информация для сервисного обслуживания

| *Таблица 20. Контактная информация для сервисного обслуживания* | |
|---|---|
| **Характеристики** | **Поле ввода** |
| Имя компании | |
| | |
| Имя администратора | |
| Адрес электронной почты | |
| Номер телефона | |
| Дополнительный номер телефона | |
| Номер факса | |
| Дополнительный номер телефона | |
| | |
| Адрес местонахождения | |
| Адрес местонахождения 2 | |
| Город или населенный пункт | |
| Состояние | |
| Почтовый индекс | |
| Страна или регион | |
| Местонахождение HMC (если совпадает с вышеуказанным адресом администратора, укажите “то же”): | |
| Адрес местонахождения | |
| Адрес местонахождения 2 | |
| Город или населенный пункт | |
| Состояние | |
| Почтовый индекс | |
| Страна или регион | |

## Связь с сервисным центром и доступ

Выберите тип соединения для контактов с сервисным центром. Описание указанных методов, включая требования к характеристикам защиты и конфигурации, приведено в разделе “Выбор из существующих серверов вызова сервисного центра для соединения со службой поддержки для данной HMC” на стр. 72.

| *Таблица 21. Связь с сервисным центром и доступ* | |
|---|---|
| **Характеристики** | **Поле ввода** |
| SSL через Интернет | _____ |
| VPN через Интернет | _____ |

**SSL через Интернет:**
Если подключение консоли HMC к Интернету уже существует, то его можно использовать для подключения к обслуживающей системе. С сервисным центром можно связываться напрямую

по существующему интернет-соединению, защищенному SSL. Если требуется настроить SSL для соединения через прокси-сервер SSL, выберите **Использовать прокси-сервер SSL**.

| *Таблица 22. SSL* | |
|---|---|
| **Характеристики** | **Поле ввода** |
| Использовать SSL? (да/нет) | |
| Если "да", введите информацию ниже: | |
| Адрес: | |
| Порт: | |
| Идентифицировать на прокси-сервере SSL? | |
| Если "да", введите информацию ниже: | |
| Пользователь: | |
| Пароль: | |

**Используемый протокол соединения с Интернетом**

Дополнительная информация о различных протоколах Интернета приведена в разделе “Настройка типов сетей HMC” на стр. 58.

___ IPv4

___ IPv6

___ IPv4 и IPv6

**Виртуальная частная сеть (VPN)**

Если подключение консоли HMC к Интернету уже существует, то его можно использовать для подключения к обслуживающей системе. Если есть соединение с Интернетом, можно подключаться напрямую к обслуживающей системе через VPN.

**Прим.:** При выборе VPN через Интернет, другие опции выбирать нельзя.

## Серверы вызова сервисного центра

Определите, какие HMC необходимо настроить в качестве серверов для вызова сервисного центра и службы поддержки. Дополнительная информация об использовании нескольких серверов вызова сервисного центра приведена в разделе “Использование нескольких серверов вызова сервисного центра” на стр. 46.

___ Эту HMC

___ Другую HMC

При выборе **Другую HMC** перечислите другие HMC, настроенные как серверы вызова сервисного центра:

| *Таблица 23. Другие HMC настроены как серверы вызова сервисного центра* |
|---|
| **Список имен хостов или IP-адресов HMC, настроенных как серверы вызова сервисного центра** |
| |
| |
| |
| |
| |

### Дополнительные преимущества поддержки

#### Мои системы и премиальный поиск

| *Таблица 24. Мои системы и премиальный поиск* | |
|---|---|
| **Характеристики** | **Поле ввода** |
| Укажите свой ИД в IBM | _____ |
| Укажите любые дополнительные ИД в IBM | _____ |

Для получения доступа к ценной персонализированной вспомогательной информации в разделах Мои системы и Премиальный поиск веб-сайта Electronic Services заказчики должны зарегистрировать ИД в IBM в данной системе. При отсутствии ИД IBM зарегистрироваться для его получения можно на: www.ibm.com/account/profile.

**Прим.:** IBM предоставляет персонализированные веб-функции, в которых используется информация, собранная приложением IBM Electronic Service Agent. Для того чтобы иметь возможность пользоваться этими функциями, необходимо сначала зарегистрироваться на веб-сайте регистрации в IBM по адресу http://www.ibm.com/account/profile.

Для предоставления пользователям права на использование информации Electronic Service Agent с целью персонализации веб-функций введите ИД в IBM, зарегистрированный на веб-сайте регистрации IBM. Для ознакомления с ценной информацией поддержки, доступной для заказчиков, зарегистрировавших ИД в IBM в своих системах, перейдите к разделу http://www.ibm.com/support/electronic.

## Настройка HMC

Рассмотрена настройка сетевых соединений, защиты, служебных приложений и некоторых параметров для пользователей.

В зависимости от предполагаемого уровня настройки конфигурации HMC, можно воспользоваться несколькими вариантами настройки HMC, выбирая из них наиболее подходящий для своих задач. Инструментальное средство Мастер пошаговой настройки из HMC позволяет легко и быстро выполнить настройку HMC. Мастер предоставляет возможность выбрать быстрое прохождение, при этом быстро создается рекомендуемая среда HMC. Кроме того, в нем предусмотрена возможность подробного ознакомления с доступными параметрами. Настройку можно также выполнить без помощи мастера в соответствии с инструкциями из раздела Настройка HMC с помощью меню HMC.

Перед выполнением настройки получите обязательную информацию о конфигурации, которая потребуется для успешного выполнения шагов. Список обязательной информации приведен в разделе “Подготовка к настройке HMC” на стр. 47. По завершении подготовки выполните инструкции из раздела “Форма настройки HMC перед установкой” на стр. 48 и вернитесь к этому разделу.

### Настройка HMC с помощью быстрого выполнения мастера пошаговой настройки

В большинстве случаев HMC можно настроить для эффективной работы с помощью многочисленных стандартных параметров. Для того чтобы быстро и эффективно подготовить HMC к работе, воспользуйтесь данной справочной таблицей быстрого выполнения. После выполнения этих действий HMC будет настроена в качестве сервера DHCP частной (подключенной напрямую) сети.

## Настройка HMC с помощью меню

В этом разделе приведен полный список всех задач настройки HMC, направляющих пользователя в процессе настройки HMC. Выберите данный пункт, если Мастер пошаговой настройки не будет использован.

Для вступления в силу параметров конфигурации необходимо будет перезапустить HMC, поэтому имеет смысл распечатать данную таблицу, чтобы пользоваться ею при настройке HMC.

В данном документе имеются ссылки на задачи, не вошедшие в документ. Доступ к Сведения об аппаратном обеспечении IBM Power Systems можно получить из HMC или в сети. В HMC ссылка на IBM Knowledge Center доступна в правом верхнем углу панели задач. В Интернете справочная система IBM Knowledge Center размещена на веб-сайте https://www.ibm.com/support/knowledgecenter.

В данном документе имеются ссылки на задачи, не вошедшие в данный PDF. Для получения доступа к дополнительным материалам поддержки можно обратиться к разделу **Дополнительные ресурсы** на начальных страницах HMC.

**Предварительные требования**

Перед тем, как приступить к настройке HMC с помощью меню HMC, выполните подготовительные действия, описанные в разделе “Подготовка к настройке HMC” на стр. 47.

*Таблица 25. Задачи настройки HMC вручную и источники связанной информации*

| **Задача** | **Где искать связанную информацию** |
|---|---|
| 1. Запустите HMC. | “Запуск HMC” на стр. 57 |
| 2. Задайте дату и время. | |
| 3. Измените стандартные пароли. | |
| 4. Создайте дополнительных пользователей и вернитесь к этой справочной таблице. | |
| 5. Настройте сетевые соединения. | “Настройка типов сетей HMC” на стр. 58 |
| 6. Для модели HMC 7063-CR1 необходимо настроить IP-адрес контроллера управления платформой (BMC). | “Настройка связи BMC” на стр. 64 |
| 7. При использовании открытой сети и фиксированных IP-адресов установите идентификационную информацию. | |
| 8. При использовании открытой сети и фиксированных IP-адресов настройте запись маршрутизации как стандартный шлюз. | “Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 67 |
| 9. При использовании открытой сети и фиксированных IP-адресов настройте службы имен доменов. | “Настройка служб имен доменов” на стр. 67 |
| 10. При использовании фиксированных IP-адресов и включении DNS настройте доменные суффиксы. | “Настройка доменных суффиксов” на стр. 68 |
| 11. Настройте сервер для соединения со службой поддержки IBM и вернитесь к данной справочной таблице после выполнения этого шага. | “Настройка локальной консоли для отправки сервисному центру сообщений об ошибках” на стр. 70 |
| 12. Настройте Администратор событий для вызова сервисного центра. | “Настройка Администратора событий для вызова сервисного центра” на стр. 74 |

| *Таблица 25. Задачи настройки HMC вручную и источники связанной информации (продолжение)* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 13. Подключите управляемую систему к источнику питания. | |
| 14. Укажите пароли для управляемой системы, а также пароли ASMI (общий и администратора). | “Задание паролей для управляемой системы” на стр. 75 |
| 15. Задайте дату и время управляемой системы с помощью ASMI. | |
| 16. Запустите управляемую систему и вернитесь к этой справочной таблице. | |
| 17. Убедитесь, что в управляемой системе создан один логический раздел. | |
| 18. Необязательно: Добавьте другую управляемую систему и вернитесь к этой справочной таблице. | |
| 19. Необязательно: При установке нового сервера с HMC настройте логические разделы и установите операционную систему. | |
| 20. Если вы не устанавливаете новый сервер, то выполните задачи заключительного этапа настройки для дополнительной настройки конфигурации. | “Действия после настройки” на стр. 76 |

### *Запуск HMC*

Войдите в HMC и выберите рабочий язык для интерфейса. Для первого входа в HMC воспользуйтесь стандартными ИД `hscroot` и паролем `abc123`.

## Об этой задаче

Для запуска HMC выполните следующие действия:

## Процедура

1. Включите HMC, нажав кнопку питания.
2. Если предпочитаемым языком является английский, перейдите к шагу 4.

   Если предпочтение отдается другому языку, введите номер **2** после предложения изменить локаль.

   **Прим.:** Для ответа на предложение пользователю дается 30 секунд.
3. Выберите необходимую локаль в окне **Выбор локали** и нажмите кнопку **OK**. Локаль определяет язык, который используется интерфейсом HMC.
4. Выберите **Войти и запустить веб-приложение Консоль аппаратного обеспечения**.
5. Войдите в HMC, используя приведенный ниже стандартный ИД и пароль пользователя:

   ИД: `hscroot`
   Пароль: `abc123`

   **HMC Enhanced**
   Отображает новый расширенный графический пользовательский интерфейс с расширенными функциями PowerVM.

**HMC Classic**
Отображает стандартный графический пользовательский интерфейс без расширенных функций PowerVM.

**Прим.:** Если HMC работает в качестве сервера DHCP, то она применяет пароль по умолчанию при первом подключении к служебному процессору.

6. Нажмите клавишу Enter.

### *Изменение даты и времени*

Работающие от батареи часы хранят дату и время для консоли аппаратного обеспечения (HMC). Иногда необходимо восстановить дату и время консоли, например, в случае замены батарей или при физическом перемещении системы в другой часовой пояс. Знакомит с процедурой изменения даты и времени для HMC.

## Об этой задаче

При смене информации о дате и времени внесенные изменения не отразятся на системах и логических разделах под управлением HMC.

Для изменения даты и времени HMC выполните следующие действия:

## Процедура

1. Проверьте, входите ли вы в группу пользователей с одной из ролей:
   - Главный администратор
   - Сотрудник сервисного представительства
   - Оператор
   - Наблюдатель
2. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
3. На панели содержимого выберите **Изменить дату и время**.
4. При выборе пункта **UTC** в поле **Часы** значение времени будет настроено автоматически как сезонное время выбранного часового пояса. Введите дату, время и часовой пояс и нажмите **OK**.

## Результаты

### *Настройка типов сетей HMC*

Настройка HMC для взаимодействия с управляемой системой, логическими разделами, удаленными пользователями и службой поддержки.

*Настройка HMC для подключения к управляемой системе по открытой сети*
Процедура настройки HMC для подключения к управляемой системе по открытой сети.

## Прежде чем начать

Для того чтобы настроить HMC для подключения к управляемой системе по открытой сети, выполните следующие действия:

*Таблица 26. Настройка HMC для подключения к управляемой системе по открытой сети*

| **Задача** | **Где искать связанную информацию** |
|---|---|
| 1. Выберите интерфейс управляемой системы. Рекомендуемый интерфейс: **eth0**. | “Форма настройки HMC перед установкой” на стр. 48 |

| *Таблица 26. Настройка HMC для подключения к управляемой системе по открытой сети (продолжение)* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 2. Выберите порты Ethernet для HMC. | “Идентификация порта Ethernet, определяемого как eth0” на стр. 61 |
| 3. Настройте адаптер Ethernet. Для этого выполните следующие задачи: | |
| a. Укажите пропускную способность. | “Установка пропускной способности” на стр. 63 |
| b. Выберите тип открытой сети. | “Выбор типа сети (частная, открытая)” на стр. 63 |
| c. Укажите статические адреса. | “Установка адреса IPv6” на стр. 65 |
| d. Укажите брандмауэр. | “Изменение параметров брандмауэра HMC” на стр. 66 |
| e. Настройте шлюз по умолчанию. | “Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 67 |
| f. Настройте DNS. | “Настройка служб имен доменов” на стр. 67 |
| 4. Настройте дополнительные адаптеры (если они установлены). | |
| 5. Проверьте соединение между управляемым сервером и HMC. | “Проверка соединения между HMC и управляемой системой” на стр. 76 |

*Настройка HMC для подключения к управляемой системе по частной сети*
Процедура настройки HMC для подключения к управляемой системе по частной сети.

## Прежде чем начать

Для того чтобы настроить HMC для подключения к управляемой системе по частной сети, выполните следующие действия:

| *Таблица 27. Настройка HMC для подключения к управляемой системе по частной сети* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 1. Выберите интерфейс управляемой системы. | “Форма настройки HMC перед установкой” на стр. 48 |
| 2. Выберите порты Ethernet для HMC. | “Идентификация порта Ethernet, определяемого как eth0” на стр. 61 |
| 3. Настройте HMC в качестве сервера DHCP. | “Настройка HMC в качестве сервера DHCP” на стр. 64 |
| 4. Проверьте соединение между управляемым сервером и HMC. | “Проверка соединения между HMC и управляемой системой” на стр. 76 |

*Настройка HMC для подключения к логическим разделам по открытой сети*

## Прежде чем начать

Для того чтобы настроить HMC для подключения к логическим разделам по открытой сети, выполните следующие действия:

| *Таблица 28. Настройка HMC для подключения к логическим разделам по открытой сети* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 1. Выберите интерфейс управляемой системы. | “Форма настройки HMC перед установкой” на стр. 48 |
| 2. Выберите порты Ethernet для HMC. | “Идентификация порта Ethernet, определяемого как eth0” на стр. 61 |
| 3. Настройте адаптер Ethernet. Для этого выполните следующие задачи: | |
| a. Укажите пропускную способность. | “Установка пропускной способности” на стр. 63 |
| b. Выберите тип открытой сети. | “Выбор типа сети (частная, открытая)” на стр. 63 |
| c. Укажите статические адреса. | “Установка адреса IPv6” на стр. 65 |
| d. Укажите брандмауэр. | “Изменение параметров брандмауэра HMC” на стр. 66 |
| e. Настройте шлюз по умолчанию. | “Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 67 |
| f. Настройте DNS. | “Настройка служб имен доменов” на стр. 67 |
| 4. Настройте дополнительные адаптеры (если они установлены). | |
| 5. Проверьте соединение между управляемым сервером и HMC. | “Проверка соединения между HMC и управляемой системой” на стр. 76 |

*Настройка HMC для подключения к удаленным пользователям по открытой сети*

## Прежде чем начать

Для того чтобы настроить HMC для подключения к удаленным пользователям по открытой сети, выполните следующие действия:

| *Таблица 29. Настройка HMC для подключения к удаленным пользователям по открытой сети* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 1. Выберите интерфейс управляемой системы. | “Форма настройки HMC перед установкой” на стр. 48 |
| 2. Выберите порты Ethernet для HMC. | “Идентификация порта Ethernet, определяемого как eth0” на стр. 61 |
| 3. Настройте адаптер Ethernet. Для этого выполните следующие задачи: | |
| a. Укажите пропускную способность. | “Установка пропускной способности” на стр. 63 |
| b. Выберите тип открытой сети. | “Выбор типа сети (частная, открытая)” на стр. 63 |
| c. Укажите статические адреса. | “Установка адреса IPv6” на стр. 65 |
| d. Укажите брандмауэр. | “Изменение параметров брандмауэра HMC” на стр. 66 |

| *Таблица 29. Настройка HMC для подключения к удаленным пользователям по открытой сети (продолжение)* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| e. Настройте шлюз по умолчанию. | “Настройка записи маршрутизации в качестве стандартного шлюза” на стр. 67 |
| f. Настройте DNS. | “Настройка служб имен доменов” на стр. 67 |
| g. Настройте суффиксы. | “Настройка доменных суффиксов” на стр. 68 |
| 4. Настройте дополнительные адаптеры (если они установлены). | |

*Настройка параметров сервера HMC для вызова сервисного центра*

## Прежде чем начать

Для настройки параметров сервера HMC для вызова сервисного центра и отправки сообщений о неполадках выполните следующие шаги:

| *Таблица 30. Настройка параметров сервера HMC для вызова сервисного центра* | |
|---|---|
| **Задача** | **Где искать связанную информацию** |
| 1. Убедитесь, что у вас есть все необходимые сведения о клиенте | “Форма настройки HMC перед установкой” на стр. 48 |
| 2. Настройте HMC для отправки сообщений об ошибках или выберите существующий сервер вызова сервисного центра | “Настройка локальной консоли для отправки сервисному центру сообщений об ошибках” на стр. 70<br>“Выбор из существующих серверов вызова сервисного центра для соединения со службой поддержки для данной HMC” на стр. 72 |
| 3. Убедитесь, что конфигурация вызова сервисного центра функционирует | “Проверка работоспособности соединения с сервисным центром и службой поддержки” на стр. 72 |
| 4. Предоставьте пользователям права доступа для просмотра собранных системных данных | “Предоставление пользователям права доступа для просмотра собранных системных данных” на стр. 73 |
| 5. Запланируйте передачу системных данных | “Передача сервисных данных” на стр. 73 |

*Идентификация порта Ethernet, определяемого как eth0*
Ethernet должна подключаться к управляемому серверу через порт Ethernet `eth0` в HMC.

Если в разъемах PCI HMC не установлены дополнительные адаптеры Ethernet, то основной встроенный порт Ethernet HMC всегда определяет как `eth0` или `eth1` при использовании HMC в качестве сервера DHCP для управляемых систем.

Если дополнительные адаптеры Ethernet в разъемах PCI установлены, то определение порта как `eth0` будет зависеть от расположения и типа установленных адаптеров Ethernet.

**Прим.:** Следующие общие правила могут быть неприменимы в некоторых конфигурациях.

В следующей таблице описаны правила размещения адаптеров Ethernet для разных типов HMC.

| *Таблица 31. Типы HMC и соответствующие правила размещения Ethernet* | |
|---|---|
| **Тип HMC** | **Правила размещения Ethernet** |
| Смонтированные в стойке HMC с двумя встроенными портами Ethernet. | HMC поддерживает только один дополнительный адаптер Ethernet.<br>• Если дополнительный адаптер Ethernet установлен, то этот порт определяется как `eth0`. В этом случае основной встроенный порт Ethernet определяется как `eth1`, а дополнительный встроенный порт Ethernet - как `eth2`.<br>• Для двухпортового адаптера Ethernet порт с обозначением Act/Link A - `eth0`. Порт с обозначением `Act/link B` - `eth1`. В этом случае основной встроенный порт Ethernet определяется как `eth2`, а дополнительный встроенный порт Ethernet - как `eth3`.<br>• Если ни один адаптер не установлен, то основной встроенный порт Ethernet определяется как `eth0`. |
| Автономные модели с одним встроенным портом Ethernet. | Рассмотренные определения будут зависеть от типа устанавливаемого адаптера Ethernet:<br>• Если установлен только один адаптер Ethernet, то он будет определяться как `eth0`.<br>• Для двухпортового адаптера Ethernet порт с обозначением `Act/link A` - `eth0`. Порт с обозначением `Act/link B` - `eth1`. При этом основной встроенный порт Ethernet определяется как `eth2`.<br>• Если ни один адаптер не установлен, то встроенный порт Ethernet определяется как `eth0`.<br>• Если установлено несколько адаптеров Ethernet, прочитайте раздел “Определение имени интерфейса для адаптера Ethernet” на стр. 62. |

*Определение имени интерфейса для адаптера Ethernet*
При настройке HMC в качестве сервера DHCP этот сервер сможет работать только с соединителями сетевой интерфейсной платы (NIC), которые HMC идентифицирует как `eth0` и `eth1`. Также необходимо выбрать соединитель NIC для подключения кабеля Ethernet. Обратитесь к соответствующей информации по выбору соединителей NIC, которые HMC идентифицирует как `eth0` и `eth1`.

## Об этой задаче

Для того чтобы определить имя, присваиваемое HMC адаптеру Ethernet, выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Управление HMC**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. В окне **Изменить параметры сети** откройте вкладку **Адаптеры LAN**. В следующем примере показано, что этот порт Ethernet определен как `eth0`: `Ethernet eth0 52:54:00:fa:b6:8e (<IP-адрес-HMC>)`.
4. Запишите результаты. Если необходимо просмотреть или изменить параметры адаптера LAN, щелкните на **Сведения**.
5. Нажмите кнопку **OK**.

*Установка пропускной способности*
Процедура установки пропускной способности и дуплексного режима адаптера Ethernet.

## Прежде чем начать

Стандартным параметром адаптера HMC является **Автоматическое определение**. Если адаптер подключен к коммутатору LAN, то необходимо настроить параметры портов коммутатора. Для настройки пропускной способности и дуплексного режима выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и щелкните на **Сведения**.
5. В разделе информации о локальной сети (LAN) выберите **Автоматическое обнаружение** или укажите требуемую пропускную способность и дуплексный режим.
6. Нажмите кнопку **OK**.

*Выбор типа сети (частная, открытая)*
*Частная сеть обслуживания* состоит из консоли аппаратного обеспечения (HMC) и управляемых систем. Частная сеть обслуживания ограничивается консолями и системами, которыми они управляют. Это сеть, отдельная от сети компании. *Открытая сеть* состоит из частной сети обслуживания и сети компании. Кроме консолей и управляемых систем, в открытую сеть могут входить конечные точки сети, и сеть может охватывать несколько подсетей и сетевых устройств.

## Об этой задаче

Для выбора частной или общей сети выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.

4. Выберите нужный адаптер LAN и щелкните на **Сведения**.
5. Перейдите на вкладку **Адаптер LAN**.
6. На странице информации о локальной сети выберите **Частная** или **Открытая**.
7. Нажмите кнопку **OK**.

*Настройка HMC в качестве сервера DHCP*
Протокол динамической настройки хостов (DHCP) является автоматическим способом динамической настройки клиента.

Для настройки консоли аппаратного обеспечения (HMC) в качестве сервера DHCP выполните следующие действия:

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите нужный адаптер LAN и щелкните на **Сведения**.
4. Выберите **Частная** и укажите тип сети.
5. В разделе Сервер DHCP включите переключатель **Разрешить сервер DHCP**, чтобы разрешить HMC в качестве сервера DHCP.

   **Прим.:** HMC можно настроить в качестве сервера DHCP только в частной сети. Если используется открытая сеть, то опция **Включить DHCP** будет недоступна.
6. Введите диапазон адресов сервера DHCP.
7. Нажмите кнопку **OK**.

Если HMC настроена в качестве сервера DHCP в частной сети, необходимо проверить правильность настройки частной сети HMC DHCP. Информация о соединении HMC с частной сетью приведена в разделе “Выбор типа сети (частная, открытая)” на стр. 63.

См. раздел “ HMC в качестве сервера DHCP” на стр. 41.

*Настройка связи BMC*
Можно настроить или просмотреть сетевые параметры BMC для консоли управления.

**Прим.:** Эта задача относится только к 7063-CR1. Это соединение необходимо для подключения к контроллеру управления платформой (BMC) в HMC.

Для настройки соединения BMC выполните следующие действия:

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети BMC/IPMI**.
3. Выберите режим соединения (**DHCP** или **Статический**).

   Если выбран режим **Статический**, то укажите следующие адреса:

   - **IP address**
   - **Маска подсети**
   - **Шлюз**
4. Нажмите кнопку **OK**.

Сетевое соединение BMC можно также настроить с помощью интерфейса загрузчика ядра Petitboot. Дополнительная информация приведена в разделе Настройка IP-адреса встроенного программного обеспечения.

*Установка IPv4-адреса*
Знакомит с процессом установки IPv4-адреса на HMC.

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и щелкните на **Сведения**.
5. Выберите вкладку **Основные параметры**.
6. Выберите адрес IPv4.
7. Если выбран пункт Указать IP-адрес, введите адрес интерфейса TCP/IP и маску сети интерфейса TCP/IP.
8. Нажмите кнопку **OK**.

*Установка адреса IPv6*
Описан процесс установки адреса IPv6 на HMC.

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и щелкните на **Сведения**.
5. Выберите вкладку **Параметры IPv6**.
6. Выберите опцию **Автонастройка** или добавьте статический IP-адрес.
7. При добавлении IP-адреса, введите адрес IPv6 и длину префикс, а затем нажмите **OK**.
8. Нажмите кнопку **OK**.

*Использование только адресов IPv6*
Настройка HMC для использования только адресов IPv6.

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и щелкните на **Сведения**.
5. Выберите **Без адресов IPv4**.
6. Выберите вкладку **Параметры IPv6**.
7. Выберите **Использовать DHCPv6 для настройки параметров IP** или добавьте статические IP-адреса и нажмите кнопку **OK**.

## Дальнейшие действия

После нажатия кнопки **OK** необходимо перезапустить HMC, чтобы изменения вступили в силу.

### *Изменение параметров брандмауэра HMC*

В открытой сети брандмауэр обычно используется для управления внешним доступом к сети компании. В HMC также имеется брандмауэр на каждом Ethernet адаптере. Для удаленного управления HMC или предоставления удаленного доступа другим пользователям измените параметры брандмауэра адаптера Ethernet на консоли HMC, подключенной к вашей открытой сети.

## Об этой задаче

Для настройки брандмауэра выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**.
3. Щелкните на вкладке **Сетевые адаптеры**.
4. Выберите нужный адаптер LAN и щелкните на **Сведения**.
5. Выберите вкладку **Брандмауэр**.
6. С помощью одного из приведенных ниже методов можно разрешить любой IP-адрес, использующий конкретное приложение через брандмауэр, или указать один или несколько IP-адресов:
   - Разрешить любой IP-адрес, использующий конкретное приложение через брандмауэр:
     a. В верхнем окне выделите приложение.
     b. Выберите **Разрешить входящие**. Приложение появится в нижнем окне - это говорит о том, что приложение выбрано.
   - Укажите IP-адреса, разрешенные через брандмауэр:
     a. В верхнем окне выделите приложение.
     b. Выберите **Разрешить входящие по IP-адресу**.
     c. В окне Разрешенные хосты введите IP-адрес и маску сети.
     d. Выберите **Добавить** и нажмите кнопку **OK**.
7. Нажмите кнопку **OK**.

*Включение доступа через удаленную оболочку с ограничениями*

При настройке брандмауэра можно включить доступ через удаленную оболочку с ограничениями.

## Об этой задаче

Для включения доступа через удаленную оболочку с ограничениями выполните следующие действия:

## Процедура

1. В области навигации выберите **Управление HMC**.
2. Выберите **Удаленное выполнение команд**.
3. Выберите **Разрешить удаленное выполнение команд по протоколу ssh** и нажмите кнопку **OK**.

## Дальнейшие действия

Доступ через удаленную оболочку с ограничениями включен.

*Включение удаленного доступа с помощью веб-браузера*

Можно включить удаленный доступ к консоли аппаратного обеспечения (HMC) через веб-браузер.

## Об этой задаче

Для включения удаленного доступа через веб-браузер выполните следующие действия:

## Процедура

1. В области навигации выберите **Управление HMC**.
2. Выберите **Удаленная работа**.
3. Выберите **Включить** и нажмите кнопку **OK**.

## Дальнейшие действия

Удаленный доступ включен.

### *Настройка записи маршрутизации в качестве стандартного шлюза*

Знакомит с настройкой записи маршрутизации в качестве стандартного шлюза. Эта задача доступна, когда используется открытая сеть.

## Прежде чем начать

Для настройки записи маршрутизации в качестве шлюза по умолчанию выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите вкладку **Маршрутизация**.
4. В области Информация о шлюзе по умолчанию введите адрес и устройства шлюза записи маршрутизации в качестве стандартного шлюза.
5. Нажмите кнопку **OK**.

### *Настройка служб имен доменов*

При установке открытой сети настройте службы имен доменов.

## Об этой задаче

При установке открытой сети настройте службы имен доменов. Система имен доменов (DNS) - это распределенная база данных для управления именами хостов и их соответствующими адресами протокола IP (IP-адресами). Для настройки служб имен доменов необходимо включить DNS и указать порядок просмотра доменных суффиксов.

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.

2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Изменение параметров сети.
3. Выберите вкладку **Службы имен**.
4. Для включения DNS выберите **DNS включено**.
5. Укажите порядок просмотра серверов DNS и доменных суффиксов и нажмите кнопку **Добавить**.
6. Нажмите кнопку **OK**.

### *Настройка доменных суффиксов*
Список доменных суффиксов служит для поиска IP-адреса, начиная с первой записи списка.

## Об этой задаче

Доменный суффикс - это строка после имени хоста, которая помогает определить его IP-адрес. Например, адрес имени хоста `myname` может быть не определен. Но если в таблице доменных суффиксов присутствует строка `myloc.mycompany.com`, то сервер попытается определить также адрес имени `myname.mloc.mycompany.com`.

Для настройки записи суффикса домена выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Изменить параметры сети**. Откроется окно Настройка параметров сети.
3. Выберите вкладку **Службы имен**.
4. Введите строку в качестве записи доменного суффикса.
5. Выберите **Добавить**, и запись будет добавлена в список.

### *Настройка HMC для использования удаленной идентификации с помощью LDAP*
Консоль аппаратного обеспечения (HMC) можно настроить для использования удаленной идентификации с помощью LDAP (Упрощенный протокол доступа к каталогам).

## Прежде чем начать

Когда пользователь входит в HMC, сначала идентификация осуществляется путем сравнения с локальным файлом пароля. Если локальный файл пароля не обнаружен, HMC может связаться с удаленным сервером LDAP для идентификации. Для использования удаленной идентификации с помощью LDAP необходимо настроить HMC.

**Прим.:** Прежде чем настраивать HMC для использования удаленной идентификации с помощью LDAP, необходимо убедиться, что существует рабочее сетевое соединение между HMC и серверами LDAP. Дополнительная информация о настройке сетевых соединений HMC приведена в разделе “Настройка типов сетей HMC” на стр. 58.

## Об этой задаче
Для настройки идентификации LDAP в HMC выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Пользователи и защита**  , затем выберите **Защита систем и консоли**.

2. На панели содержимого выберите **Управление LDAP**. Откроется окно Описание сервера LDAP.
3. Выберите **Включить LDAP**.
4. Укажите сервер LDAP, который будет использоваться при идентификации.
5. Определите атрибут LDAP, используемый для идентификации пользователя. Значение по умолчанию - **uid**, но можно использовать собственное.
6. Определите для сервера LDAP дерево отличительного имени, также известное как база поиска.
7. Нажмите кнопку **OK**.
8. Если пользователь желает использовать идентификацию с помощью LDAP, он должен настроить свой профайл для использования удаленной идентификации LDAP вместо локальной идентификации.

## *Настройка HMC для использования Центров рассылки ключей (KDC) для удаленной идентификации Kerberos*

HMC можно настроить для использования Центров рассылки ключей для удаленной идентификации Kerberos

### Прежде чем начать

Когда пользователь входит в HMC, идентификация сначала выполняется по локальному файлу паролей. Если локальный файл пароля не обнаружен, HMC может связаться с удаленным сервером Kerberos для идентификации. Для использования удаленной идентификации Kerberos необходимо настроить HMC.

**Прим.:** Прежде чем настраивать HMC для использования Центров рассылки ключей для удаленной идентификации Kerberos, необходимо убедиться, что существует рабочее сетевое соединение между HMC и Центрами рассылки ключей. Дополнительная информация о настройке сетевых соединений HMC приведена в разделе “Настройка типов сетей HMC” на стр. 58.

### Об этой задаче

Для настройки HMC, чтобы она использовала серверы KDC для удаленной идентификации Kerberos, выполните следующие действия:

### Процедура

1. Включите службу Протокола сетевого времени (NTP) в HMC и задайте синхронизацию времени серверов HMC и KDC с одним и тем же сервером NTP. Для того чтобы включить службу NTP в HMC выполните следующие действия:
   a) В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
   b) На панели содержимого выберите **Изменить дату и время**.
   c) Выберите вкладку **Конфигурация NTP**.
   d) Выберите **Включить службу NTP в данной HMC**.
   e) Нажмите кнопку **OK**.
2. Настройте каждый профайл удаленного пользователя HMC для использования удаленной идентификации Kerberos, а не локальной идентификации.
3. (необязательно) Импортируйте файл служебных ключей в HMC. В файле служебных ключей содержится субъект хоста, идентифицирующий HMC для сервера KDC. Файлы служебных ключей также известны как *keytab*. Для того чтобы импортировать файл служебных ключей в HMC, выполните следующие действия:

a) В области навигации щелкните на значке **Пользователи и защита**  , затем выберите **Защита систем и консоли**.

b) На панели содержимого выберите **Управление KDC**.

c) Выберите **Действия > Импортировать служебный ключ**. Откроется окно Импорта служебного ключа.

d) Введите расположение файла служебного ключа.

e) Нажмите кнопку **OK**.

4. Добавьте новый сервер KDC в HMC. Для добавления нового сервера KDC в данную HMC этого выполните следующие действия:

a) В области навигации щелкните на значке **Пользователи и защита**  , затем выберите **Защита систем и консоли**.

b) На панели содержимого выберите **Управление KDC**.

c) Выберите **Действия > Добавить сервер KDC**. Откроется окно Импорта служебного ключа.

d) Введите область и имя хоста или IP-адрес сервера KDC.

e) Нажмите кнопку **OK**.

## *Настройка локальной консоли для отправки сервисному центру сообщений об ошибках*

Настройте HMC таким образом, чтобы она могла отправлять сервисному центру сообщения об ошибках с помощью соединений LAN.

*Настройка HMC для соединения со службой поддержки с помощью мастера настройки вызова сервисного центра*

Настройка HMC в качестве сервера вызова сервисного центра с помощью мастера.

### Прежде чем начать

В этой процедуре описывается, как настроить HMC в качестве сервера вызова сервисного центра с помощью прямых (по LAN) и непрямых (по SSL) интернет-соединений.

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. См. раздел “Подготовка к настройке HMC” на стр. 47.
- В случае настройки доступа к Интернету через прокси-сервер также необходима следующая информация:
  - IP-адрес и порт прокси-сервера
  - Идентификационные данные прокси-сервера
- Используемый адаптер **eth1** (адаптер для подключения к открытой сети). См. раздел “Выбор параметров сети в HMC” на стр. 38.
- Кабель Ethernet физически соединяет HMC с LAN.

Для настройки HMC в качестве сервера вызова сервисного центра с помощью мастера выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Мастер настройки вызова сервисного центра**. Откроется мастер настройки соединений и серверов вызова сервисного центра. Для настройки вызова сервисного центра следуйте инструкциям мастера установки.

*Настройка локальной консоли для отправки сервисному центру сообщений об ошибках*
Настройте HMC таким образом, чтобы она могла отправлять сервисному центру сообщения об ошибках с помощью соединений LAN.

*Настройка HMC для связи со службой поддержки через Интернет и SSL по LAN*
Процедура настройки HMC в качестве сервера вызова сервисного центра с помощью прямых (по LAN) и косвенных (через SSL) соединений с Интернетом.

## Прежде чем начать

Прежде чем приступить к выполнению процедуры, убедитесь в том, что:

- Администратор сети проверил, что соединение разрешено. См. раздел “Подготовка к настройке HMC” на стр. 47.
- Настроена контактная информация клиента. Для проверки контактной информации зайдите в интерфейс HMC и выберите **Обслуживание > Управление службами > Управление информацией о клиентах**.
- В случае настройки доступа к Интернету через прокси-сервер также необходима следующая информация:
  - IP-адрес и порт прокси-сервера
  - Идентификационные данные прокси-сервера
- Необходим по крайней мере один настроенный открытый сетевой интерфейс. См. раздел “Частные и открытые сети в среде HMC” на стр. 40.
- Кабель Ethernet физически соединяет HMC с LAN.

## Об этой задаче

Для настройки HMC в качестве сервера вызова сервисного центра через Интернет по LAN и SSL выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
2. В разделе Соединение выберите **Управление исходящими соединениями**. Откроется окно Консоли сервера вызова сервисного центра.
3. Выберите **Настроить**.
4. В окне Параметры исходящих соединений отметьте **Разрешить использование локальной системы в качестве сервера вызова сервисного центра**.
5. Примите условия соглашения.
6. В окне Параметры исходящих соединений выберите страницу **Интернет**.
7. Поставьте отметку в окне **Разрешить существующие соединения с Интернетом для обслуживания**.

8. При использовании SSL прокси-сервера поставьте отметку в окне **Использовать SSL прокси-сервер**.
9. Если используется прокси-сервер SSL, введите его адрес и порт. Такую информацию можно получить у администратора системы.
10. Если отмечено окно **Использовать SSL прокси-сервер**, и прокси-сервер требует идентификации по идентификатору и паролю пользователя, поставьте отметку в окне **Идентификация на SSL прокси-сервере**. Введите ИД пользователя и пароль. Информацию об ИД и пароле пользователя получите у администратора системы.
11. Выберите **Протокол связи с Интернетом**, который необходимо использовать.
12. На странице **Интернет** выберите **Проверить**.
13. В окне Тестирование Интернета нажмите кнопку **Запустить**.
14. Убедитесь, что проверка была успешно выполнена.
15. В окне Тестирование Интернета нажмите кнопку **Отмена**.
16. В окне Параметры исходящих соединений нажмите кнопку **OK**.

*Выбор из существующих серверов вызова сервисного центра для соединения со службой поддержки для данной HMC*
Выберите существующие серверы вызова сервисного центра HMC, которые распознаны или обнаружены HMC, для передачи отчетов об ошибках.

## Прежде чем начать

Обнаруженные HMC - это HMC, которые подключены как серверы вызова сервисного центра и либо находятся в той же подсети, либо управляют той же системой, что и данная HMC.

Для того чтобы выбрать обнаруженную HMC для вызова сервисного центра, когда HMC сообщает об ошибках, выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Управление исходящими соединениями**. Откроется окно Консоли сервера вызова сервисного центра.
3. Включите переключатель **Использовать обнаруженные консоли сервера вызова сервисного центра**. В HMC будет показан IP-адрес или имя хоста HMC, настроенных для вызова сервисного центра.
4. Нажмите кнопку **OK**.

## Результаты

Также можно вручную добавить существующие серверы вызова сервисного центра HMC, которые находятся в другой подсети. Выберите IP-адрес или имя хоста HMC, настроенной для вызова сервисного центра, и нажмите кнопку **Добавить**, затем кнопку **OK**.

*Проверка работоспособности соединения с сервисным центром и службой поддержки*
Отправка тестовой неполадки для проверки работоспособности соединения с сервисным центром и службой поддержки

## Об этой задаче

Для проверки работы конфигурации вызова сервисного центра выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Создать событие**.
3. Выберите **Проверка автоматического создания отчета о неполадках** и введите комментарий.
4. Выберите **Запросить обслуживание**. Дождитесь отправки запроса.
5. В окне Служебное управление выберите **Управление событиями**.
6. Выберите **Все сообщенные неполадки**.
7. Проверьте, присвоены ли событие PMH и номер неполадке.
8. Выберите это событие и нажмите кнопку **Закрыть**.
9. В окне **Закрыть** введите свое имя и краткий комментарий.

*Предоставление пользователям права доступа для просмотра собранных системных данных*
Для просмотра данных о системе необходимо предоставить пользователям права доступа.

## Прежде чем начать

Прежде чем предоставить пользователям права доступа для просмотра собранных системных данных, необходимо получить ИД IBM. Более подробная информация о получении ИД IBM приведена в разделе “Форма настройки HMC перед установкой” на стр. 48.

## Об этой задаче

Для предоставления пользователям прав доступа для просмотра собранных системных данных выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Предоставить пользователю права доступа**.
3. Введите свой ИД IBM.
4. Нажмите кнопку **OK**.

*Передача сервисных данных*
Сведения можно передавать в сервисный центр немедленно или запланировать их регулярную передачу.

## Прежде чем начать

IBM предоставляет персонализированные веб-функции, в которых используется информация, собранная программой IBM Electronic Service Agent. Для того чтобы иметь возможность пользоваться этими функциями, необходимо сначала зарегистрироваться на веб-сайте регистрации в IBM по адресу http://www.ibm.com/account/profile. Для предоставления пользователям права пользоваться информацией Electronic Service Agent с целью персонализации веб-функций обратитесь к разделу “Предоставление пользователям права доступа для просмотра собранных системных данных” на стр. 73. Более подробная информация о преимуществах регистрации ИД IBM для систем приведена в разделе http://www.ibm.com/support/electronic.

**Прим.:** Как только HMC установлена и настроена, необходимо предоставить информацию для официального сервисного центра.

## Об этой задаче

Для передачи служебной информации выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Передать сервисные данные**.
3. Выполните задачи в окне **Передача сервисных данных** и нажмите кнопку **OK**.

### *Настройка Администратора событий для вызова сервисного центра*

Рассмотрена настройка задачи Администратор событий для вызова сервисного центра. Эта задача позволяет отслеживать и утверждать данные, передаваемые из HMC в IBM.

Задача Администратор событий для вызова сервисного центра включается и выключается с помощью интерфейса командной строки HMC. Включение задачи Администратор событий для вызова сервисного центра предусматривает выключение автоматического вызова сервисного центра. Для того чтобы запретить вызов сервисного центра без подтверждения, необходимо включить режим Администратор событий для вызова сервисного центра на всех HMC в среде.

Для включения или выключения задачи Администратор событий для вызова сервисного центра выполните следующую команду:

```
chhmc -c emch
-s {enable | disable}
[--callhome {enable | disable}]
[--help]
```

**Прим.:** Включение задачи Администратор событий для вызова сервисного центра блокирует события вызова сервисного центра до их утверждения для задачи вызова сервисного центра. При выключении задачи Администратор событий для вызова сервисного центра не происходит автоматического включения функции вызова сервисного центра. Такая конфигурация позволяет избежать непреднамеренной передачи данных в IBM. Для задания требуемой конфигурации предусмотрены следующие опции командной строки:

- Включить задачу Администратор событий для вызова сервисного центра: **`chhmc -c emch -s enable`**
- Выключить задачу Администратор событий для вызова сервисного центра и повторно включить автоматический вызова сервисного центра: **`chhmc -c emch -s disable --callhome enable`**
- Выключить задачу Администратор событий для вызова сервисного центра без повторного включения автоматического вызова сервисного центра: **`chhmc -c emch -s disable --callhome disable`**

Убедитесь, что HMC может обмениваться данными с другими HMC, развернутыми в этой среде. В ходе регистрации HMC администратор событий для вызова сервисного центра выполняет проверку связи.

HMC можно зарегистрировать с помощью администратора событий для вызова сервисного центра. После регистрации HMC администратор событий запрашивает в зарегистрированной HMC события, ожидающие вызова сервисного центра IBM. администратор событий отображает данные, отправляемые в IBM, и утверждает события. После утверждения администратор событий разрешает зарегистрированной HMC продолжить операцию вызова сервисного центра.

Задачу Администратор событий для вызова сервисного центра можно запустить из любой HMC или из нескольких HMC. Для регистрации консоли управления в задаче Администратор событий для вызова сервисного центра выполните следующие действия:

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Администратор событий для вызова сервисного центра**.
2. На панели **Администратор событий для вызова сервисного центра** выберите **Управление консолями**.
3. В окне **Управление зарегистрированными консолями** выберите **Добавить консоль** для ввода информации для регистрации консоли управления в Администраторе событий для вызова сервисного центра.
4. Нажмите кнопку **OK**, чтобы сохранить изменения в списке зарегистрированных консолей управления.

**Прим.:** Администратор событий для вызова сервисного центра может работать, когда режим администратора событий выключен. Вы сможете зарегистрировать HMC и просмотреть события, однако администратор событий не будет управлять отправкой событий в сервисный центр.

### *Задание паролей для управляемой системы*

Вам необходимо задать пароли как для своего сервера, так и для расширенного интерфейса управления системой (ASM). Использование интерфейса HMC для задания этих паролей описывается далее.

#### Прежде чем начать

При получении сообщения Ожидание идентификации HMC предлагает пользователю установить пароли для управляемой системы.

#### Об этой задаче

Если сообщение Ожидание идентификации не получено, выполните следующие шаги, чтобы установить пароли для управляемой системы.

*Обновление пароля сервера*

#### Прежде чем начать

Для обновления пароля своего сервера выполните следующие действия:

#### Процедура

1. В области навигации выберите управляемую систему и щелкните на значке **Пользователи и защита**  , затем выберите **Пользователи и роли**.
2. Нажмите кнопку **Изменить пароль**. Откроется окно Обновление пароля.
3. Введите требуемую информацию и нажмите **OK**.

*Обновление общего пароля расширенного управления системой (ASM)*

#### Прежде чем начать

**Прим.:** Пароль по умолчанию для ИД обычного пользователя - `general`, для ИД администратора - `admin`.

Для обновления общего пароля ASM выполните следующие действия:

#### Процедура

1. Выберите управляемую систему в области навигации HMC.
2. В области задач выберите **Операции**.

3. Выберите **Расширенное управление системой (ASM)**. Откроется окно Запуск интерфейса ASM.
4. Выберите IP-адрес служебного процессора и нажмите **OK**. Откроется интерфейс ASM.
5. На панели приветствия ASMI введите ИД пользователя и пароль. Нажмите кнопку **Вход в систему**.
6. В области навигации разверните **Профайл входа в систему**.
7. Выберите **Изменить пароль**.
8. Укажите необходимую информацию и нажмите **Продолжить**.

*Восстановление пароля администратора расширенного управления системой (ASM)*

### Прежде чем начать
Для сброса пароля администратора обратитесь в официальный сервисный центр.

### *Проверка соединения между HMC и управляемой системой*
Проверка подключения к сети.

### Об этой задаче

Проверку соединения с сетью могут выполнять пользователи со следующими ролями:

- Главный администратор
- Сотрудник сервисного представительства

Для проверки соединения между HMC и управляемой системой выполните следующие действия:

### Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Параметры консоли**.
2. На панели содержимого выберите **Тест сетевого подключения**.
3. Во вкладке Отправить пробный пакет введите имя хоста или IP-адрес любой системы, с которой нужно установить соединение. Для проверки открытой сети введите имя шлюза. Нажмите кнопку **Проверить связь**.

### Результаты

Если логические разделы еще не созданы, то проверить связь с адресами невозможно. Для этого можно воспользоваться HMC. Дополнительная информация приведена в разделе Логические разделы.

Для того чтобы разобраться, как можно использовать HMC в сети, обратитесь к разделу “Сетевые соединения HMC” на стр. 38.

Дополнительная информация о настройке HMC для соединения с сетью приведена в разделе “Настройка HMC с помощью меню ” на стр. 56.

## Действия после настройки

После установки и настройки HMC можно создать резервную копию данных HMC.

### Резервное копирование данных консоли управления

Эта задача создает резервную копию (архив) данных, хранящихся на жестком диске HMC и являющихся критическими для поддержки операций HMC.

### Прежде чем начать

Для этого в удаленной системе должна быть настроена сетевая файловая система (NFS) или защищенная оболочка (ssh), и эта сеть должна быть доступной из HMC. Для выполнения указанной задачи необходимо завершить выполнение и перегрузить HMC. Эти задачи следует выполнять только с помощью HMC.

### Об этой задаче

Резервное копирование жесткого диска HMC в удаленную систему могут выполнять пользователи со следующими ролями:

- Главный администратор
- Оператор
- Сотрудник сервисного представительства

Резервное копирование данных HMC необходимо выполнять после внесения изменений в HMC или информацию, связанную с логическими разделами.

Данные HMC, хранящиеся на жестком диске, можно сохранять на DVD-RAM в локальной системе, в удаленной системе, смонтированной (например, по NFS) к HMC, или на удаленном сервере FTP.

**Прим.:** Для HMC модели 7063-CR1 можно подключить внешний привод DVD через USB.

С помощью HMC можно создать резервную копию всех важных данных. Типы таких данных перечислены ниже:

- Файлы пользовательских параметров
- Информация пользователей
- Файлы конфигурации платформы HMC
- Файлы протокола HMC
- Обновления HMC, внесенные посредством Службы исправлений.

Для резервного копирования жесткого диска HMC в удаленную систему выполните следующие действия:

### Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Создать резервную копию данных консоли управления**.
3. В окне **Создать резервную копию данных консоли управления** выберите опцию архивирования.
4. Нажмите кнопку **Далее**, затем следуйте инструкциям в соответствии с выбранной опцией.
5. Нажмите кнопку **OK**, чтобы продолжить процесс резервного копирования.

## Обновление, модернизация и миграция машинного кода HMC

Для HMC периодически выходят обновления, позволяющие добавить новые возможности и улучшить существующие. В этом разделе приведено различий операций обновления, модернизации и миграции машинного кода HMC. Кроме того, рассмотрены процедуры обновления, модернизации и миграции машинного кода HMC.

После завершения каждой задачи выполняется перезагрузка HMC без остановки разделов.

**Обновление кода HMC**

Применение пакета обслуживания для текущего уровня HMC.

Не требуется выполнять задачу **Сохранить данные модернизации**.

**Модернизация кода HMC**
Замена программного обеспечения HMC новым выпуском или уровнем исправления.

Требуется загрузка с носителя восстановления.

**Миграция кода HMC**
Перемещение данных HMC из одной версии HMC в другую.

Миграция является частным случаем модернизации.

**Прим.:** Для HMC модели 7063-CR1 можно подключить внешний привод DVD через USB.

## Определение версии и выпуска машинного кода HMC

Информация о том, как определить версию и выпуск машинного кода HMC.

### Об этой задаче

Набор доступных функций, включая оперативное обслуживание встроенного программного обеспечения сервера, а также расширения для модернизации до нового выпуска, определяется уровнем машинного кода HMC.

Для просмотра версии и выпуска машинного кода HMC выполните следующие действия:

### Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком **Информация о текущем драйвере HMC**, включая версию HMC, выпуск, уровень обслуживания, уровень компоновки и базовые версии.

## Получение и применение обновлений машинного кода для HMC через интернет-соединение

Знакомит с получением обновлений машинного кода для HMC при наличии соединения с Интернетом.

### Об этой задаче

Для получения обновлений машинного кода для HMC выполните все шаги.

### *Шаг 1. Убедитесь в наличии соединения с Интернетом*

### Об этой задаче

Для того чтобы загрузить в HMC или на сервер обновления из системы обслуживания и технической поддержки или с веб-сайта службы поддержки, требуется одно из следующих соединений:

- Соединение SSL с или без прокси-сервера SSL
- VPN через Интернет

Для того чтобы убедиться в наличии соединения с Интернетом, выполните следующее:

## Процедура

1. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
2. На панели содержимого выберите **Управление исходящими соединениями**.
3. Откройте вкладку, соответствующую типу исходящего соединения, выбранному для HMC (VPN или SSL-соединение через Интернет).

   **Прим.:** Если соединение со службой поддержки отсутствует, настройте его перед продолжением выполнения этого сценария. Инструкции по настройке соединения со службой поддержки приведены в разделе Настройка сервера для связи с сервисным центром IBM.
4. Нажмите кнопку **Проверить**.
5. Убедитесь, что проверка была успешно выполнена.

   Если проверка не была пройдена, устраните неполадку соединения перед продолжением выполнения этой процедуры. Кроме того, можно получить обновление на DVD.

   **Прим.:** Для HMC модели 7063-CR1 можно подключить внешний привод DVD через USB.
6. Перейдите к “Шаг 2. Просмотр текущего уровня машинного кода HMC” на стр. 79.

### *Шаг 2. Просмотр текущего уровня машинного кода HMC*

## Об этой задаче

Для просмотра текущего уровня машинного кода HMC выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере HMC, включая: версию HMC, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Перейдите к “Шаг 3. Просмотр доступных уровней машинного кода HMC” на стр. 79.

### *Шаг 3. Просмотр доступных уровней машинного кода HMC*

## Об этой задаче

Для просмотра доступных уровней машинного кода HMC выполните следующие действия:

## Процедура

1. С компьютера или сервера, подключенного к Интернету, перейдите на веб-сайт http://www.ibm.com/eserver/support/fixes.
2. Выберите нужное семейство серверов в списке Product.
3. Выберите **Hardware Management Console** в списке Product or fix type.
4. Нажмите кнопку **Продолжить**.

   Будет показан консоли аппаратного обеспечения.
5. Прокрутите список до нужного уровня версии HMC и для просмотра доступных уровней.

   **Прим.:** При необходимости обратитесь в службу поддержки.

6. Перейдите к “Шаг 4. Применение обновления машинного кода HMC” на стр. 80.

### *Шаг 4. Применение обновления машинного кода HMC*

#### Об этой задаче

Для применения обновления машинного кода HMC выполните следующие действия:

#### Процедура

1. Перед установкой обновлений для машинного кода HMC следует создать резервную копию важнейшей информации о консоли на HMC.

   Соответствующие инструкции приведены в разделе “Резервное копирование данных консоли управления” на стр. 76. Затем перейдите к следующему шагу.
2. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
3. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**. Откроется окно Установка исправления.
4. Следуйте инструкциям по установке обновления.
5. Для того чтобы обновления вступили в силу, завершите работу и перезапустите HMC.
6. Выберите **Войти и запустить веб-приложение Консоль аппаратного обеспечения**.
7. Войдите в интерфейс HMC.

### *Шаг 5.Проверка правильности установки обновления машинного кода HMC*

#### Об этой задаче

Для проверки установки обновления машинного кода HMC выполните следующие действия:

#### Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере HMC, включая: версию HMC, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
5. Если показана другая версия кода, выполните следующие действия:
   a. Выберите сетевое соединение в HMC.
   b. Повторно обновите встроенное программное обеспечение, используя другое хранилище.
   c. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

## Получение и применение обновлений машинного кода для HMC на DVD или через сервер FTP

Процедура получения обновлений машинного кода для консоли аппаратного обеспечения (HMC) с помощью DVD или сервера FTP.

## Об этой задаче

Для получения обновлений машинного кода HMC выполните все шаги.

**Прим.:** Для HMC модели 7063-CR1 можно подключить внешний привод DVD через USB.

### *Шаг 1. Просмотр текущего уровня машинного кода HMC*

## Прежде чем начать

Для просмотра текущего уровня машинного кода HMC выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере HMC, включая: версию HMC, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Перейдите к “Шаг 2. Просмотр доступных уровней машинного кода HMC” на стр. 81.

### *Шаг 2. Просмотр доступных уровней машинного кода HMC*

## Прежде чем начать

Для просмотра доступных уровней машинного кода HMC выполните следующие действия:

## Об этой задаче

## Процедура

1. На компьютере или сервере, подключенном к Интернету, откройте веб-сайт Fix Central.
2. Прокрутите список до нужного уровня версии HMC и для просмотра доступных уровней.

   **Прим.:** При необходимости обратитесь в службу поддержки IBM .
3. Перейдите к “Шаг 3. Получение обновления машинного кода HMC” на стр. 81.

### *Шаг 3. Получение обновления машинного кода HMC*

## Прежде чем начать

Для получения обновления машинного кода HMC выполните следующие действия:

## Об этой задаче

Обновление машинного кода HMC можно заказать на веб-сайте Центр доставки исправлений или в службе поддержки. Кроме того, его можно загрузить на сервер FTP.

**Заказ обновления машинного кода HMC через веб-сайт Центр доставки исправлений**

1. На компьютере или сервере, подключенном к Интернету, откройте веб-сайт Fix Central.
2. В продуктах, поддерживаемых HMC, выберите последний уровень HMC.
3. Прокрутите страницу вниз до области File names / Package area и найдите обновление, которое требуется заказать.
4. В столбце Заказ выберите **Перейти**.

5. Щелкните на ссылке **Continue** для получения идентификатора IBM.
6. Для того чтобы отправить заказ, следуйте инструкциям, появляющимся на экране.

**Загрузка обновления машинного кода HMC на съемные носители**

1. На компьютере или сервере, подключенном к Интернету, откройте веб-сайт Fix Central.
2. В продуктах, поддерживаемых HMC, выберите последний уровень HMC.
3. Прокрутите страницу вниз до области File names / Package area и найдите обновление, которое требуется загрузить.
4. Выберите обновление, которое требуется загрузить.
5. Примите условия лицензионного соглашения и сохраните обновление на съемном носителе.

## Дальнейшие действия

По окончании перейдите к “Шаг 4. Применение обновления машинного кода HMC” на стр. 82.

### *Шаг 4. Применение обновления машинного кода HMC*

## Прежде чем начать

Для применения обновления машинного кода HMC выполните следующие действия:

## Процедура

1. Перед установкой обновлений для машинного кода HMC создайте резервную копию данных HMC. За дополнительной информацией обратитесь к разделу “Резервное копирование данных консоли управления” на стр. 76.
2. Если вы получили или создали обновление на DVD-RAM, вставьте его в дисковод DVD на консоли HMC. Если вы получили или создали обновление на накопителе USB, то установите его.
3. Перед установкой обновлений для машинного кода HMC следует создать резервную копию важнейшей информации о консоли на HMC.

   Соответствующие инструкции приведены в разделе “Резервное копирование данных консоли управления” на стр. 76. Затем перейдите к следующему шагу.
4. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
5. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**. Откроется окно Установка исправления.
6. Следуйте инструкциям по установке обновления.
7. Для того чтобы обновления вступили в силу, завершите работу, перезапустите и вновь войдите на HMC.
8. Перейдите к “Шаг 5.Проверка правильности установки обновления машинного кода HMC” на стр. 82.

### *Шаг 5.Проверка правильности установки обновления машинного кода HMC*

## Прежде чем начать

Для проверки успешности установки обновления машинного кода HMC выполните следующие действия:

### Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере HMC, включая: версию HMC, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.
5. Если показана другая версия кода, выполните следующие действия:
   a. Повторно обновите машинный код. Если для выполнения этой процедуры был создан диск DVD, замените его.
   b. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

## Модернизация программного обеспечения HMC

Процедура модернизации программного обеспечения на HMC до следующего выпуска с сохранением данных конфигурации HMC.

### Об этой задаче

Для обновления машинного кода в HMC выполните все описанные шаги.

**Прим.:** Для HMC моделей 7063-CR1 и 7063-CR2 можно подключить внешний привод DVD через USB.

### *Шаг 1. Получение модернизации*

### Об этой задаче

Обновление машинного кода HMC можно заказать на веб-сайте Центр доставки исправлений.

Для того чтобы получить обновление с веб-сайта Центр доставки исправлений, выполните следующие действия:

### Процедура

1. На компьютере или сервере с доступом в Интернет откройте веб-страницу консоли аппаратного обеспечения http://www-933.ibm.com/support/fixcentral/.
2. Нажмите кнопку **Продолжить**.

   Будет показан консоли аппаратного обеспечения.
3. Найдите версию HMC, которую вы хотите обновить.
4. Найдите раздел загрузки и заказа.

   **Прим.:** Если доступа к Интернету нет, закажите обновление на DVD в службе сопровождения и поддержки IBM.
5. Для того чтобы отправить заказ, следуйте инструкциям, появляющимся на экране.
6. Получив обновление, перейдите к шагу “Шаг 2. Просмотр текущего уровня машинного кода HMC” на стр. 83.

### *Шаг 2. Просмотр текущего уровня машинного кода HMC*

### Об этой задаче

Для определения текущего уровня машинного кода HMC выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**. В области навигации выберите **Обновления**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере HMC, включая версию HMC, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Перейдите к “Шаг 3. Создание резервной копии данных профайла управляемой системы” на стр. 84.

### *Шаг 3. Создание резервной копии данных профайла управляемой системы*

## Об этой задаче

Для того чтобы скопировать данные профайлов управляемой системы, выполните следующие действия:

## Процедура

1. Выберите систему для сохранения данных профайла.
2. Выберите **Действия** > **Показать все действия** > **Устаревшие функции** > **Управление данными раздела** > **Создать резервную копию**.
3. Введите и запишите имя файла с резервной копией.
4. Нажмите кнопку **OK**.
5. Повторите эти действия для каждой системы.
6. Перейдите к “Шаг 4. Резервное копирование данных HMC” на стр. 84.

### *Шаг 4. Резервное копирование данных HMC*

## Об этой задаче

Перед установкой новой версии программного обеспечения HMC следует выполнить резервное копирование данных HMC; это позволит восстановить предыдущие версии программного обеспечения в случае ошибок в процессе модернизации ПО. После успешной установки новой версии программного обеспечения HMC сохраненную информацию применять не следует.

**Прим.:** Для сохранения данных консоли на съемном носителе необходимо предварительно подготовить соответствующий носитель.

Для резервного копирования особо важных данных HMC выполните следующие действия:

## Процедура

1. Если резервную копию предполагается создать на съемном носителе, отформатируйте носитель:
   a. Вставьте носитель в накопитель.
   b. В области навигации щелкните на значке **Обслуживание**  , затем выберите **Управление обслуживанием**.
   c. На панели содержимого выберите **Форматирование носителя**.
   d. Выберите тип носителя.
   e. Выберите тип форматирования.

f. Нажмите кнопку **OK**.

2. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
3. На панели содержимого выберите **Резервное копирование данных консоли управления**.

   Откроется окно **Создать резервную копию данных консоли управления**.
4. Выберите параметры архивации.

   Резервную копию можно сохранить на носителе в локальной системе, в удаленной системе, смонтированной в файловой системе HMC, например NFS, или отправить на удаленный сервер FTP.

   - Для создания резервной копии на носителе выберите **Сохранить на носителе в локальной системе** и следуйте показанным инструкциям.
   - Для создания резервной копии в смонтированной удаленной системе выберите **Сохранить в смонтированной удаленной системе** и следуйте показанным инструкциям.
   - Для создания резервной копии на сервере FTP выберите **Отправить резервную копию важнейших данных на удаленный сервер** и следуйте показанным инструкциям.
5. Перейдите к “Шаг 5. Запись информации о текущей конфигурации HMC” на стр. 85.

### *Шаг 5. Запись информации о текущей конфигурации HMC*

#### Об этой задаче

Перед обновлением версии программного обеспечения HMC в качестве меры предосторожности следует записать информацию о конфигурации HMC.

Для записи текущей конфигурации HMC выполните следующие действия:

#### Процедура

1. Выберите управляемую систему и разделы, для которых необходимо записать информацию конфигурации HMC.
2. В меню выберите **Действия** > **Запланированные операции**.

   Будут показаны все запланированные операции для выбранного целевого объекта.
3. Выберите **Сортировать** > **По объекту**.
4. Последовательно выберите каждый объект и запишите следующие сведения:

   - Имя объекта
   - Запланированная дата
   - Время выполнения (в 24-часовом формате)
   - Повторяющийся (если указано значение Да, выполните следующие действия):

     a. Выберите **Вид** > **Сведения о расписании**.

     b. Запишите информацию об интервале.

     c. Закройте окно запланированных операций.

     d. Повторите эти действия для каждой запланированной операции.
5. Закройте окно **Настроить запланированные операции**.
6. Перейдите к “Шаг 6. Запись состояния удаленной команды” на стр. 86.

### *Шаг 6. Запись состояния удаленной команды*

## Об этой задаче

Для записи состояния удаленной команды выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **Пользователи и защита**  , затем выберите **Защита систем и консоли**.
2. На панели содержимого выберите **Включить удаленное выполнение команд**.
3. Запишите состояния переключателя **Разрешить удаленное выполнение команд по протоколу ssh**.
4. Нажмите **Отмена**.
5. Перейдите к “Шаг 7. Сохранение данных модернизации” на стр. 86.

### *Шаг 7. Сохранение данных модернизации*

## Об этой задаче

Текущую конфигурацию HMC можно сохранить в выделенном разделе диска HMC или на локальном носителе. Данные об обновлении необходимо сохранять непосредственно перед переходом к следующему выпуску программного обеспечения HMC. Параметры конфигурации HMC можно восстановить после обновления.

**Прим.:** Сохранить можно только одну резервную копию. Каждый раз при сохранении данных обновления предыдущие данные удаляются.

Для того чтобы сохранить данные обновления, выполните следующие действия:

## Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Сохранить данные обновления**. Откроется мастер **Сохранить данные обновления**.
3. Выберите носитель для сохранения данных обновления. Если выбран съемный носитель, то установите его. Нажмите кнопку **Далее**.
4. Нажмите кнопку **Закончить**.
5. Дождитесь завершения задачи.

   Если задача Сохранить данные обновления не будет выполнена, обратитесь на следующий уровень поддержки.

   **Прим.:** Если задача сохранения данных обновления не будет выполнена, процесс обновления следует приостановить.
6. Нажмите кнопку **OK**.
7. Перейдите к “Шаг 8. Модернизация программного обеспечения HMC” на стр. 87.

### *Шаг 8. Модернизация программного обеспечения HMC*

#### Об этой задаче

Для модернизации программного обеспечения HMC перезапустите систему, установив в дисковод DVD съемный носитель.

#### Процедура

1. Вставьте установочный диск продукта HMC в дисковод DVD.
2. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
3. На панели содержимого выберите **Выключение или перезапуск консоли управления**.
4. Проследите за тем, чтобы был выбран пункт **Перезапустить HMC**.
5. Нажмите кнопку **OK**.

   В ходе перезапуска HMC в окне прокручивается системная информация.
6. Выберите **Обновить** и нажмите кнопку **Далее**.
7. Выберите один из вариантов:
   - Если данные обновления были сохранены при выполнении предыдущей задачи, перейдите к следующему шагу.
   - Если данные обновления не были сохранены, перед продолжением их следует сохранить.
8. Выберите **Обновить с носителя** и нажмите кнопку **Далее**.
9. Подтвердите параметры и нажмите кнопку **Готово**.
10. Следуйте инструкциям.

    **Прим.:**
    - Если экран станет пустым, для просмотра информации нажмите пробел.
    - Установка первого DVD может занять приблизительно 20 минут.
11. В приглашении входа в систему введите ИД пользователя и пароль.

    Установка кода HMC завершена.
12. Перейдите к “Шаг 9. Проверка правильности установки модернизации машинного кода HMC” на стр. 87.

### *Шаг 9. Проверка правильности установки модернизации машинного кода HMC*

#### Об этой задаче

Для проверки успешности установки обновления HMC выполните следующие действия:

#### Процедура

1. В области навигации щелкните на значке **HMC Управление**  и выберите **Управление консолью**.
2. На панели содержимого выберите **Обновить консоль аппаратного обеспечения**.
3. В новом окне просмотрите и запишите информацию, приведенную под заголовком Информация о текущем драйвере HMC, включая версию HMC, выпуск, уровень обслуживания, уровень компоновки и базовые версии.
4. Убедитесь, что версия и выпуск совпадают с версией установленного обновления.

5. Если показана другая версия кода, повторите операцию с другим диском DVD. Если ошибка возникнет снова, обратитесь на следующий уровень поддержки.

## Обновление HMC из удаленного расположения с помощью образов сетевого обновления

Инструкции по обновлению программного обеспечения HMC из удаленного расположения с помощью образов сетевого обновления.

### Об этой задаче

Инструкции по обновлению программного обеспечения HMC из удаленного расположения с помощью образов сетевого обновления.

### Процедура

1. С компьютера или сервера, подключенного к Интернету, перейдите на веб-сайт загрузок и поддержки консоли аппаратного обеспечения (http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html).
2. Загрузите подходящие сетевые образы HMC 9 и сохраните их на сервере FTP.

   Эти файлы нельзя загрузить непосредственно в HMC. Файлы образов необходимо загрузить на сервер, принимающий запросы FTP.
3. Загрузите следующие файлы:
   - img2a
   - img3a
   - base.img
   - disk1.img
   - hmcnetworkfiles.sum
4. Сохраните данные обновления в HMC. Выполните следующие команды для сохранения данных обновления:
   - Для сохранения данных на диске DVD и жестком диске выполните следующие команды:

     **mount /media/cdrom**

     **saveupgdata -r diskdvd**
   - Для сохранения данных на жестком диске выполните следующую команду:

     **saveupgdata -r disk**
5. Скопируйте файлы обновления в загрузочный раздел диска HMC. Выполните команду **getupgfiles** для копирования файлов.

   Пример: **getupgfiles -h <сервер-ftp> -u <ИД-пользователя> -d <удаленный-каталог>**

   Где,
   - **сервер-ftp** - это имя хоста или IP-адрес сервера FTP, содержащий сетевые образы HMC.
   - **ИД-пользователя** - это допустимый ИД пользователя на сервере FTP. Если пароль не указан в аргументе `--passwd`, то он будет запрошен.
   - **удаленный-каталог** - это каталог на сервере FTP, в котором сохранены сетевые образы HMC.
6. Перезапустите HMC, чтобы обновить код, скопированный в раздел загрузочного диска. Выполните команду **chhmc -c altdiskboot -s enable --mode upgrade** для перезапуска HMC.
7. Перезапустите HMC и начните обновление. Выполните команду **hmcshutdown -r -t now** для запуска процедуры обновления.

# Обеспечение безопасности HMC

Узнайте о том, как обеспечить безопасность консоли аппаратного обеспечения (HMC) в соответствии с корпоративными стандартами безопасности.

Стандартная конфигурация HMC обеспечивает достаточно высокий уровень безопасности для большинства корпоративных пользователей. В HMC версии 8.4.0 и выше существует возможность дополнительно усилить безопасность, чтобы она соответствовала корпоративным стандартам. Для усиления безопасности HMC настройте уровень безопасности не ниже 1. В зависимости от конфигурации среды и предъявляемых в компании требований к безопасности можно выбрать уровень 2 или 3.

**Прим.:** Перед изменением уровня безопасности проконсультируйтесь у специалистов по безопасности в вашей компании.

## Безопасность уровня 1

Для обеспечения безопасности HMC на уровне 1 выполните следующие действия:

1. Измените предустановленный пароль стандартного пользователя `hscroot`. За дополнительной информацией о стратегии управления паролями обратитесь к разделу “Улучшенная стратегия управления паролями” на стр. 91.
2. Если HMC не находится в физически защищенном помещении, установите пароль `grub` с помощью следующей команды: `chhmc -c grubpasswd -s enable --passwd <новый пароль grub>`
3. Если в HMC настроен Integrated Management Module (IMM), настройте надежный пароль IMM.
4. Задайте надежный пароль для пользователя *admin* и других пользователей на всех серверах.
5. Установите последние исправления безопасности в HMC. Дополнительные сведения об исправлениях безопасности опубликованы на сайте IBM Fix Central.

## Безопасность уровня 2

При наличии нескольких пользователей безопасность HMC можно усилить путем выполнения следующих действий:

1. Создайте учетную запись для каждого пользователя в HMC и назначьте ей необходимые роли и ресурсы. За дополнительной информацией о предусмотренных в HMC ролях обратитесь к разделу Задачи HMC, роли и идентификаторы пользователей и связанные команды.

   **Прим.:** Создаваемым в HMC пользователям следует назначать минимально необходимый набор ролей и ресурсов. При необходимости можно создать нестандартные роли.
2. Включите репликацию данных о пользователях между консолями аппаратного обеспечения. Репликация данных о пользователях может выполняться в режиме главный-подчиненный или режиме равноправных узлов. За дополнительной информацией о репликации данных о пользователях обратитесь к разделу Управление репликацией данных.
3. Импортируйте сертификат, подписанный сертификатной компанией.

## Безопасность уровня 3

При наличии нескольких консолей аппаратного обеспечения и системных администраторов безопасность HMC можно усилить путем выполнения следующих действий:

1. Используйте централизованную идентификацию, например с помощью LDAP или Kerberos. За дополнительной информацией о настройке LDAP обратитесь к документу Как настроить LDAP в HMC.
2. Включите репликацию данных о пользователях между консолями аппаратного обеспечения.
3. Убедитесь в том, что HMC работает в режиме совместимости с NIST SP 800-131A, то есть применяет только надежные шифры.

4. Заблокируйте ненужные порты на брандмауэре. Информация о доступных для использования портах HMC приведена в следующей таблице:

*Таблица 32. Порты, применяемые пользователями для взаимодействия с HMC*

| Порт | Описание | Тип | Версия протокола (режим по умолчанию) | Версия протокола (режим NIST) |
|---|---|---|---|---|
| 22 | Open SSH | TCP | SSH v3 | SSH v3 |
| 123 | NTP | UDP | NTP | NTP |
| 161 | SNMP Agent | UDP | SNMP v3 | SNMP v3 |
| 162 | SNMP Trap | UDP | SNMP v3 | SNMP v3 |
| 427 | SLP | UDP | нд | нд |
| 443 | GUI HMC и REST API | TCP | HTTPS (TLS 1.2) | HTTPS (TLS 1.2) |
| 657 | RMC | TCP/UDP | RSCT (открытый текст с хэшем и подписью) | RSCT (открытый текст с хэшем и подписью) |
| 2300 | Терминал 5250 для IBM i | TCP | Открытый текст | Открытый текст |
| 2301 | Безопасный терминал 5250 для IBM i | TCP | TLS 1.2 | TLS 1.2 |
| 5989 | CIM (устаревший порт, не работает) | TCP | Не работает | Не работает |
| 9900 | FCS: поиск HMC-HMC | UDP | FCS | FCS |
| 9920 | FCS: связь HMC-HMC | TCP | HTTPS (TLS 1.2) | HTTPS (TLS 1.2) |
| 9960 | Аплет VTerm в GUI | TCP | HTTPS (TLS 1.2) | HTTPS (TLS 1.2) |
| 12443 | HMC REST API (старый порт) | TCP | HTTPS (TLS 1.2) | HTTPS (TLS 1.2) |
| 12347 | Равноправный домен RSCT | UDP | RSCT (открытый текст с хэшем и подписью) | RSCT (открытый текст с хэшем и подписью) |
| 12348 | Равноправный домен RSCT | UDP | RSCT (открытый текст с хэшем и подписью) | RSCT (открытый текст с хэшем и подписью) |

**Примечания:**

- Необходимо использовать только SSH (порт 22), HTTPS (порт 443 и порт 12443), безопасный терминал 5250 для IBM i (порт 2301) и VTerm (порт 9960) - эти порты должны быть открыты в интранете. Все остальные порты должны использоваться в частной или изолированной сети. Дополнительно можно использовать отдельный порт Ethernet и VLAN для подсистемы

контроля и управления ресурсами (RMC) (порт 657), FCS (порты 9900 и 9920), а также равноправного домена RSCT (порты 12347 и 12348).

- Порты, перечисленные в команде **netstat**, используются только для внутренних процессов.

## Улучшенная стратегия управления паролями

В Консоль аппаратного обеспечения (HMC) можно задать требования к паролям локальных пользователей. Улучшенная стратегия управления паролями позволяет системному администратору задать ограничения на пароли. Эта стратегия действует для всех систем, в которых установлена программа HMC.

Системные администраторы могут использовать улучшенную стратегию управления паролями, чтобы задать единую стратегию для всех пользователей. HMC поддерживает стратегию управления паролями, обеспечивающую средний уровень безопасности, активировав которую системный администратор может настроить ограничения на пароли. Вместо стандартной стратегии со средним уровнем безопасности системный администратор может активировать другую пользовательскую стратегию. Стратегию управления паролями со средним уровнем безопасности, предоставляемую программой HMC, нельзя удалить из системы. В следующей таблице указаны применяемые по умолчанию значения атрибутов стратегии управления паролями со средним уровнем безопасности.

*Таблица 33. Атрибуты стратегии управления паролями со средним уровнем безопасности из программы HMC*

| Атрибут | Описание | Значение по умолчанию |
|---|---|---|
| min_pwage | Минимальное число дней, в течение которых пароль должен оставаться активным. | 1 |
| pwage | Максимальное число дней, в течение которых пароль может оставаться активным. | 180 |
| min_length | Минимальная длина пароля. | 8 |
| hist_size | Число предыдущих паролей, которые нельзя повторять. | 10 |
| warn_pwage | Число дней до истечения срока действия пароля, за которое пользователю отправляется предупреждение. | 7 |
| min_digits | Минимальное число цифр в пароле. | Нет |
| min_uppercase | Минимальное число прописных букв. | 1 |
| min_lowercase | Минимальное число строчных букв. | 6 |
| min_special_chars | Минимальное число специальных символов, которое должно быть использовано в пароле. | Нет |

Обратите внимание на следующие особенности стратегии управления паролями со средним уровнем безопасности программы HMC:

- Эта стратегия не действует для пользователей **hscroot**, **hscpe** и **root**.
- Эта стратегия действует только для локальных пользователей, которыми управляет HMC, и ее область действия нельзя распространить на пользователей LDAP или Kerberos.
- Системный администратор может настроить ограничения на повторное использование паролей как в стратегии управления паролями со средним уровнем безопасности, предоставляемой программой HMC, так и в пользовательской стратегии.
- Предоставляемая программой HMC стратегия управления паролями со средним уровнем безопасности доступна только для чтения, и ее атрибуты нельзя изменить. При необходимости

можно создать пользовательскую стратегию управления паролями и задать в ней другие ограничения на пароли.

Для работы со стратегией управления паролями со средним уровнем безопасности, предоставляемой программой HMC, можно использовать следующие команды:

**mkpwdpolicy**
Импортирует стратегию управления паролями из файла, содержащего все параметры, или создает новую стратегию.

**lspwdpolicy**
Показывает все доступные профайлы стратегий управления паролями и выполняет поиск по заданным параметрам. Кроме того, позволяет просмотреть ту стратегию, которая сейчас активна.

**rmpwdpolicy**
Удаляет неактивную стратегию управления паролями.

**Прим.:** Активную стратегию со средним уровнем безопасности и применяемую по умолчанию стратегию управления паролями, которая доступна только для чтения, удалить нельзя.

**chpwdpolicy**
Изменяет параметры неактивной стратегии управления паролями.

# Профили безопасности: Общеевропейский регламент о защите персональных данных (GDPR) и Стандарт безопасности данных в сфере платежных карт (PCI-DSS)

Узнайте о том, каким образом консоль аппаратного обеспечения (HMC) обрабатывает персональные данные пользователей.

Консоль аппаратного обеспечения (HMC) представляет собой закрытую систему, в которой не хранятся никакие данные о держателях платежных карт. Таким образом, к HMC применима только часть требований и процедур оценки ИТ-безопасности, которые определены в стандарте PCI-DSS. В HMC может устанавливаться только безопасный код, распространяемый компанией IBM. При обнаружении любой уязвимости через процесс IBM PSIRT выпускаются временные исправления. Требования и рекомендации включают в себя следующее:

## Вопросы относительно GDPR

*Таблица 34. Вопросы относительно GDPR .* В следующей таблице приведены ответы на вопросы, имеющие отношение к GDPR.

| **Вопросы** | **Ответы** |
|---|---|
| Какие данные хранятся в HMC? | В HMC хранится информация о конфигурации систем Power и виртуальных сред PowerVM, а также характеристики производительности. |
| Обрабатывает ли HMC какие-либо персональные данные? | По желанию можно указать свои контактные данные для функции вызова сервисного центра. Предоставлять контактные данные необязательно. |
| Какие предопределенные учетные записи администраторов системы предусмотрены в HMC? | Администратор системы использует имя пользователя *hscroot*. |
| Связаны ли какие-либо учетные записи в HMC с конкретным человеком? | Нет. |
| Обязательно ли указывать свои персональные данные в HMC? | Нет. Предоставлять персональные данные необязательно. Однако это можно сделать. |

| *Таблица 34. Вопросы относительно GDPR .* В следующей таблице приведены ответы на вопросы, имеющие отношение к GDPR. *(продолжение)* | |
|---|---|
| **Вопросы** | **Ответы** |
| Сохраняются ли какие-либо персональные данные в файле протокола HMC? | Нет. |
| Можно ли полностью и необратимо удалить персональные данные? | Да. Для этого необходимо удалить конфигурацию функции вызова сервисного центра. |

## Вопросы относительно PCI-DSS

| *Таблица 35. Вопросы относительно PCI-DSS .* В следующей таблице приведены ответы на вопросы, имеющие отношение к PCI-DSS. | |
|---|---|
| **Вопросы** | **Ответы** |
| Каким образом настроить брандмауэр для защиты данных о держателе карты? | В HMC не хранятся и не используются никакие данные о держателях карт. Однако в HMC предусмотрена возможность настройки брандмауэра, с помощью которого пользователь может закрывать и открывать отдельные порты. |
| Можно ли использовать установленные вендором значения по умолчанию для паролей к системе и других параметров безопасности? | Перед подключением системы к сети необходимо изменить все предустановленные пароли пользователя *hscroot*. |
| Каким образом в HMC обеспечивается защита сохраненных данных о держателе карты? | В HMC не хранятся и не используются никакие данные о держателях карт. |
| Каким образом HMC зашифровывает данные о держателе карты во время их передачи по незащищенным общедоступным сетям? | В HMC не хранятся и не используются никакие данные о держателях карт. |
| Каким образом можно использовать и регулярно обновлять антивирусные программы? | HMC представляет собой закрытую систему. Это значит, что в нее не могут проникнуть вредоносные программы. |
| Каким образом можно обеспечить безопасность систем и приложений во время разработки и использования? | Исправления необходимо загружать с веб-сайта IBM Fix Central и устанавливать их вручную. В HMC может устанавливаться только безопасный код, распространяемый компанией IBM. |
| Ограничивает ли HMC доступ к данным о держателе карты? | В HMC не хранятся и не используются никакие данные о держателях карт. |
| Каким образом присвоить уникальный ИД каждому пользователю, имеющему доступ к компьютеру? | Для соблюдения этого требования необходимо проследить за тем, чтобы никакие идентификаторы не использовались совместно несколькими пользователями, а также соблюдать стратегии управления паролями. |
| Каким образом ограничить физический доступ к данным о держателе карты? | В HMC не хранятся и не используются никакие данные о держателях карт. |
| Каким образом можно отслеживать доступ к сетевым ресурсам и данным о держателе карты? | В HMC не хранятся и не используются никакие данные о держателях карт. |

| *Таблица 35. Вопросы относительно PCI-DSS .* В следующей таблице приведены ответы на вопросы, имеющие отношение к PCI-DSS. *(продолжение)* | |
|---|---|
| **Вопросы** | **Ответы** |
| Каким образом в HMC проверяется безопасность системы и процессов? | Все выпущенные версии HMC проверяются на безопасность с помощью инструментов сканирования. Применяются следующие инструменты сканирования: *Qualys*, *Nessus*, *testssl*, *sslscan* и *ASoC*. |
| Каким образом реализовать политику безопасности, предусматривающую защиту информации от сотрудников и подрядчиков? | Системный администратор должен деактивировать вход в систему для удаленных пользователей, активировать учетные записи пользователей по мере необходимости и деактивировать учетные записи пользователей, которым больше не нужен доступ. |

# Решение распространенных проблем с безопасностью HMC

Здесь описаны способы решения распространенных проблем, которые возникают при обеспечении безопасности HMC.

## Как обеспечить безопасность соединения между консолью аппаратного обеспечения (HMC) и системой?

Для подключения к системе HMC использует Flexible Service Processor (FSP). FSP и гипервизор Power взаимодействуют под управлением двоичного протокола Network Client (NETC), который является нашей собственной разработкой. Порты, которые применяются HMC, указаны в следующей таблице:

| *Таблица 36. Порты FSP, используемые для взаимодействия с HMC* | | | |
|---|---|---|---|
| **Порты FSP** | **Описание** | **Версия протокола (режим по умолчанию)** | **Версия протокола (режим NIST)** |
| 443 | Расширенный интерфейс управления системой | HTTPS (TLS 1.2) | HTTPS (TLS 1.2) |
| 30000 | NETC | NETC (TLS 1.2). С возможностью понижения до SSLv3 для поддержки старого встроенного ПО. | NETC (TLS 1.2) |
| 30001 | VTerm | NETC (TLS 1.2). С возможностью понижения до SSLv3 для поддержки старого встроенного ПО. | NETC (TLS 1.2) |

## Как заблокировать доступ к HMC?

Для большей безопасности можно использовать устройство с системой предотвращения вторжений (IPS) или поместить все консоли аппаратного обеспечения и серверы IBM Power Systems за брандмауэр. Кроме того, если консоль HMC никогда не используется удаленно, либо ее

необходимо полностью заблокировать, в ней можно деактивировать все сетевые службы. Для деактивации сетевых служб в HMC выполните следующие действия:

1. Отключите удаленное выполнение команд через порт SSH.
2. Отключите удаленный виртуальный терминал (порт VTerm).
3. Отключите удаленный доступ через Интернет (графический пользовательский интерфейс HMC и REST API).
4. Заблокируйте порты на брандмауэре, узнав настроенные порты Ethernet в параметрах сети HMC.

## Как включить режим совместимости с NIST SP 800-131A в HMC?

В HMC версии 8.1.0 и выше поддерживается режим совместимости, в котором разрешается использовать только очень надежные методы шифрования, указанные в документе NIST SP 800-131A. При этом вы можете потерять возможность подключаться к старым серверам Power Systems, например серверам POWER5, не поддерживающим протокол Transport Layer Security (TLS 1.2). За дополнительной информацией об изменении режима обеспечения безопасности обратитесь к документу Режим NIST в HMV V8R8.

## Как просмотреть и изменить шифры, используемые HMC?

В HMC версии 8.1.0 и выше поддерживаются более безопасные комплекты шифров, чем указанные в документе NIST 800-131A. Применяемые по умолчанию шифры являются достаточно надежными. Для того чтобы узнать, какие шифры использует HMC, введите команду **lshmcencr**. Если согласно внутреннему регламенту вашей компании должен использоваться другой комплект шифров, то измените шифры с помощью команды **chhmcencr**.

Для того чтобы узнать, какие шифры используются HMC для шифрования паролей, вызовите следующую команду:

```
lshmcencr -c passwd -t c
```

Для того чтобы узнать, какие шифры используются в веб-интерфейсе HMC и REST API, вызовите следующую команду:

```
lshmcencr -c webui -t c
```

Для того чтобы узнать, какие шифры и алгоритм MAC используются в интерфейсе SSH консоли HMC, вызовите следующую команду:

```
lshmcencr -c ssh -t c
```

```
lshmcencr -c sshmac -t c
```

## Как проверить надежность сертификата HMC?

Применяемые в HMC самоподписанные сертификаты используют шифрование SHA256 с 2048-разрядным ключом RSA, которое является достаточно надежным. Если вы решите использовать сертификаты, подписанные сертификатной компанией (CA), следует убедиться в том, что в них не используется шифрование с 1024-разрядным ключом, которое является слабым. В HMC можно использовать следующие сертификаты:

- Для графического пользовательского интерфейса HMC и REST API (портов 443 и 12443) можно использовать сертификат, подписанный сертификатной компанией.
- Порт 9920 используется для связи между HMC. Его сертификат нельзя заменить на выбранный вами сертификат.

## Что стоит выбрать: самоподписанный сертификат (стандартный) или сертификат, подписанный CA?

HMC автоматически генерирует сертификат во время установки. При необходимости в HMC можно сгенерировать запрос на подписание сертификата для получения нового сертификата, выданного сертификатной компанией. Этот сертификат можно импортировать в HMC. В дополнение к нему необходимо получать доменное имя для HMC. За дополнительной информацией о сертификатах в HMC обратитесь к разделу Управление сертификатами.

## Как контролировать использование HMC?

Средства контроля консоли аппаратного обеспечения главным образом отслеживают настроенные шифры и операции различных пользователей HMC. Для просмотра операций различных пользователей HMC можно использовать следующие команды:

*Таблица 37. Применяемые в HMC шифры*

| **Предназначение** | **Команда** |
|---|---|
| Шифрование паролей (глобальный параметр) | `lshmcencr -c passwd -t c` |
| Шифрование пароля каждого пользователя | `lshmcusr -Fname:password_encryption` |
| Шифры SSH | `lshmcencr -c ssh -t c` |
| SSH MAC | `lshmcencr -c sshmac -t c` |
| Шифры, применяемые в графическом пользовательском интерфейсе HMC и REST API | `lshmcencr -c webui -t c` |

Для мониторинга различных событий консоли и обслуживаемых событий, возникающих при использовании HMC, предназначены следующие команды:

*Таблица 38. Команды для просмотра активных пользователей, а также событий консоли и обслуживаемых событий в HMC*

| **Информация** | **Команда** |
|---|---|
| Пользователи GUI | `lslogon –r webui –u` |
| Задачи GUI | `lslogon –r webui –t` |
| Пользователи CLI | `lslogon –r ssh –u` |
| Задачи CLI | `lslogon –r ssh –t` |
| Операции в HMC | `lssvcevents -t console -d <кол-во дней>` |
| Операции в системе | `lssvcevents –t hardware –m <управляемая система> -d <кол-во дней>` |

**Централизованный мониторинг событий HMC**: при наличии большого количества консолей аппаратного обеспечения можно собирать всю информацию об их использовании в файл `rsyslog`.

## Каким образом IBM устраняет уязвимости HMC?

В IBM реализован процесс реагирования на инциденты безопасности, который называется IBM Product Security Incident Response Team (PSIRT). IBM Product Security Incident Response Team (PSIRT) - это международный коллектив специалистов, отвечающих за получение, анализ и внутреннюю координацию обработки информации об уязвимостях безопасности в предложениях IBM. Поставляемые в составе HMC компоненты с открытым исходным кодом и разработанные IBM

компоненты оперативно проверяются и анализируются. Для всех поддерживаемых выпусков HMC компания IBM выпускает временные исправления и исправления безопасности.

### Как узнавать о появлении новых временных исправлений HMC?

Информация об уязвимостях и временных исправлениях поддерживаемых версий HMC распространяется в виде бюллетеня безопасности. Для того чтобы оперативно узнавать о временных исправлениях HMC, можно:

- Регулярно знакомиться с последними бюллетенями безопасности, выполняя их поиск в блоге IBM Security Bulletin.
- Подписаться на канал @IBMPowereSupp в Twitter и следить за публикуемыми в нем уведомлениями.
- Подписаться на почтовую рассылку на веб-сайте IBM Support.

## Расположения портов HMC

Расположения портов можно найти с помощью кодов расположений. Диаграммы расположений портов HMC помогают сопоставить код расположения с положением порта HMC на сервере.

### Расположение портов HMC в модели 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H и 9223-22S

С помощью этой диаграммы и таблицы можно найти порты HMC в системе 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H и 9223-22S.

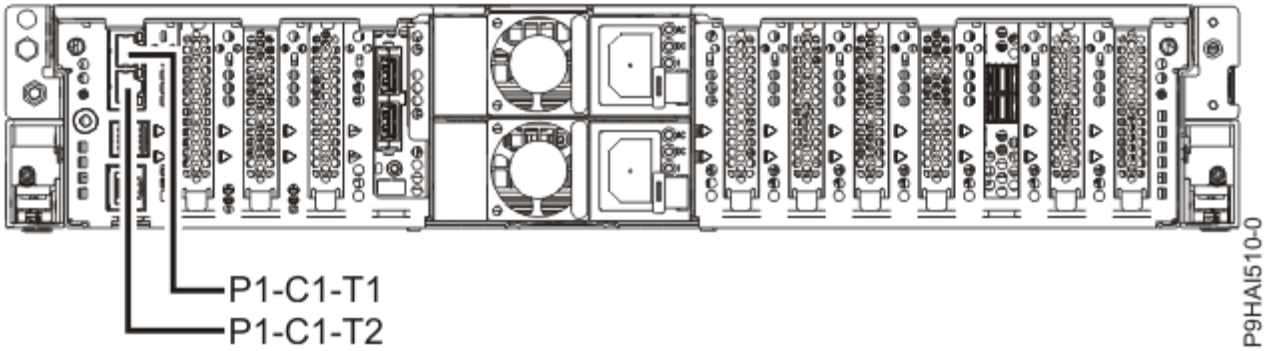



*Рисунок 10. Расположения портов HMC 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H и 9223-22S*

*Таблица 39. Расположения портов HMC 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H и 9223-22S*

| Порт | Код физического расположения | Индикатор идентификации |
|---|---|---|
| Порт HMC 1 | Un-P1-C1-T1 | Нет |
| Порт HMC 2 | Un-P1-C1-T2 | Нет |
| Дополнительная информация о расположении портов HMC в 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H или 9223-22S приведена в разделе Расположение компонентов и коды расположения для 9008-22L, 9009-22A, 9009-22G, 9223-22H и 9223-22S. | | |

## Расположение портов HMC в модели 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H и 9223-42S

С помощью этой диаграммы и таблицы можно найти порты HMC в системе 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H и 9223-42S.

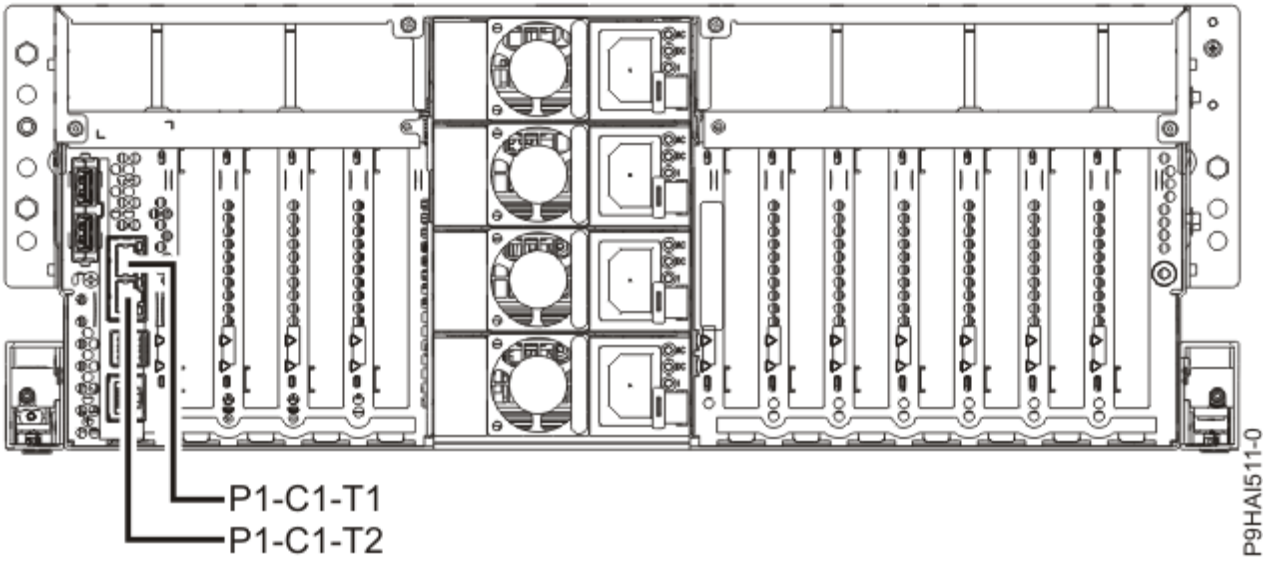



*Рисунок 11. Расположения портов HMC 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H и 9223-42S*

*Таблица 40. Расположения портов HMC 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H и 9223-42S*

| **Порт** | **Код физического расположения** | **Индикатор идентификации** |
|---|---|---|
| Порт HMC 1 | Un-P1-C1-T1 | Нет |
| Порт HMC 2 | Un-P1-C1-T2 | Нет |
| Дополнительная информация о расположении портов HMC в 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H или 9223-42S приведена в разделе Расположение компонентов и коды расположения для 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H и 9223-42S. | | |

## Расположения портов HMC в моделях 9040-MR9

С помощью этой диаграммы и таблицы можно найти порты HMC в системе 9040-MR9.

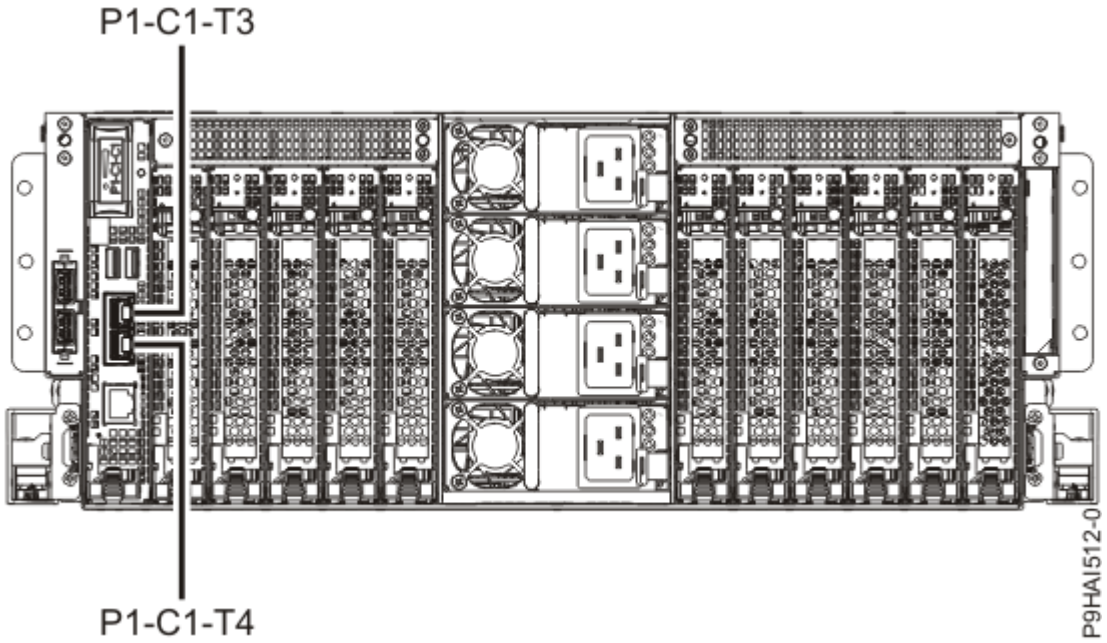



*Рисунок 12. Расположения портов HMC 9040-MR9*

| *Таблица 41. Расположения портов HMC 9040-MR9* | | |
|---|---|---|
| **Порт** | **Код физического расположения** | **Индикатор идентификации** |
| Порт HMC 1 | Un-P1-C1-T3 | Нет |
| Порт HMC 2 | Un-P1-C1-T4 | Нет |
| Дополнительная информация о расположении портов HMC в системах 9040-MR9 приведена в разделе Расположение компонентов и коды расположения. | | |

## Расположения портов HMC в моделях 9080-M9S

С помощью этой диаграммы и таблицы можно найти порты HMC в системе 9080-M9S.

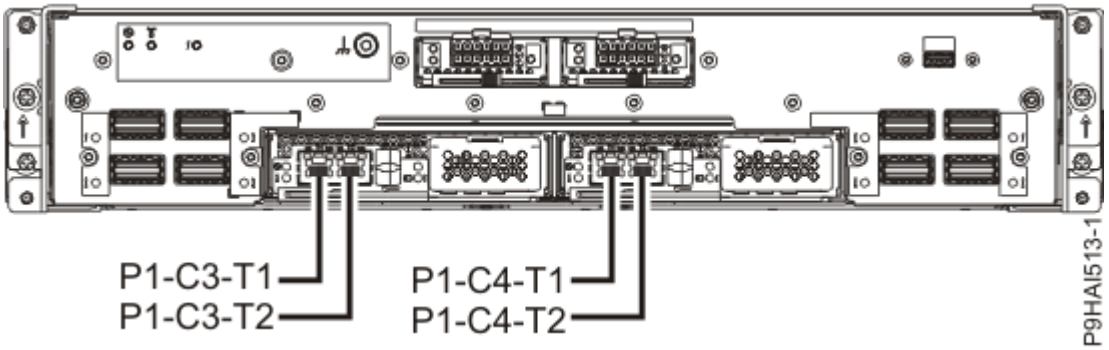



*Рисунок 13. Расположения портов HMC 9080-M9S*

| *Таблица 42. Расположения портов HMC 9080-M9S* | | |
|---|---|---|
| **Порт** | **Физическое расположение порта** | **Индикатор идентификации** |
| Карта служебного процессора 1 - порт HMC 1 | Un-P1-C3-T1 | Нет |

| *Таблица 42. Расположения портов HMC 9080-M9S (продолжение)* | | |
|---|---|---|
| **Порт** | **Физическое расположение порта** | **Индикатор идентификации** |
| Карта служебного процессора 1 - порт HMC 2 | Un-P1-C3-T2 | Нет |
| Карта служебного процессора 2 - порт HMC 1 | Un-P1-C4-T1 | Нет |
| Карта служебного процессора 2 - порт HMC 2 | Un-P1-C4-T2 | Нет |
| Дополнительная информация о расположении портов HMC в системах 9080-M9S приведена в разделе Расположение компонентов и коды расположения. | | |

# Замечания

Эта информация касается продуктов и услуг, предлагаемых в США.

IBM не имеет права предоставлять продукты, услуги или возможности, описанные в данном документе, в других странах. Обратитесь к местному представителю IBM за информацией о продуктах и услугах, доступных в вашем регионе на данный момент. Любые отсылки к продукту, программе или услуге IBM не означают и не подразумевают под собой, что может использоваться только этот продукт, эта программа или эта услуга IBM. Вместо них можно использовать любые функционально эквивалентные продукты, программы или услуги, которые не нарушают прав IBM на интеллектуальную собственность. Однако на пользователе лежит ответственность за оценку и проверку работы любых продуктов, программ или услуг, предоставляемых не со стороны IBM.

IBM может обладать патентами или представленными на рассмотрение заявками на патенты, которые относятся к предмету данного документа. Предоставление данного документа не дает вам никакой лицензии на эти патенты. Заявки на получение лицензии можно отправлять по указанному ниже адресу:

*IBM Director of Licensing*
*IBM Corporation*
*North Castle Drive, MD-NC119*
*Armonk, NY 10504-1785*
*US*

INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ) ПРЕДПОЛАГАЕМЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ АВТОРСКИХ ПРАВ, РЫНОЧНОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ. В некоторых странах для ряда сделок не допускается отказ от явных или предполагаемых гарантий; в таком случае данное положение к вам не относится.

В данной публикации могут встретиться технические неточности и типографские опечатки. В приведенную информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления вносить улучшения и изменения в продукты и программы, описанные в настоящей публикации.

Любые ссылки в этой публикации на веб-сайты других фирм предоставлены только для удобства и не служат никоим образом в качестве поддержки этих веб-сайтов. Материалы, размещенные на этих веб-сайтах, не являются частью материалов для настоящего продукта IBM и ответственность за их применение лежит на пользователе.

IBM оставляет за собой право использовать или распространять любую предоставленную вами информацию любым способом по своему усмотрению без каких-либо обязательств перед вами.

Данные о производительности и примеры клиентов приведены исключительно иллюстративных целях. Фактические показатели производительности могут отличаться в зависимости от конкретной конфигурации и условий эксплуатации.

Информация о продуктах, выпущенных сторонними компаниями, была получена от поставщиков этих продуктов, из опубликованных документах или других общедоступных источников. IBM не тестировала подобные продукты и не может подтвердить точность сведений о производительности, совместимости и других заявленных характеристиках. Вопросы о функциях продуктов других фирм должны быть направлены поставщикам этих продуктов.

Заявления о будущих действиях или намерениях IBM могут быть изменены или аннулированы без предупреждения и должны рассматриваться исключительно как заявления о предполагаемых целях.

Все указанные цены являются рекомендуемыми розничными ценами IBM, эти цены текущие и могут быть изменены без соответствующего уведомления. Цены поставщиков могут он них отличаться.

Данная информация предназначена исключительно для целей планирования. Она может быть изменена до того, как будут выпущены описанные в ней продукты.

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для большего правдоподобия эти примеры снабжены именами и фамилиями, названиями фирм, торговых марок и продуктов. Все эти имена являются вымышленными и любое сходство с настоящими лицами или предприятиями полностью случайно.

В электронной версии настоящей информации могут отсутствовать фотографии и цветные изображения.

Запрещается полностью или частично воспроизводить содержащиеся в этом документе рисунки и спецификации без письменного разрешения IBM.

Эта информация подготовлена IBM для использования с указанными компьютерами. IBM не утверждает, что данная публикация пригодна для каких-либо иных целей.

Компьютерные системы IBM содержат механизмы, разработанные для снижения вероятности невыявленного повреждения или потери данных. Однако этот риск не может быть исключен полностью. Пользователи, сталкивающиеся с незапланированными остановками, неполадками систем, нестабильностью или отключениями питания или отказами компонентов, должны убеждаться в надежности выполняемых операций и сохранения или передачи данных системой во время или перед отключением или отказом. Кроме того, пользователи должны учредить процедуры по обеспечению независимой проверки данных перед применением к этим данным критичных или сомнительных операций. Пользователям следует регулярно заходить на веб-сайты поддержки IBM изготовителя получения обновленной информации или исправлений, относящихся к системе и связанному программному обеспечению.

### Заявление о сертификации

Этот продукт может быть не сертифицирован в вашей стране для подключения любыми средствами к интерфейсам общедоступных телекоммуникационных сетей. Может потребоваться дополнительная сертификация перед установкой такого подключения. Обратитесь к представителю IBM или посреднику по любым вопросам.

## Специальные возможности серверов IBM Power Systems

Специальные возможности помогают пользователям с ограниченными возможностями, например, с ограниченной подвижностью или со слабым зрением, эффективно использовать информационные технологии.

### Обзор

На серверах IBM Power Systems реализованы следующие основные специальные возможности:

- Работа только с использованием клавиатуры
- Операции с использованием средства чтения с экрана

Серверы IBM Power Systems используют последний стандарт W3C WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) для обеспечения соответствия требованиям раздела 508 (США) (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) и Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Для того чтобы использовать специальные возможности, воспользуйтесь новейшим выпуском средства чтения с экрана и новейшим веб-браузером, который поддерживается серверами IBM Power Systems.

Интерактивная документация по серверам IBM Power Systems в Центре знаний IBM поддерживает специальные возможности. Функции специальных возможностей IBM Knowledge Center описаны в

разделе Специальные возможности справочной системы IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

### Клавиатурная навигация

Этот продукт использует стандартные клавиши навигации.

### Сведения об интерфейсе

Пользовательский интерфейс серверов IBM Power Systems не имеет содержимого, которое мерцает со скоростью от 2 до 55 раз в секунду.

Пользовательский веб-интерфейс серверов IBM Power Systems использует каскадные таблицы стилей для надлежащего вывода материалов и обеспечения удобного взаимодействия. Приложение предоставляет пользователям со слабым зрением эквивалентный способ использовать параметры системного дисплея, в том числе режим высокой контрастности. Регулировать размер шрифта с помощью параметров устройства или веб-браузера невозможно.

Пользовательский веб-интерфейс серверов IBM Power Systems содержит навигационные ориентиры WAI-ARIA, которые можно использовать для быстрой навигации по функциональным областям приложения.

### ПО независимых поставщиков

На серверах IBM Power Systems используется определенное программное обеспечение независимых поставщиков, которое не охвачено лицензионным соглашением IBM. IBM не дает никаких заверений относительно специальных возможностей данных продуктов. За информацией о специальных возможностях таких продуктов обращайтесь к их поставщикам.

### Связанная информация о специальных возможностях

Помимо стандартных веб-сайтов справочной системы и службы поддержки, IBM имеет телефонную службу TTY, которую пользователи с глухотой или слабым слухом могут использовать для доступа к продажам и услугам поддержки:

Служба TTY
800-IBM-3383 (800-426-3383)
(в Северной Америке)

Дополнительная информация о стратегии IBM в отношении специальных возможностей приведена на веб-странице IBM Accessibility (www.ibm.com/able).

## Замечания о правилах работы с личными данными

Продукты IBM Software, включающие решения Программа как услуга, (“Предложения программ”) могут использовать cookie или другие технологии сбора информации об использовании продукта для помощи в усовершенствовании интерфейса конечного пользователя, для организации взаимодействия с конечным пользователем или для других целей. В большинстве случаев Предложения программ не собирают персональную информацию. Некоторые из наших предложений программ могут помочь вам в сборе персональной информации. Если данное предложение программ использует cookie для сбора персональной информации, ниже приведены сведения об использовании cookie в данном предложении.

В зависимости от развернутых конфигураций, данное Предложение программ может использовать сеансовые cookie, собирающие имя и IP-адрес для каждого пользователя с целью управления сеансом. Эти cookie можно отключить, но их отключение приведет к потере функциональности, которые они обеспечивают.

Если развернутые конфигурации данного Предложения программ предоставляют вам как клиенту возможность сбора персональной информации от конечных пользователей с помощью cookie и

других технологий, необходимо проконсультироваться с юристом о законах, применимых к сбору таких данных, включая требования о замечаниях и согласии.

Дополнительная информация об использовании различных технологий, в том числе cookie, для таких целей приведена на странице Политика конфиденциальности IBM по адресу http://www.ibm.com/privacy/ru/ru и в Политика конфиденциальности IBM в Интернете по адресу http://www.ibm.com/privacy/details/us/en/ в разделе "Cookie, Web Beacon и другие технологии".

# Товарные знаки

IBM, эмблема IBM и ibm.com являются товарными знаками или зарегистрированными товарными знаками International Business Machines Corp., зарегистрированными во многих юрисдикциях мира. Названия других продуктов и услуг могут быть товарными знаками IBM и других компаний. Текущий список товарных знаков IBM опубликован на веб-странице Copyright and trademark information.

Зарегистрированный товарный знак Linux, сублицензирован у организации Linux Foundation, являющейся исключительным лицензиатом Линуса Торвальдса (Linus Torvalds) - владельца товарного знака на международном уровне.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph и Gluster являются товарными знаками или зарегистрированными товарными знаки компании Red Hat, Inc. или ее дочерних компаний в США и других странах.

Microsoft и Windows являются торговыми марками Microsoft в США и/или других странах.

Java и все товарные знаки и логотипы на основе Java являются товарными знаками или зарегистрированными товарными знаками компании Oracle и (или) ее дочерних компаний.

# Предупреждение об электронной эмиссии

## Замечания класса A

Следующие заявления об оборудовании класса A относятся к серверам IBM с процессорами POWER9 и их компонентам, если в описании компонента не указано, что он относится к классу B электромагнитной совместимости (EMC).

Для подключения монитора к оборудованию необходимо использовать специально предназначенный кабель для монитора и устройства подавления помех, поставляемые с монитором.

### Уведомление для Канады

CAN ICES-3 (A)/NMB-3(A)

### Уведомление для ЕС и Марокко

Данная продукция соответствует требованиям к защите, изложенным в директиве 2014/30/EU Европарламента и Совета ЕС касательно приведения в соответствие законодательства стран-членов Содружества, связанных с электромагнитной совместимостью. Компания IBM не несет ответственности за любое несоответствие требованиям защиты в результате нерекомендованного изменения продукта, включая использование дополнительных плат других производителей (отличных от IBM).

Использование данного продукта в жилых районах может вызвать появление помех. Такое использование возможно только при условии принятия специальных мер по снижению электромагнитного излучения во избежание возникновения помех в радио- и телевизионном сигнале.

Предупреждение: по своим характеристикам данное оборудование относится к классу A согласно классификации CISPR 32. При его использовании в жилых районах могут возникать радиопомехи.

## Уведомление для Германии

**Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit**

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaatenund hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

**Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten**

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

**Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A**

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Телефон: +49 (0) 800 225 5426
Электронная почта: HalloIBM@de.ibm.com

Generelle Informationen:

**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.**

## Уведомление о соответствии требованиям ассоциации JEITA

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

Это заявление относится к устройствам, потребляющих ток менее 20 A на фазу.

高調波電流規格 JIS C 61000-3-2 適合品

Данное заявление относится к устройствам, потребляющим ток более 20 A, одна фаза.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：6（単相、ＰＦＣ回路付）
• 換算係数 ：0

Данное заявление относится к устройствам, потребляющим ток более 20 A на фазу, три фазы.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：5（3相、ＰＦＣ回路付）
• 換算係数 ：0

**Уведомление о соответствии требованиям Японского добровольного совета по контролю помех (VCCI)**

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

**Уведомление для Кореи**

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

**Уведомление для КНР**

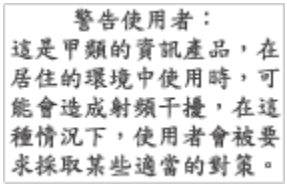
声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

**Уведомление для России**

ВНИМАНИЕ! Настоящее изделие относится к классу А. В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

### Уведомление для Тайваня




**Контактная информация для подразделения IBM в Тайване:**

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

### Уведомление о соответствии требованиям Федеральной комиссии по связи (FCC) США

Данное оборудование было протестировано на соответствие требованиям, предъявляемым к цифровым устройствам класса A в соответствии с частью 15 спецификаций FCC, и было признано соответствующим всем предъявляемым требованиям. Эти требования обеспечивают защиту от вредного излучения при работе оборудования в нежилых помещениях. Это оборудование генерирует, использует и излучает радиоволны. Если оборудование установлено не в соответствии с прилагаемым руководством, то оно может приводить вызывать радиопомехи. При эксплуатации данного оборудования в жилых помещениях весьма вероятно возникновение помех, влияние которых в этом случае заказчик должен устранить самостоятельно.

Для того чтобы данное оборудование соответствовало ограничениям на излучение, установленным FCC, необходимо пользоваться только правильно экранированными и заземленными кабелями и соединителями. Необходимые кабели и разъемы можно приобрести у официальных дилеров IBM. IBM не несет ответственности за любые помехи в радио- и телевизионном сигнале, вызванные применением кабелей и разъемов, отличных от рекомендуемых, или внесением несанкционированных изменений или модификаций в это оборудование. В случае несанкционированного изменения или модификации пользователю может быть запрещено работать с оборудованием.

Данное
устройство соответствует части 15 спецификаций FCC. Во время эксплуатации должны выполняться следующие два условия:
(1) это устройство не может вызывать вредные помехи, и (2) это устройство должно принимать любые полученные помехи, включая помехи, способные нарушить режим работы.

Ответственная сторона:
International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
Для связи по вопросам соответствия требованиям FCC: fccinfo@us.ibm.com

## Замечания класса B

Приведенные ниже замечания класса B применимы к функциям, определяемым в описании компонента как электромагнитная совместимость (EMC).

Для подключения монитора к оборудованию необходимо использовать специально предназначенный кабель для монитора и устройства подавления помех, поставляемые с монитором.

## Уведомление для Канады

CAN ICES-3 (B)/NMB-3(B)

## Уведомление для ЕС и Марокко

Данная продукция соответствует требованиям к защите, изложенным в директиве 2014/30/EU Европарламента и Совета ЕС касательно приведения в соответствие законодательства стран-членов Содружества, связанных с электромагнитной совместимостью. Компания IBM не несет ответственности за любое несоответствие требованиям защиты в результате нерекомендованного изменения продукта, включая использование дополнительных плат других производителей (отличных от IBM).

## Уведомление для Германии

**Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit**

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaatenund hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

**Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten**

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

**Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B**

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der
Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Телефон: +49 (0) 800 225 5426
Электронная почта: HalloIBM@de.ibm.com

Generelle Informationen:

**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse B**

### Уведомление о соответствии требованиям ассоциации JEITA

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

Это заявление относится к устройствам, потребляющих ток менее 20 A на фазу.

高調波電流規格 JIS C 61000-3-2 適合品

Данное заявление относится к устройствам, потребляющим ток более 20 A, одна фаза.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：6（単相、ＰＦＣ回路付）
• 換算係数 ：0

Данное заявление относится к устройствам, потребляющим ток более 20 A на фазу, три фазы.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：5（3相、ＰＦＣ回路付）
• 換算係数 ：0

### Уведомление о соответствии требованиям Японского добровольного совета по контролю помех (VCCI)

この装置は，クラスB情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　VCCI－B

### Уведомление для Тайваня

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

### Уведомление о соответствии требованиям Федеральной комиссии по связи (FCC) США

Данное оборудование было протестировано на соответствие требованиям, предъявляемым к цифровым устройствам класса B в соответствии с частью 15 спецификаций FCC, и было признано соответствующим всем предъявляемым требованиям. Эти требования обеспечивают защиту от вредного излучения при работе оборудования в жилых помещениях. Это оборудование генерирует, использует и может излучать энергию частоты радиоволн, и оно может вызвать помехи в системах радиосвязи, если установлено и используется не в соответствии с инструкциями. Однако нет никакой гарантии, что в определенных условиях установки помехи не появятся. Если это оборудование создает вредные помехи для радио- и телесигналов, что можно определить путем выключения и включения оборудования, то пользователю рекомендуется попытаться устранить помехи одним из следующих способов:

- Перенаправить или переместить антенну.
- Увеличить расстояние между оборудованием и приемником.
- Подключить оборудование в розетку не из той сети, в которую включен приемник.
- Проконсультироваться с авторизованным дилером IBM или сотрудником сервисного представительства.

Для того чтобы данное оборудование соответствовало ограничениям на излучение, установленным FCC, необходимо пользоваться только правильно экранированными и заземленными кабелями и соединителями. Необходимые кабели и разъемы можно приобрести у официальных дилеров IBM. IBM не несет ответственности за любые помехи в радио- и телевизионном сигнале, вызванные применением кабелей и разъемов, отличных от рекомендуемых, или внесением несанкционированных изменений или модификаций в это оборудование. В случае несанкционированного изменения или модификации пользователю может быть запрещено работать с оборудованием.

Данное устройство соответствует части 15 спецификаций FCC. Работа устройства регулируется следующими двумя условиями:

(1) это устройство не должно создавать вредные помехи, (2) это устройство должно быть устойчивым к любым помехам, включая помехи, способные нарушить режим работы.

Ответственная сторона:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504
Для связи по вопросам соответствия требованиям FCC: fccinfo@us.ibm.com

## Положения и условия

Разрешение на использование этих публикаций предоставляется на следующих условиях.

**Применимость:** Эти положения и условия являются дополнением к условиям использования веб-сайта IBM.

**Личное использование:** Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

**Коммерческое использование:** Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов вне своей организации без явного согласия IBM.

**Права:** На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если, по мнению производителя, использование этой публикации может принести ущерб его интересам или если IBM установят, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА СОДЕРЖАНИЕ ЭТИХ ПУБЛИКАЦИЙ. ЭТИ ПУБЛИКАЦИИ ПРЕДОСТАВЛЯЮТСЯ НА УСЛОВИЯХ "КАК ЕСТЬ", БЕЗ ПРЕДОСТАВЛЕНИЯ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ, СОБЛЮДЕНИЯ ПРАВ ИЛИ ПРИГОДНОСТИ ДЛЯ КАКИХ-ЛИБО КОНКРЕТНЫХ ЦЕЛЕЙ.