

Руководство по управлению рабочей средой

Профессиональные настольные компьютеры HP

© Copyright 2009 Hewlett-Packard Development Company, L.P. Информация, содержащаяся в настоящем документе, может быть изменена без предварительного уведомления.

Microsoft, Windows, Windows Vista и Windows 7 являются торговыми марками или зарегистрированными торговыми марками корпорации Microsoft в США и/или других странах/регионах.

Intel и vPro являются охраняемыми товарными знаками корпорации Intel Corporation в США и других странах/регионах.

Все виды гарантий на продукты и услуги компании HP указываются исключительно в заявлениях о гарантии, прилагаемых к указанным продуктам и услугам. Никакие сведения, содержащиеся в данном документе, не должны истолковываться как предоставление дополнительных гарантий. Компания HP не несет ответственности за технические или редакторские ошибки или пропуски, которые могут содержаться в настоящем документе.

Представленные в данном руководстве сведения защищены законами, регулирующими отношения авторского права. Никакая часть настоящего руководства не может быть воспроизведена какими-либо средствами (в том числе фотокопировальными) без специального письменного разрешения компании Hewlett-Packard.

Руководство по управлению рабочей средой

Профессиональные настольные компьютеры HP

Четвертое издание (сентябрь 2009 г.)

Номер документа: 581009-251

Об этом руководстве

Данное руководство содержит описания и инструкции по использованию средств безопасности и управления, предварительно установленных на некоторых моделях.

-
- ⚠ **ВНИМАНИЕ!** Помеченный таким образом текст означает, что несоблюдение рекомендаций может привести к тяжелым телесным повреждениям или гибели человека.
 - ⚠ **ПРЕДУПРЕЖДЕНИЕ.** Помеченный таким образом текст означает, что несоблюдение рекомендаций может привести к повреждению оборудования или потере информации.
 - 📝 **ПРИМЕЧАНИЕ.** Помеченный таким образом текст означает важную дополнительную информацию.
-

Содержание

1 Управление рабочей средой — обзор

2 Начальная настройка и развертывание

Агент HP Client Automation	2
HP Client Manager	3

3 Удаленная установка системы

4 Обновление программного обеспечения и управление им

Интерфейс управления клиентом HP Client Management Interface	5
Диспетчер HP SoftPaq Download Manager	6
Диспетчер HP System Software Manager	6
Диспетчер HP ProtectTools Security Manager	7
HP Client Automation Starter и Standard Edition	8
HP Client Automation Enterprise Edition	8
Диспетчер HP Client Manager компании Symantec	9
Пакет Altiris Client Management Suite	10
HP Client Catalog для продуктов Microsoft System Center и SMS	10
Технология удаленного управления	10
Настройка Intel Management Engine	11
Verdiem Surveyor	13
Служебная программа HP Proactive Change Notification	13
Веб-узел Subscriber's Choice	14
Устаревшие решения	14

5 Флэш-ПЗУ

Удаленная перезапись ПЗУ	15
Служебная программа HPQFlash	15

6 Режим аварийного восстановления загрузочного блока

7 Копирование настройки компьютера

Копирование на один компьютер	18
-------------------------------------	----

Копирование на несколько компьютеров	19
Создание загрузочного устройства	20
Поддерживаемое USB-устройство флэш-памяти	20
Неподдерживаемое USB-устройство флэш-памяти	22

8 Двухпозиционная кнопка питания

9 Веб-узел поддержки HP

10 Отраслевые стандарты

11 Средства отслеживания и защиты активов

Защита паролем	31
Установка пароля на доступ к программе настройки компьютера с помощью программы настройки компьютера	32
Установка пароля на включение компьютера с помощью служебной программы настройки компьютера	32
Ввод пароля на включение питания	33
Ввод пароля на доступ к программе настройки	33
Изменение пароля на включение компьютера или на доступ к программе настройки	34
Удаление пароля на включение компьютера или пароля программы настройки	34
Национальные символы-разделители, используемые на клавиатуре	35
Сброс паролей	35
Блокировка дисков (DriveLock)	35
Использование функции DriveLock	36
Приложения DriveLock	36
Датчик снятия крышки	38
Установка уровня защиты датчика снятия крышки	38
Блокировка крышки	38
Включение блокировки крышки.	39
Выключение блокировки крышки.	39
Использование аварийного ключа блокировки крышки	39
Замок с тросиком	40
Технология идентификации по отпечаткам пальцев	40
Уведомление о сбоях и восстановлению	40
Система защиты диска	40
Помехозащищенный блок питания	41
Датчик температуры	41

Указатель 42

1 Управление рабочей средой — обзор

Пакет HP Client Management Solutions предоставляет основанные на отраслевых стандартах решения для управления настольными компьютерами, рабочими станциями и переносными компьютерами, объединенными в сеть. С выпуском в 1995 году первых полностью управляемых настольных персональных компьютеров компания Hewlett-Packard стала первооткрывателем в области управляемости рабочей среды. Компания Hewlett-Packard получила патент на технологию управления HP Intelligent Manageability. С того времени компания HP предпринимает усилия по разработке отраслевых стандартов и инфраструктуры, необходимых для эффективного развертывания, управления и настройки настольных компьютеров, рабочих станций и портативных компьютеров. Компания HP разрабатывает собственное программное обеспечение для управления и тесно сотрудничает с ведущими поставщиками решений по управлению для обеспечения совместимости этих продуктов с пакетом HP Client Management Solutions. Решения HP Client Management Solutions являются важным аспектом расширенных обязательств компании по обеспечению пользователей решениями, помогающими снизить общую стоимость владения и эксплуатации компьютеров на протяжении всего периода их службы.

Система обладает следующими основными средствами и возможностями по управлению рабочей средой.

- Начальная настройка и развертывание
- Удаленная установка системы
- Обновление программного обеспечения и управление им
- Перезапись ПЗУ
- Конфигурация параметров оборудования
- Средства отслеживания и защиты активов
- Уведомления о сбоях и средства восстановления



ПРИМЕЧАНИЕ. Поддержка тех или иных функций, описанных в этом руководстве, может варьироваться в зависимости от модели или версии программного обеспечения.

2 Начальная настройка и развертывание

Компьютер поставляется с образом предварительно установленного системного программного обеспечения. После непродолжительного процесса «распаковки» программного обеспечения компьютер готов к работе.

Можно заменить образ предустановленного программного обеспечения индивидуальным набором системного и прикладного программного обеспечения. Существует несколько способов развертывания индивидуального образа программного обеспечения. К ним относятся:

- Установка дополнительных прикладных программ после «распаковки» образа предварительно установленного программного обеспечения.
- Использование программных средств развертывания, таких как HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (на основе технологии Radia) для замены предварительно установленного программного обеспечения образом индивидуального программного обеспечения.
- Использование процесса клонирования дисков для копирования содержимого с одного жесткого диска на другой.

Выбор оптимального метода развертывания зависит от используемой среды и применяемых процессов ИТ.

Установка с использованием ПЗУ и аппаратное обеспечение ACPI обеспечивают дополнительную помощь при восстановлении системного программного обеспечения, управлении конфигурацией, устранении неполадок и управлении электропитанием.

Агент HP Client Automation

Агент управления, используемый обеими версиями HP Client Automation (Standard и Enterprise Edition), предварительно установлен на компьютере. После установки он обеспечивает связь с консолью управления HP.

Для установки агента HP Client Automation:

1. Нажмите кнопку **Пуск**.
2. Выберите пункт **Все программы**.
3. Выберите **HP Manageability**.

4. Щелкните **HP Management Agent Readme**, применительно для желаемого языка.
5. Для установки HP Client Automation Agent просмотрите файл Readme и следуйте его указаниям.

Агент HP Client Automation Agent является ключевым компонентом инфраструктуры, необходимым для работы всех решений HP Client Automation. Для получения дополнительных сведений о других компонентах инфраструктуры, необходимых для применения решений по управлению конфигурацией HP посетите веб-узел <http://h20229.www2.hp.com/solutions/ascm/index.html>.

HP Client Manager

Диспетчер HP Client Manager (HPCM) бесплатно предоставляется компанией Symantec для всех поддерживаемых моделей профессиональных настольных, портативных компьютеров, рабочих станций и рабочих станций HP Blade. HPCM объединяет такие инструменты HP, как System Software Manager, HP Instant Support Professional Edition и HP Client Management Interface для обеспечения централизованного управления, отслеживания и наблюдения всего поддерживаемого аппаратного обеспечения HP.

HP Client Manager 7.0 — совершенно новый портал, универсальное средство, с помощью которого администратор может выполнять следующие задачи управления:

- Учет
- Предупреждения
- Управление системой BIOS
- Обновление драйверов
- Запуск сканирования и диагностики состояния с помощью HP Instant Support
- Запуск задач встроенной безопасности
- Просмотр HP Health Alert Trend за последние 3-6 месяцев
- Просмотр соответствия поддерживаемых компьютеров с помощью программы сканирования и диагностики состояния HP Instant Support
- Просмотр сводки по компьютерам HP – анализ поддерживаемых настольных и портативных компьютеров, рабочих станций и рабочих станций HP Blade PC
- Просмотр предупреждений: средства, пороги, состояние оборудования
- Отчеты
- Административные задачи для обновления специфических средств HP

HPCM можно загрузить со страницы <http://www.symantec.com/business/theme.jsp>, щелкнув **HP Client Manager** в разделе **Strategic Partner Products** (Продукты стратегических партнеров). Также на странице загрузки присутствует бесплатная постоянная лицензия.

На странице <http://www.symantec.com/connect> также присутствуют видеоролки «Как сделать». Найдите **HP Client Manager 7.0** для просмотра видеороликов поэтапного выполнения различных задач HPCM.

3 Удаленная установка системы

Удаленная установка системы позволяет запустить и настроить систему с помощью программного обеспечения и сведений о конфигурации, хранящихся на сетевом сервере, через протокол удаленной загрузки PXE. Функция удаленной установки системы обычно используется в качестве средства установки и настройки систем для выполнения следующих задач.

- Форматирование жесткого диска.
- Развертывание образа программного обеспечения на одном или нескольких новых компьютерах.
- Удаленное обновление базовой системы ввода-вывода (BIOS) во флэш-ПЗУ ([Удаленная перезапись ПЗУ на стр. 15](#)).

 **ПРИМЕЧАНИЕ.** Это средство записи BIOS системы из операционной системы Microsoft Windows.

- Настройка параметров базовой системы ввода-вывода (BIOS).

Чтобы запустить удаленную установку системы (Remote System Installation), нажмите клавишу **F12**, когда во время загрузки компьютера в нижнем правом углу экрана с эмблемой HP появится сообщение **F12 = Network Service Boot**. Продолжайте процедуру в соответствии с указаниями, появляющимися на экране. Порядок загрузки по умолчанию определяется одним из параметров BIOS; его можно изменить так, чтобы первой всегда выполнялась попытка загрузки PXE.

4 Обновление программного обеспечения и управление им

Компания HP поставляет несколько инструментальных средств для управления и обновления программного обеспечения на настольных компьютерах, рабочих станциях и портативных компьютерах:

- Интерфейс HP Client Management Interface
- Диспетчер HP SoftPaq Download Manager
- Диспетчер HP System Software Manager
- Диспетчер безопасности HP ProtectTools Security Manager
- HP Client Automation Starter, Standard Edition и Enterprise Edition
- Диспетчер HP Client Manager компании Symantec
- Пакет Altiris Client Management Suite
- HP Client Catalog для продуктов Microsoft System Center и SMS
- Компьютеры Intel vPro с технологией Active Management
- Средство Verdiem Surveyor
- Служебная программа HP Proactive Change Notification
- Веб-узел HP Subscriber's Choice

Интерфейс управления клиентом HP Client Management Interface

Независимо от того, какие средства управления системой используются в отделе ИТ, для организации в целом огромное значение имеет вопрос эффективного управления оборудованием и программным обеспечением, которое позволяло бы поддерживать низкий уровень расходов на ИТ и повышать динамичность делопроизводства. Администратор может получить доступ к интерфейсу HP Client Management Interface с помощью простых сценариев, интегрированных с тем или иным программным решением по собственному усмотрению.

С помощью интерфейса HP Client Management Interface (HP CMI) можно эффективно интегрировать новые профессиональные компьютеры HP в вашу управляемую ИТ-среду. HP CMI предоставляет интерфейс, упрощающий интеграцию профессиональных компьютеров HP с популярными в отрасли средствами управления компьютерами (включая Microsoft Systems

Management Server, IBM Tivoli Software и HP Operations) и индивидуальными корпоративными приложениями управления. С помощью HP CMI приложения и средства управления компьютерами могут запрашивать подробные инвентаризационные сведения о клиенте, получать сведения о состоянии и управлять параметрами BIOS, взаимодействуя непосредственно с клиентским компьютером, что снижает потребность в агентах и связующих программах при интеграции.

HP Client Management Interface основывается на отраслевых стандартах, включающих Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) и Advanced Configuration and Power Interface (ACPI). HP CMI является основной технологией, используемой в решениях HP Client Management. Благодаря HP CMI вам предоставляется гибкость выбора способа управления вашими клиентскими компьютерами HP.

Интерфейс HP Client Management Interface, используемый в сочетании с программным обеспечением для управления системой, обладает следующими возможностями:

- Запрос подробных инвентаризационных сведений о клиенте – сбор подробных сведений о процессоре, жестком диске, памяти, BIOS, драйверах, включая данные с датчиков (такие как скорость вентилятора, напряжение и температура).
- Получение сведений о состоянии – подписка на отправку широкого ряда оповещений оборудования клиентов (например, перегрев, остановка вентилятора и изменения конфигурации оборудования) на консоль управления системой, в приложение или на локальный клиентский компьютер. Оповещения, запущенные событиями оборудования, отправляются в реальном времени.
- Управление параметрами BIOS системы – выполнение функций F10, включая установку и изменение паролей BIOS и порядка загрузки компьютера удаленно с консоли управления системой на какой-либо или всех клиентских системах без физического присутствия около системы.

Дополнительную информацию об интерфейсе HP Client Management Interface можно найти по адресу: <http://www.hp.com/go/hpcmi/>.

Диспетчер HP SoftPaq Download Manager

Диспетчер HP SoftPaq Download Manager представляет собой бесплатный и простой в использовании интерфейс для обнаружения и загрузки обновлений программного обеспечения для моделей клиентских персональных компьютеров HP в рабочей среде. Указав модель, операционную систему и язык, можно быстро найти, отсортировать и выбрать нужные пакеты программного обеспечения. Для загрузки диспетчера HP SoftPaq Download Manager посетите веб-узел <http://www.hp.com/go/sdm>.

Диспетчер HP System Software Manager

Диспетчер HP System Software Manager (SSM) – это бесплатная служебная программа, которая обеспечивает автоматическое удаленное развертывание драйверов устройств и обновление BIOS для объединенных в сеть профессиональных компьютеров компании HP. При запуске диспетчер SSM автоматически (без взаимодействия с пользователем) определяет версии драйверов и установленной BIOS на каждой подключенной к сети клиентской системе и сравнивает эти данные с протестированным системным программным обеспечением SoftPaqs, которое хранится в центральном хранилище файлов. Затем диспетчер SSM автоматически обновляет все системное программное обеспечение, версия которого ниже хранящегося в хранилище файлов, на подключенных к сети компьютерах. Поскольку диспетчер SSM позволяет

распространять обновления SoftPaq только на соответствующие модели клиентских систем, администраторы могут уверенно и эффективно использовать SSM для постоянного обновления системного программного обеспечения.

Диспетчер System Software Manager используется совместно со средствами распространения программного обеспечения на предприятии, например с решениями HP Client Automation, диспетчером HP Client Manager компании Symantec и пакетом Microsoft Systems Management Server (SMS). С помощью диспетчера SSM можно распространять обновления, созданные пользователем или независимыми производителями и оформленные в формате SSM.

Диспетчер SSM можно бесплатно загрузить с веб-узла <http://www.hp.com/go/ssm>.



ПРИМЕЧАНИЕ. SSM в настоящее время не поддерживает удаленную запись ПЗУ на системах, в которых включена программа Windows BitLocker Drive Encryption и используется механизм доверенного платформенного модуля TPM для защиты ключей BitLocker, поскольку запись BIOS уничтожит подпись, которую BitLocker создает для этой платформы. Отключите BitLocker с помощью оснастки Групповая политика для записи BIOS системы.

Вы можете активировать поддержку Функции BitLocker, не выполняя измерений BIOS при помощи схемы безопасности TPM, чтобы клавиши BitLocker оставались действительными. Компания HP рекомендует создать резервную копию реквизитов BitLocker на тот случай, если потребуется их экстренное восстановление.

Диспетчер HP ProtectTools Security Manager

HP ProtectTools security обеспечивает средства безопасности, которые помогают предотвратить неавторизованный доступ к компьютеру, сетям и критическим данным. Повышенная функциональность безопасности обеспечивается следующими программными модулями и доступна через диспетчер безопасности HP ProtectTools Security Manager:

Диспетчер безопасности HP ProtectTools Security Manager — единая консоль, через которую доступны все остальные модули.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security for HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro for HP ProtectTools

HP ProtectTools предоставляет две версии для использования: Диспетчер HP ProtectTools Security и консоль администрирования HP ProtectTools. Обе версии, административная и пользовательская доступны через меню **Пуск > Все программы**.

Доступные модули программного обеспечения зависят от модели компьютера. Например, модуль Embedded Security for HP ProtectTools доступен только на компьютерах с установленной микросхемой встроенной системы безопасности модуля доверяемой платформы (TPM).

Программные модули HP ProtectTools могут быть предварительно установлены, загружены или доступны для загрузки на веб-узле HP. Для некоторых настольных компьютеров HP Pro модули HP ProtectTools доступны в качестве дополнительной опции после приобретения. Для получения дополнительных сведений посетите веб-узел <http://www.hp.com/products/security>.

HP Client Automation Starter и Standard Edition

HP Client Automation — это решение по управлению программным и аппаратным обеспечением для сред Windows Vista, Windows XP и HP Thin Client, которым легко пользоваться и которое быстро разворачивается, при этом предоставляя надежное основание для удовлетворения будущих требований. Оно предоставляется в двух изданиях.

- Начальное издание (Starter Edition) — это бесплатный продукт для управления настольными и переносными компьютерами и рабочими станциями HP, обеспечивающий сбор инвентаризационных сведений об аппаратном и программном обеспечении, удаленное управление, контроль оповещений HP, обновления BIOS и драйверов HP, интеграцию с HP Protect Tools и дополнительную поддержку технологии AMT корпорации Intel. Начальное издание также поддерживает развертывание и управление клиентами HP Thin Client.
- Стандартное издание (Standard Edition), доступное для приобретения, включает все функции начального издания, а также развертывание и перенос Windows, возможности управления пакетами исправлений, распространение программного обеспечения и измерение частоты использования программного обеспечения.

Начальное и стандартное издания HP Client Automation предоставляют путь для переноса издания HP Client Automation Enterprise Edition (на основе технологии Radia) для автоматического управления большими, разнородными и непрерывно меняющимися ИТ-средами.

Дополнительные сведения о решениях HP Client Automation можно найти по адресу: <http://www.hp.com/go/client>.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition (издание для предприятий) — это основанное на политиках решение для управления изменениями и настройкой, позволяющее администраторам эффективно и надежно осуществлять учет, развертывание и исправление программного обеспечения и содержимого на разнородных клиентских платформах. Издание HP Client Automation Enterprise Edition позволяет специалистам по ИТ:

- автоматизировать полный процесс управления жизненным циклом от обнаружения, развертывания и управления текущими ресурсами до переноса и списания;
- выполнять автоматическое развертывание и непрерывное управление полным комплектом программного обеспечения (операционными системами, приложениями, пакетами исправлений, настройками и содержимым) для достижения желаемого состояния;
- управлять программным обеспечением практически на любом устройстве, включая рабочие станции, настольные и переносные компьютеры в разнородной или изолированной инфраструктуре;
- управлять программным обеспечением в большинстве операционных систем.

Клиенты HP сообщают о значительном сокращении затрат на ИТ, уменьшении периода от начала разработки программного обеспечения и содержимого до его выхода на рынок и увеличении

производительности пользователей и степени их удовлетворения при постоянном управлении конфигурацией.

Дополнительные сведения о решениях HP Client Automation можно найти по адресу:
<http://www.hp.com/go/client>.

Диспетчер HP Client Manager компании Symantec

Диспетчер HP Client Manager производства компании Symantec, разработанный совместно с компанией Altiris, бесплатно предоставляется для всех поддерживаемых моделей профессиональных настольных, портативных компьютеров и рабочих станций HP. Диспетчер SSM встроен в диспетчер HP Client Manager и обеспечивает централизованное отслеживание, наблюдение и управление аппаратными характеристиками клиентских систем HP.

Диспетчер HP Client Manager компании Symantec используется для следующего.

- Получение ценных сведений об оборудовании, например, о ЦП, памяти, видеоподсистеме и параметрах безопасности.
- Контроль состояния системы с целью устранения неполадок еще до того, как они возникнут.
- Автоматическая загрузка и установка драйверов и обновлений BIOS без физического присутствия на каждом компьютере.
- Удаленная настройка BIOS и параметров безопасности.
- Автоматизация процессов для быстрого устранения неполадок оборудования.

Тесное объединение со средствами мгновенной поддержки HP снижает время на устранение неполадок в оборудовании.

- Диагностика – удаленный запуск и просмотр отчетов на настольных и переносных компьютерах и рабочих станциях компании HP.
- Проверка работоспособности системы – поиск известных неисправностей оборудования в установленной базе клиентских систем HP.
- Active Chat –подключение к центру технического обслуживания HP для устранения неисправностей.
- База знаний HP – ссылка на экспертную информацию.
- Автоматической процесс сбора и доставки пакетов SoftPaq для быстрого устранения неполадок с оборудованием.
- Идентификация, учет и инициализация систем с помощью встроенной микросхемы безопасности ProtectTools компании Hewlett-Packard.
- Возможность локального отображения оповещений о состоянии на клиентской системе.
- Предоставление основных инвентаризационных сведений для клиентов других производителей (не HP).
- Настройка и конфигурация микросхемы безопасности TPM.
- Централизованное планирование резервного копирования и восстановления клиентских компонентов.
- Дополнительная поддержка для управления технологией Intel AMT.

Дополнительные сведения о диспетчере HP Client Manager компании Symantec можно найти на веб-узле <http://www.hp.com/go/clientmanager>.

Пакет Altiris Client Management Suite

Altiris Client Management Suite — простое в использовании решение для программного управления настольными и портативными компьютерами, а также рабочими станциями на протяжении всего срока службы. Client Management Suite включает следующие продукты Altiris:

- Решение для инвентаризации
- Решение для развертывания
- Решение для доставки программного обеспечения
- Решение для управления исправлениями
- Решение для учета приложений
- Решение для управления приложениями
- Решение для копирования

Дополнительные сведения о пакете Altiris Client Management Suite можно найти по адресу: <http://www.symantec.com/business/client-management-suite>.

HP Client Catalog для продуктов Microsoft System Center и SMS

Каталог HP Client Catalog позволяет ИТ-специалистам, использующим продукты Майкрософт, автоматизировать развертывание обновлений программного обеспечения HP (пакетов Softpaq) на профессиональных персональных компьютерах HP. В файле каталога содержатся подробные сведения о платформах профессиональных настольных, портативных компьютеров и рабочих станций HP. Его можно использовать совместно со специальными функциями учета и обновления продуктов Майкрософт для обеспечения автоматических обновлений драйверов и исправлений на управляемых клиентских компьютерах HP.

Продукты Майкрософт, поддерживаемые каталогом HP Client Catalog, указаны ниже.

- System Center Configuration Manager 2007.
- System Center Essentials 2007.
- Systems Management Server (SMS) 2003 R2.

Дополнительную информацию о каталоге HP Client Catalog для SMS можно найти по адресу: <http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html>.

Технология удаленного управления

Модели содержат либо технологию vPro, либо стандартную технологию. Обе они обеспечивают лучшее обнаружение, исправление и защиту сетевых вычислительных ресурсов. Обе технологии позволяют управлять компьютерами независимо от того, включена ли система, выключена или «зависла».

Три формы удаленного управления доступны для профессиональных ПК. Это Alert Standard Format (ASF), Intel Active Management Technology (AMT) и Desktop and mobile Architecture for Systems Hardware (DASH).

Технология удаленного управления выполняет следующие функции.

- Обнаружение сети
- Инвентаризационные сведения об оборудовании
- Наблюдение за состоянием платформы
- Управление электропитанием – включение/выключение питания, выключение питания с последующим включением
- Удаленная диагностика и устранение неполадок
 - Перенаправление текстовой консоли позволяет управлять консолью удаленного ПК во время загрузки
 - Перенаправление носителя позволяет выполнять загрузку с удаленного загрузочного привода, диска или образа ISO (два варианта данной возможности это IDE-Redirect (IDE-R) на платформах AMT и USB Media Redirection)
- Аппаратная локализация и восстановление – ограничение или запрет сетевого доступа к компьютеру при обнаружении действий, похожих на действия вирусов
- Отслеживание и аудит событий платформы
- Встроенный портал управления с веб-узлом для удаленного доступа и настройки
- Технологии удаленного управления встроены в консоль управления HP партнеров



ПРИМЕЧАНИЕ. Все вышеперечисленные функции доступны не для всех платформ.

Настройка Intel Management Engine



ПРИМЕЧАНИЕ. Обзор технологии Intel vPro доступен на странице <http://www.intel.com/vpro>.

Информацию HP по технологии Intel vPro см. в официальной документации на веб-узле <http://www.hp.com/support>. Выберите свою страну/регион и язык, выберите пункт **Посмотреть информацию о поддержке и нахождении и устранении неисправностей**, введите номер модели компьютера и нажмите клавишу **Enter**. В категории **Ресурсы** щелкните **Руководства (справочники, приложения, дополнения и т.п.)**. В меню **Быстрый переход к руководствам по категориям...** выберите **Официальная документация**.

Доступные технологии управления включают следующие.

- AMT (включает DASH 1.0)
- ASF
- DASH 1.1 (используется сетевая карта Broadcom)

Технологии ASF и AMT поддерживаются, но могут не настраиваться одновременно.

Для настройки систем Intel vPro для использования технологий AMT или ASF:

1. Включите или перезагрузите компьютер. В операционной системе Microsoft Windows выберите **Пуск > Завершение работы > Перезагрузка**.
2. После включения компьютера, но до загрузки операционной системы нажмите сочетание клавиш **Ctrl+P**.



ПРИМЕЧАНИЕ. Если своевременно не нажать сочетание клавиш **Ctrl+P**, для входа в служебную программу придется повторно перезагружать компьютер и нажимать сочетание клавиш **Ctrl+P** до загрузки операционной системы.

Данное сочетание клавиш используется для запуска программы настройки Intel Management Engine BIOS Execution (MEBx). С помощью данной программы можно настроить различные параметры технологии управления. Некоторые из параметров конфигурации перечислены ниже.

- Main Menu (Основное меню).
 - Intel ® ME Configuration (Конфигурация Intel ® ME).
 - Intel ® AMT Configuration (Конфигурация Intel ® AMT).
 - Change Intel ® ME Password (Изменение пароля Intel ® ME).
 - Exit (Выход).
- Intel ® ME Platform Configuration (Конфигурация платформы Intel ® ME).
 - Intel ® ME State Control (enable/disable) (Включение или отключение управления состоянием Intel ® ME).
 - Intel ® ME Firmware Local Update (enable/disable) (Включение или отключение локального обновления микропрограммного обеспечения Intel ® ME).
 - Intel ® ME Features Control (Управление функциями Intel ® ME).
 - Intel ® ME Power Control (Управление питанием Intel ® ME).
- Intel ® AMT Configuration (Конфигурация Intel ® AMT).
 - Host Name (Имя хоста).
 - TCP/IP.
 - Provision Model (Модель подготовки) (Enterprise, SMB).
 - Setup and Configuration (Установка и настройка).
 - Un-Provision (Отмена подготовки).
 - SOL/IDE-R (enable/disable) (Включение или выключение SOL/IDE-R).

- Password Policy (Политика паролей).
- Secure Firmware Update (enable/disable) (Включение или отключение безопасного обновления микропрограммного обеспечения).
- Set PRTC (Установка PRTC).
- Idle Timeout (Тайм-аут бездействия).
- Change Intel ® ME Password (Изменение пароля Intel ® ME) (настоятельно рекомендуется изменить этот пароль. Пароль по умолчанию — **admin**.)

Для удаленного управления системами AMT администратору нужно использовать консоль удаленного управления, поддерживающую AMT. Корпоративные консоли управления доступны от таких поставщиков, как HP, Altiris и Microsoft SMS. В режиме SMB клиент предоставляет интерфейс для обозревателя Интернета. Для доступа к этой функции откройте обозреватель на любом компьютере в сети и введите http://имя_узла:16992, где имя_узла - это имя, назначенное компьютеру. Вместо имени узла можно использовать IP-адрес.

Для настройки систем с сетевой картой, поддерживающей Broadcom DASH:

Ознакомьтесь с последней документацией на веб-узле <http://www.hp.com> в разделе **Support & Troubleshooting** (Поддержка и устранение неисправностей), затем выберите вашу модель, выберите **Manuals** (Руководства), выберите **White papers** (Официальная документация), относящуюся к сетевым картам Broadcom.

Verdiem Surveyor

Средство Verdiem Surveyor представляет собой программное решение, которое помогает в управлении расходами на энергопитание ПК. Surveyor оценивает потребление энергии каждым ПК и предоставляет отчет. Кроме того, средство предоставляет возможность управления параметрами электропитания ПК, позволяя администраторам легко применять стратегии энергосбережения в сетях. Пакет программ HP, содержащий агент Surveyor, можно загрузить с веб-узла технической поддержки HP и установить на поддерживаемые модели промышленных настольных компьютеров. Лицензии Surveyor для управления компьютерами можно приобрести через представителя компании HP.

Служебная программа HP Proactive Change Notification

В программе заблаговременного распространения уведомлений об изменениях (Proactive Change Notification) используется веб-узел Subscriber's Choice, чтобы автоматически и заранее выполнять следующие действия.

- Отправлять пользователям по электронной почте уведомления PCN (Proactive Change Notification), заблаговременно (за 60 дней) информируя их об изменениях в оборудовании и программном обеспечении для большинства коммерческих компьютеров и серверов
- Отправлять пользователям по электронной почте сообщения, содержащие выпуски бюллетеней для клиентов, советов для клиентов, замечаний для клиентов, бюллетеней безопасности и уведомлений о драйверах для большинства коммерческих компьютеров и серверов.

Чтобы получать информацию, относящуюся только к своей ИТ-среде, пользователь создает собственный профиль. Получить дополнительные сведения о программе Proactive Change

Notification и создать свой собственный профиль можно на веб-узле по адресу:
<http://h30046.www3.hp.com/subhub.php>

Веб-узел Subscriber's Choice

Subscriber's Choice – это клиентская служба HP.

Основываясь на профиле пользователя, компания HP дает ему индивидуальные рекомендации по продуктам, сообщает о выходящих статьях, а также посылает предупреждения и уведомления о драйверах и технической поддержке.

Службы предупреждения и уведомления о драйверах и технической поддержке Subscriber's Choice отправляют по электронной почте уведомления о том, что информация, на которую вы подписались в своем профиле, доступна для просмотра и извлечения. Чтобы получить дополнительные сведения о службе Subscriber's Choice и создать свой профиль, посетите веб-узел <http://h30046.www3.hp.com/subhub.php>.

Устаревшие решения

Два программных пакета, Altiris Local Recovery и Dantz Retrospect больше не поставляются для настольных, портативных компьютеров и рабочих станций HP.

5 Флэш-ПЗУ

BIOS компьютера хранится в программируемом флэш-ПЗУ. Установкой пароля в служебной программе настройки компьютера (F10) можно защитить ПЗУ от случайного обновления или перезаписи. Это важно для обеспечения работоспособности компьютера. Если необходимо обновить BIOS, можно загрузить последние образы BIOS со страницы драйверов и поддержки HP, <http://www.hp.com/support/files>.

- △ **ПРЕДУПРЕЖДЕНИЕ.** Для обеспечения максимальной защиты ПЗУ следует убедиться, что установлен пароль для входа в программу настройки компьютера. Пароль для входа в программу настройки компьютера препятствует несанкционированному обновлению ПЗУ. System Software Manager позволяет системному администратору установить пароль на программу настройки для одного или нескольких компьютеров одновременно. Для получения дополнительных сведений посетите веб-узел <http://www.hp.com/go/ssm>.

Удаленная перезапись ПЗУ

Возможность удаленной перезаписи ПЗУ позволяет системному администратору безопасно обновлять ПЗУ на удаленных компьютерах Hewlett-Packard непосредственно с центральной консоли управления сетью. Возможность удаленного выполнения этой задачи системным администратором одновременно на нескольких компьютерах позволяет согласовано проводить развертывание образов BIOS на находящихся в сети компьютерах Hewlett-Packard и лучше контролировать этот процесс. Это также способствует повышению производительности и снижению затрат на обслуживание.

-  **ПРИМЕЧАНИЕ.** SSM в настоящее время не поддерживает удаленную запись ПЗУ на системах, в которых включена программа Windows BitLocker Drive Encryption и используется механизм доверенного платформенного модуля TPM для защиты ключей BitLocker, поскольку запись BIOS уничтожит подпись, которую BitLocker создает для этой платформы. Отключите BitLocker с помощью оснастки Групповая политика для записи BIOS системы.

Для удаленной перезаписи ПЗУ компьютер должен находиться во включенном состоянии или должны быть задействованы средства дистанционного включения компьютера по сети.

Для получения дополнительных сведений об удаленной записи флэш-ПЗУ обратитесь к справке HP Client Manager Software или System Software Manager по адресу <http://www.hp.com/go/ssm/>.

Служебная программа HPQFlash

Служебная программа HPQFlash используется для выполнения локального обновления или восстановления BIOS системы на персональном компьютере, работающем под управлением операционной системы Windows.

Для получения дополнительных сведений о HPQFlash посетите веб-узел <http://www.hp.com/support/files> и в ответ на предложение введите номер модели компьютера.

6 Режим аварийного восстановления загрузочного блока

Режим аварийного восстановления загрузочного блока позволяет выполнить восстановление системы в маловероятном случае отказа при перезаписи ПЗУ. Например, при отключении питания во время обновления BIOS перезапись ПЗУ будет выполнена не полностью. Это приведет к непригодности BIOS системы. Загрузочный блок представляет собой защищенный от перезаписи раздел ПЗУ, содержащий код, который при включении питания системы находит годный образ BIOS системы.

- Если образ BIOS системы не содержит ошибок, компьютер загружается как обычно.
- Если образ BIOS системы содержит ошибки, аварийный загрузочный блок BIOS позволяет выполнить поиск файлов образа BIOS на сменных носителях. При нахождении подходящего файла образа BIOS он автоматически записывается в ПЗУ.

При обнаружении ошибок в образе BIOS системы индикатор питания мигает красным цветом 8 раз (один раз в секунду) Одновременно с этим раздастся 8 сигналов динамика. Если часть системного ПЗУ, содержащая образ ПЗУ встроенного видеоадаптера, не повреждена, на экране появится сообщение **Boot Block Emergency Recovery Mode**.

Чтобы восстановить систему после ее входа в режим аварийного восстановления загрузочного блока, выполните следующие действия:

1. Выключите питание.
2. Вставьте компакт-диск или флэш-устройство USB, в корневом каталоге которого записан нужный файл образа BIOS.

 **ПРИМЕЧАНИЕ.** Носитель должен быть отформатирован под файловую систему FAT12, FAT16 или FAT32.

3. Включите компьютер.

Если соответствующий образа BIOS не найден, будет выведено сообщение о необходимости вставить носитель с файлом образа BIOS.

После успешного перепрограммирования ПЗУ система автоматически выключится.

4. Извлеките сменный носитель, использованный для обновления BIOS.
5. Включите питание, чтобы перезагрузить компьютер.

 **ПРИМЕЧАНИЕ.** BitLocker предотвращает загрузку Windows Vista, если в оптическом приводе находится компакт-диск, который содержит файл образа BIOS. Если BitLocker включен, извлеките компакт-диск перед загрузкой Windows Vista.

7 Копирование настройки компьютера

Описанные ниже процедуры позволяют администратору легко скопировать параметры BIOS компьютера на другой компьютер такой же модели. Это позволяет быстро и согласованно настроить несколько компьютеров.

 **ПРИМЕЧАНИЕ.** Для выполнения обеих процедур необходим дисковод гибких дисков или поддерживаемый флэш-накопитель USB.

ПРИМЕЧАНИЕ. System Software Manager (SSM) можно использовать для репликации данных о настройке компьютера в операционной системе Windows. Дополнительные сведения см. в руководстве пользователя SSM по адресу <http://www.hp.com/go/ssm>.

Копирование на один компьютер

△ **ПРЕДУПРЕЖДЕНИЕ.** Настройка параметров BIOS зависит от модели компьютера. Копирование настройки с компьютера на компьютер другой модели может привести к повреждению файловой системы последнего. Например, не копируйте настройку с компьютера dc7xxx на компьютер dx7xxx.

1. Выберите исходную настройку, которую необходимо скопировать. Выключите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Завершение работы**.
2. Если используется флэш-устройство USB, вставьте его.
3. Включите компьютер.
4. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

5. Если используется дискета, вставьте ее.
6. Выберите последовательно **File** (Файл) > **Replicated Setup** (Копируемая настройка) > **Save to Removable Media** (Сохранить на съемном носителе). Следуйте инструкциям на экране для создания дискеты или флэш-устройства USB с настройкой.
7. Выключите компьютер, на который будет переноситься настройка, и вставьте в его дисковод дискету или подключите к нему флэш-устройство USB с настройкой.
8. Включите компьютер, на который будет переноситься настройка.

9. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.
10. Выберите последовательно **File** (Файл) > **Replicated Setup** (Копируемая настройка) > **Restore from Removable Media** (Восстановить со съемного носителя) и следуйте инструкциям на экране.
11. Перезапустите компьютер после завершения его настройки.

Копирование на несколько компьютеров

△ **ПРЕДУПРЕЖДЕНИЕ.** Настройка параметров BIOS зависит от модели компьютера. Копирование настройки с компьютера на компьютер другой модели может привести к повреждению файловой системы последнего. Например, не копируйте настройку с компьютера dc7xxx на компьютер dx7xxx.

В описываемом методе процедура подготовки дискеты или флэш-устройства USB для настройки займет несколько больше времени, чем в предыдущем случае, однако процесс копирования на целевой компьютер будет осуществляться значительно быстрее.

📋 **ПРИМЕЧАНИЕ.** Для выполнения данной процедуры требуется загрузочная дискета или загрузочное флэш-устройство USB. Если отсутствует возможность создать загрузочную дискету с помощью Windows XP, следует использовать описанный выше метод копирования на один компьютер (см. [Копирование на один компьютер на стр. 18](#)).

1. Создайте загрузочную дискету или флэш-устройство USB. См. [Поддерживаемое USB-устройство флэш-памяти на стр. 20](#) или [Неподдерживаемое USB-устройство флэш-памяти на стр. 22](#).

△ **ПРЕДУПРЕЖДЕНИЕ.** Не все компьютеры можно загрузить с флэш-устройства USB. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с устройства USB предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

2. Выберите исходную настройку, которую необходимо скопировать. Выключите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Завершение работы**.
3. Если используется флэш-устройство USB, вставьте его.
4. Включите компьютер.
5. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

📋 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

6. Если используется дискета, вставьте ее.
7. Выберите последовательно **File** (Файл) > **Replicated Setup** (Копируемая настройка) > **Save to Removable Media** (Сохранить на съемном носителе). Следуйте инструкциям на экране для создания дискеты или флэш-устройства USB с настройкой.

8. Загрузите служебную программу BIOS для копирования настройки (repset.exe) и скопируйте ее на настроенную дискету или флэш-устройство USB. Чтобы получить эту служебную программу, посетите веб-узел <http://welcome.hp.com/country/us/en/support.html> и введите номер модели компьютера.
9. Создайте на дискете или флэш-устройстве USB с настройкой файл autoexec.bat, содержащий следующую команду:

`repset.exe`
10. Выключите компьютер, на который будет переноситься настройка. Вставьте в его дисковод дискету или подключите к нему флэш-устройство USB и включите компьютер. Произойдет автоматический запуск служебной программы настройки.
11. Перезапустите компьютер после завершения его настройки.

Создание загрузочного устройства

Поддерживаемое USB-устройство флэш-памяти

На поддерживаемых устройствах имеется заранее установленный образ, упрощающий процесс их превращения в загрузочные. На всех USB-устройствах флэш-памяти HP и Compaq и на большинстве остальных устройств имеется заранее установленный образ. Если на используемом флэш-устройстве USB такой образ отсутствует, следует использовать процедуру, описание которой также будет приведено в данном разделе (см. [Неподдерживаемое USB-устройство флэш-памяти на стр. 22](#)).

Чтобы создать загрузочное флэш-устройство USB, необходимо иметь:

- поддерживаемое флэш-устройство USB;
- загрузочную дискету DOS с программами FDISK и SYS (если программный файл SYS отсутствует, то можно использовать программу FORMAT, но все существующие на флэш-устройстве USB файлы будут утеряны);
- ПК, который может загружаться с флэш-устройства USB.

△ **ПРЕДУПРЕЖДЕНИЕ.** Некоторые более старые компьютеры могут не загружаться с флэш-устройства USB. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с устройства USB предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

1. Выключите компьютер.
2. Подключите флэш-устройство USB к одному из портов USB компьютера и отключите все другие накопители USB, за исключением дисководов USB.
3. Вставьте загрузочную дискету DOS с программами FDISK.COM и SYS.COM (или FORMAT.COM) в дисковод и включите компьютер, чтобы выполнить загрузку с загрузочной дискеты DOS.
4. Запустите программу FDISK из командной строки **A:**, набрав **FDISK** и нажав клавишу **Enter**. При появлении запроса щелкните **Yes (Y)** (Да), чтобы включить поддержку больших дисков.

5. Выберите вариант [5], чтобы отобразить накопители компьютера. Флэш-устройству USB будет соответствовать накопитель, указанная емкость которого близка к его фактической емкости. Обычно это последний накопитель в отображаемом списке. Запишите букву, соответствующую имени этого накопителя.

Флэш-устройство USB: _____

△ **ПРЕДУПРЕЖДЕНИЕ.** Если емкость накопителя не совпадает с емкостью флэш-устройства USB, выполнение описываемой процедуры следует прекратить, поскольку все данные могут быть потеряны. Проверьте все порты USB на наличие других накопителей. Если имеется какой-либо накопитель, отключите его, выполните перезагрузку компьютера и повторите описываемую процедуру, начиная с шага 4. Если накопителей не имеется, то либо данный компьютер не поддерживает флэш-устройство USB, либо это устройство неисправно. НЕ продолжайте попыток сделать флэш-устройство USB загрузочным.

6. Выйдите из программы FDISK, нажав клавишу **ESC**, чтобы вернуться к запросу **A:**.
7. Если на загрузочной дискете DOS имеется программа SYS.COM, переходите к шагу 8. В противном случае переходите сразу к шагу 9.
8. Введите из запроса **A:** команду **SYS x:**, где **x** соответствует букве имени накопителя, записанной нами на шаге.

△ **ПРЕДУПРЕЖДЕНИЕ.** Убедитесь в правильности ввода имени накопителя, соответствующего флэш-устройству USB.

После завершения переноса системных файлов программа SYS возвратится к запросу **A:**. Перейдите к шагу 13.

9. Скопируйте все необходимые файлы с флэш-устройства USB во временную папку на другом диске (например, на внутренний жесткий диск компьютера).
10. Введите из запроса **A:** команду **FORMAT /S x:**, где **x** соответствует букве имени накопителя, записанной ранее.

△ **ПРЕДУПРЕЖДЕНИЕ.** Убедитесь в правильности ввода имени накопителя, соответствующего флэш-устройству USB.

Команда **FORMAT** выведет одно или несколько сообщений, каждый раз запрашивая разрешения продолжить. Каждый раз нажимайте клавишу **Y**. Команда **FORMAT** выполнит форматирование USB-устройства флэш-памяти, добавит на него системные файлы и запросит метку тома.

11. Нажмите клавишу **Enter**, чтобы отказаться от ввода метки или введите ее, если хотите это сделать.
12. Скопируйте все файлы, сохраненные на шаге 9, обратно на флэш-устройство USB.
13. Удалите дискету и выполните перезагрузку компьютера. Компьютер загрузится с флэш-устройства USB, которое отобразится в качестве диска **C**.

📝 **ПРИМЕЧАНИЕ.** Порядок загрузки по умолчанию на различных компьютерах может быть разным и может быть изменен с помощью служебной программы настройки компьютера (F10).

При использовании версии DOS из Windows 9x некоторое время может отображаться экран с логотипом Windows. Если это нежелательно, добавьте файл нулевого размера с именем **LOGO.SYS** в корневой каталог флэш-устройства USB.

Далее см. раздел [Копирование на несколько компьютеров на стр. 19](#).

Неподдерживаемое USB-устройство флэш-памяти

Чтобы создать загрузочное флэш-устройство USB, необходимо иметь:

- флэш-устройство USB;
- загрузочную дискету DOS с программами FDISK и SYS (если программный файл SYS отсутствует, то можно использовать программу FORMAT, но все существующие на флэш-устройстве USB файлы будут утеряны);
- ПК, который может загружаться с флэш-устройства USB.

△ **ПРЕДУПРЕЖДЕНИЕ.** Некоторые более старые ПК могут не загружаться с флэш-устройства USB. Если в служебной программе настройки компьютера (F10) указан порядок загрузки по умолчанию, предусматривающий, что попытка загрузки с устройства USB предшествует загрузке с жесткого диска, то загрузка данного компьютера с флэш-устройства USB возможна. В противном случае необходимо будет использовать загрузочную дискету.

1. Если в компьютере имеются платы PCI с подключенными накопителями SCSI, ATA RAID или SATA, выключите компьютер и отключите шнур питания.

△ **ПРЕДУПРЕЖДЕНИЕ.** Шнур питания ДОЛЖЕН БЫТЬ обязательно отключен.

2. Откройте корпус компьютера и удалите все платы PCI.
3. Подключите флэш-устройство USB к одному из портов USB компьютера и отключите все другие накопители USB, за исключением дисководов USB. Закройте корпус компьютера.
4. Подключите шнур питания и включите компьютер.
5. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

6. Выберите последовательно **Advanced** (Дополнительно) > **PCI Devices** (PCI-устройства), чтобы отключить контроллеры PATA и SATA. При отключении контроллера SATA запомните номер IRQ, назначенный этому контроллеру. Этот номер потребуется позднее назначить снова. Выйдите из программы настройки, подтвердив сделанные изменения.

SATA IRQ: _____

7. Вставьте загрузочную дискету DOS с программами FDISK.COM и SYS.COM (или FORMAT.COM) в дисковод и включите компьютер, чтобы выполнить загрузку с загрузочной дискеты DOS.
8. Запустите программу FDISK и удалите все имеющиеся на флэш-устройстве USB разделы. Создайте новый раздел и пометьте его в качестве активного. Выйдите из программы FDISK, нажав клавишу **ESC**.
9. Если после выхода из программы FDISK не произойдет автоматической перезагрузки компьютера, нажмите клавиши **Ctrl+Alt+Del**, чтобы выполнить загрузку с дискеты DOS.

10. Введите после приглашения **A:** `FORMAT C: /S` и нажмите клавишу **Enter**. Программа Format выполнит форматирование флэш-устройства USB, добавит системные файлы и предложит ввести метку тома.
11. Нажмите клавишу **Enter**, чтобы отказаться от ввода метки или введите ее, если хотите это сделать.
12. Выключите компьютер и отключите шнур питания. Откройте корпус компьютера и снова установите удаленные ранее платы PCI. Закройте корпус компьютера.
13. Подключите шнур питания, удалите дискету и включите компьютер.
14. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.
15. Выберите **Advanced** (Дополнительно) > **PCI Devices** (PCI-устройства), чтобы снова включить контроллеры PATA и SATA, отключенные на шаге 6. Назначьте контроллеру SATA его исходный номер IRQ.
16. Сохраните изменения и выйдите из служебной программы. Компьютер загрузится с флэш-устройства USB, которое отобразится в качестве диска C.



ПРИМЕЧАНИЕ. Порядок загрузки по умолчанию различается у разных компьютеров и может быть изменен в служебной программе настройки компьютера (F10). Инструкции см. в разделе *Использование служебной программы настройки компьютера (F1)*.

При использовании версии DOS из Windows 9x, некоторое время может отображаться экран с логотипом Windows. Если это нежелательно, добавьте файл нулевого размера с именем LOGO.SYS в корневой каталог флэш-устройства USB.

Далее см. раздел [Копирование на несколько компьютеров на стр. 19](#).

8 Двухпозиционная кнопка питания

При включенном интерфейсе управления питанием (ACPI, Advanced Configuration and Power Interface) кнопка питания может выполнять как функцию включения и отключения питания, так и функцию перевода компьютера в ждущий режим. Средство приостановки работы не производит полного отключения питания, а переводит компьютер в режим пониженного энергопотребления. Это позволяет быстро приостановить работу компьютера, не закрывая приложений, а затем так же быстро вернуться в исходный рабочий режим без потери данных.

Для изменения функций кнопки питания выполните следующие действия.

1. **Левой кнопкой мыши щелкните кнопку **Пуск**, затем выберите **Панель управления > Электропитание**.**
2. **В окне **Свойства: электропитание** выберите вкладку **Дополнительно**.**
3. **В разделе **Кнопки питания** выберите **Переход в ждущий режим**.**

Настроив кнопку питания для работы в качестве кнопки перехода в ждущий режим, нажмите ее для перевода компьютера в режим с очень низким потреблением энергии (ждущий режим). Для быстрого возобновления работы компьютера повторно нажмите на кнопку питания. Для полного отключения подачи энергии нажмите и удерживайте кнопку питания в течение четырех секунд.

△ **ПРЕДУПРЕЖДЕНИЕ.** Используйте кнопку отключения питания компьютера, только если система не отвечает. Выключение питания компьютера без взаимодействия с операционной системой может привести к повреждению или потере данных на жестком диске.

9 Веб-узел поддержки HP

Для обеспечения высокой производительности, совместимости и надежности компьютеров Hewlett-Packard инженеры компании осуществляют строгий контроль и отладку программного обеспечения, разработанного компанией Hewlett-Packard и независимыми производителями, а также разрабатывают специальное программное обеспечение.

При переходе на новые или измененные операционные системы необходимо установить программное обеспечение поддержки, разработанное для соответствующей операционной системы. Если планируется использовать версию операционной системы Microsoft Windows, отличающуюся от версии, имеющейся на компьютере, для обеспечения правильной работы всех функций следует установить соответствующие драйверы устройств и служебные программы.

В HP упростили задачу поиска, доступа, оценки и установки последних программ поддержки. Программу можно загрузить с веб-узла <http://www.hp.com/support>.

На веб-узле имеются последние версии драйверов устройств, служебных программ и образы флэш-ПЗУ, необходимые для последней версии операционной системы Microsoft Windows, установленной на данном компьютере Hewlett-Packard.

10 Отраслевые стандарты

Предлагаемые компанией Hewlett-Packard решения по управлению объединяются с другими приложениями для управления компьютером и основываются на таких отраслевых стандартах, как:

- Управление предприятиями с веб-интерфейсом – Web-Based Enterprise Management (WBEM)
- Интерфейс управления Windows – Windows Management Interface (WMI)
- Технология Wake on LAN
- Интерфейс ACPI
- SMBIOS
- Поддержка предзагрузочной среды выполнения (PXE)

11 Средства отслеживания и защиты активов

С помощью средств отслеживания ресурсов, реализованных на данном компьютере, собираются данные для диспетчеров HP Systems Insight Manager, HP Client Manager, решения HP Configuration Management Solution, диспетчера HP Client Configuration Manager и других приложений управления компьютерами. Тесная автоматизированная связь между компонентами средств отслеживания и этими программными продуктами позволяет выбрать средство управления, которое лучше всего подходит для данной информационно-вычислительной среды и позволяет получить большую отдачу от сделанных вложений в программное обеспечение.

Компания Hewlett-Packard также предлагает различные решения для средств контроля доступа к важным компонентам компьютера и информации. Программное средство безопасности HP Embedded Security for ProtectTools, установленное на компьютере, предотвращает несанкционированный доступ к данным, проверяет целостность системы и выявляет попытки посторонних лиц получить доступ к системе. (Для получения дополнительных сведений см. руководство по диспетчеру безопасности *HP ProtectTools Security Manager Guide* на веб-узле <http://www.hp.com/products/security>). Средства безопасности, такие как встроенная система безопасности HP Embedded Security for ProtectTools, интеллектуальный датчик снятия крышки и блокировка крышки, доступные на некоторых моделях, помогают предотвратить несанкционированный доступ к внутренним компонентам персонального компьютера. Отключая параллельный порт, последовательный порт, порт USB или возможность загрузки со сменных носителей, можно воспрепятствовать доступу к ценным информационным ресурсам. Сообщения об изменении памяти и предупреждения датчика снятия крышки могут автоматически передаваться приложениям управления системой для обеспечения оперативного уведомления о несанкционированном доступе к внутренним компонентам компьютера.



ПРИМЕЧАНИЕ. Для некоторых систем такие средства безопасности, как встроенная безопасность для ProtectTools, датчик снятия крышки и блокировка крышки, доступны в качестве дополнительных.

Для управления параметрами безопасности компьютеров Hewlett-Packard используются следующие служебные программы.

- Локально, используя программы настройки компьютера. Дополнительные сведения и указания по использованию программ настройки компьютера см. в разделе *Руководство по использованию служебной программы настройки компьютера (F10)*.
- При удаленном управлении — диспетчер HP Client Manager компании Symantec, HP Client Automation или диспетчер System Software Manager. Эти программные средства обеспечивают безопасное, последовательное развертывание настроек безопасности и управление ими.

В приведенной ниже таблице и последующих разделах рассказано, как локально управлять средствами безопасности компьютера, используя служебные программы настройки компьютера (F10).

Таблица 11-1 Обзор средств безопасности

Пункт меню	Описание
Setup Password (Пароль программы настройки)	Установка и включение использования пароля (административного) на доступ к программе настройки компьютера. ПРИМЕЧАНИЕ. Если установлен пароль на доступ к программе настройки компьютера, его ввод будет необходим для изменения параметров в программе настройки компьютера, перезаписи ПЗУ и изменения некоторых параметров самонастраиваемых (Plug and Play) устройств в Windows.
Power-On Password (Пароль на включение компьютера)	Установка и включение использования пароля на включение питания. После перезагрузки появится запрос на ввод пароля на включение компьютера. Если не будет введен верный пароль на включение компьютера, загрузка не будет выполнена. ПРИМЕЧАНИЕ. Пароль не используется при «горячем» перезапуске (при помощи клавиш Ctrl + Alt + Delete или Restart from Windows (Перезагрузка из Windows), если это не было установлено в пункте Password Options (Параметры защиты паролем)) (см. ниже).
Password Options (Параметры защиты паролем) (Эта функция появляется только в том случае, если установлен пароль на включение питания или пароль для доступа к программе настройки компьютера.)	Выполнение следующих действий: • блокировка устаревших устройств (появляется только в том случае, если установлен пароль для программы настройки компьютера); • включение или отключение режима сетевого сервера (появляется только в том случае, если установлен пароль на включение питания); • выбор необходимости пароля для программной перезагрузки (Ctrl+Alt+Delete) (появляется только в том случае, если установлен пароль на включение питания). • Включение/выключение режима просмотра настройки (Setup Browse Mode) (появляется, только если установлен пароль для программы настройки компьютера, и позволяет просмотр параметров программы настройки (F10) без возможности их изменения и без ввода пароля). • Включение/выключение пароля повышенной безопасности (Stringent Password) (появляется при установленном пароле на включение питания). Если этот пароль включен, встроенная перемычка для сброса пароля игнорируется, и пароль на включение питания отключается. Для получения дополнительных сведений см. <i>Руководство по устранению неполадок</i>.
Smart Cover (Крышка компьютера) (на некоторых моделях)	Выполнение следующих действий: • Установка и снятие блокировки крышки. • Установка для датчика снятия крышки режима Disable (отключен), Notify User (уведомление пользователя) или Setup Password (пароль программы настройки). ПРИМЕЧАНИЕ. В режиме <i>Notify User</i> пользователю выдается уведомление о том, что, по показаниям датчика, крышка компьютера снималась. В режиме <i>Setup Password</i> (пароль для доступа к программе настройки компьютера) для загрузки компьютера требуется ввести пароль для доступа к программе настройки компьютера, если, по показаниям датчика, крышка компьютера снималась. Данная функция поддерживается только на некоторых моделях.

Таблица 11-1 Обзор средств безопасности (продолжение)

Device Security (Безопасность компьютера)	Позволяет настраивать параметр «Device Available/Device Hidden» (Устройство доступно/Устройство скрыто) для следующего. • Последовательные порты. • Параллельный порт. • Порты USB на задней панели. • Порты USB на передней панели. • Встроенные порты USB. • Аудиосистема. • Сетевые контроллеры (на некоторых моделях). • Legacy Diskette (Устаревший дисковод). • Встроенное устройство безопасности (на некоторых моделях). • SATA0. • SATA1 (на некоторых моделях). • SATA2 (на некоторых моделях). • SATA3 (на некоторых моделях). • eSATA (на некоторых моделях).
LoJack for HP ProtectTools	Позволяет удаленно наблюдать, отслеживать ваш компьютер и управлять им. Запущенная программа LoJack Pro for HP ProtectTools настраивается из Absolute Software Customer Center. Из Customer Center администратор может настраивать LoJack for HP ProtectTools для наблюдения и управления компьютером. Если систем находится в неподобающем месте или украдена, Customer Center может помочь местным властям найти и вернуть компьютер. После настройки LoJack Pro может продолжить работу, даже если жесткий диск стерт или заменен.
Network Service Boot (Служебная загрузка через сеть)	Включение или отключение возможности загрузки на компьютер операционной системы, установленной на сетевом сервере. (Эта функция доступна только в моделях с сетевым адаптером. Сетевой адаптер должен быть платой расширения PCI или встроен в системную плату.)
System IDs (Идентификаторы компьютера)	Установка следующих параметров: • Инвентарный номер (18-байтовый идентификатор), назначенный данной компанией этому компьютеру. • Идентификатор принадлежности (80-байтовый идентификатор), выводимый на экран во время проверки POST. • Серийный номер шасси или универсальный уникальный идентификатор UUID (Universal Unique Identifier). Идентификатор UUID можно обновлять только в том случае, если серийный номер шасси неправильный. (Эти идентификационные номера обычно устанавливаются производителем и используются для идентификации компьютера.) • Параметры клавиатуры в соответствии с языком страны пользования (например, английским или немецким) для идентификатора компьютера.
DriveLock Security (Блокировка дисков)	Назначение или изменение главного или пользовательского пароля для жестких дисков. Если это средство включено, в ходе выполнения POST выводится запрос на ввод одного из паролей блокировки диска. Если правильный пароль не будет введен, жесткий диск останется недоступным, пока во время выполнения последующей процедуры "холодной" загрузки не будет введен один из нужных паролей.

Таблица 11-1 Обзор средств безопасности (продолжение)

ПРИМЕЧАНИЕ. Данный параметр отображается только в том случае, когда на компьютере установлен по крайней мере один жесткий диск, поддерживающий блокировку диска.	
Уровень безопасности программы настройки	Предоставление конечным пользователям ограниченного доступа на изменение указанных параметров в программе настройки без ввода пароля программы настройки. Данная функция предоставляет администратору гибкость защиты от изменения важных параметров настройки, одновременно позволяя пользователям просматривать параметры системы и устанавливать второстепенные параметры. Администратор устанавливает права доступа для отдельных параметров настройки с помощью меню Setup Security Level (Уровень безопасности программы настройки). По умолчанию для всех параметров программы настройки установлен пароль настройки, который необходимо ввести во время проверки POST, чтобы изменить какие-либо параметры. Для отдельных элементов администратор может установить значение None (отсутствует), что означает, что пользователь может изменять значения указанных параметров, если вход в программу настройки выполнен с неправильным паролем. При установке пароля на включение компьютера вместо None (отсутствует) появляется Power-On Password (Пароль на включение компьютера). ПРИМЕЧАНИЕ. Для входа пользователей в программу настройки без ввода пароля программы настройки для параметра Setup Browse Mode (Режим просмотра настройки) должно быть установлено значение Enable (Включен).
System Security (Безопасность системы) (для некоторых моделей эти параметры зависят от оборудования)	Режим Data Execution Prevention (предотвращение выполнения данных) (включение/отключение, только на некоторых моделях) помогает предотвращать нарушения безопасности операционной системы. Virtualization Technology (Технология виртуального представления) (включение/отключение, только на некоторых моделях). Управление функциями виртуального представления процессора. Для изменения этого параметра необходимо включить и выключить компьютер. Virtualization Technology Directed I/O (Технология виртуального представления — направленный ввод/вывод) (включение/отключение, только на некоторых моделях). Управление функциями переназначения DMA виртуального представления микросхемы. Для изменения этого параметра необходимо включить и выключить компьютер. Trusted Execution Technology (Технология доверенного исполнения) (включение/отключение, только на некоторых моделях). Управление функциями основного процессора и микросхемы, необходимыми для поддержки виртуального приложения. Для изменения этого параметра необходимо включить и выключить компьютер. Чтобы включить эту функцию, необходимо включить следующие функции. • Поддержка встроенного устройства безопасности • Virtualization Technology • Virtualization Technology Directed I/O Embedded Security Device Support (Поддержка встроенного устройства безопасности) (включение/отключение, только на некоторых моделях). Позволяет включать и отключать встроенное устройство безопасности. Для изменения этого параметра необходимо включить и выключить компьютер.

Таблица 11-1 Обзор средств безопасности (продолжение)

ПРИМЕЧАНИЕ. Чтобы настроить встроенное устройство безопасности, необходимо указать пароль настройки.

- Reset to Factory Settings (Восстановить заводские значения параметров) (без восстановления/восстановление, только на некоторых моделях). Восстановление заводских значений параметров приведет к удалению всех ключей безопасности. Для изменения этого параметра необходимо включить и выключить компьютер.

ПРЕДУПРЕЖДЕНИЕ. Встроенное устройство безопасности – это очень важный компонент многих схем безопасности. Если ключи безопасности будут удалены, это приведет к отсутствию доступа к данным, защищенным встроенным устройством безопасности. Использование параметра «Восстановить заводские значения параметров» (Reset to Factory Settings) может привести к значительным потерям данных.

- Reset authentication credentials (Сброс учетных данных для проверки подлинности) (включение/отключение, только на некоторых моделях). Этот параметр позволяет отключить поддержку проверки подлинности при включении компьютера и удалить сведения, относящиеся к проверке подлинности. Для изменения этого параметра необходимо включить и выключить компьютер.

OS management of Embedded Security Device (Управление встроенным устройством безопасности через ОС) (включение/отключение, только на некоторых моделях). Позволяет пользователю ограничить возможность управления встроенным устройством безопасности через ОС. Для изменения этого параметра необходимо включить и выключить компьютер. Этот параметр позволяет пользователю ограничивать возможность управления встроенным устройством безопасности через ОС.

- Reset of Embedded Security Device through OS (Сброс параметров встроенного устройства безопасности через ОС) (включение/отключение, только на некоторых моделях). Этот параметр позволяет пользователю ограничить возможность отправки запросов на сброс параметров встроенного устройства безопасности до заводских. Для изменения этого параметра необходимо включить и выключить компьютер.

ПРИМЕЧАНИЕ. Чтобы включить этот параметр, необходимо указать пароль настройки.

PAVP (отключено/минимально/максимально, только на некоторых моделях). PAVP включает защищенный путь звука и видео (Protected Audio Video Path) на микросхеме. Это может способствовать просмотру защищенного содержания высокой четкости, воспроизведение которого иным способом запрещено. При выборе значения «Max» (Максимально) 96 Мб системной памяти будет выделено исключительно для PAVP.

Защита паролем

Пароль на включение компьютера, препятствующий его несанкционированному использованию, будет затребован каждый раз при включении или повторной инициализации компьютера для дальнейшего доступа к его прикладным программам или содержащейся в его памяти информации. Пароль на доступ к программе настройки препятствует несанкционированному доступу непосредственно к программе настройки и может также использоваться для входа в компьютер вместо пароля на включение компьютера. Таким образом, если вместо затребованного пароля на включение компьютера будет введен пароль на доступ к программе настройки, доступ к компьютеру все равно будет получен.

Пароль на доступ к программе настройки, действительный для всей сети, позволяет системному администратору зарегистрироваться на любом компьютере сети для проведения работ по обслуживанию, не зная пароля пользователя на включение компьютера, даже если он был установлен.

 **ПРИМЕЧАНИЕ.** System Software Manager (SSM) может использоваться для создания и управления паролем BIOS из операционной системы Windows. Дополнительные сведения см. в руководстве пользователя SSM по адресу <http://www.hp.com/go/ssm>.

ПРИМЕЧАНИЕ. HP Client Management Interface (HP CMI) обеспечивает управление параметрами BIOS из операционной системы Windows, включая пароль BIOS. Дополнительные сведения см. в официальной технической документации HP Client Management Interface <http://www.hp.com/go/hpcmi>.

Установка пароля на доступ к программе настройки компьютера с помощью программы настройки компьютера

Если система снабжена встроенным устройством безопасности, обратитесь к руководству *HP ProtectTools Security Manager Guide* на странице <http://www.hp.com>. Установка пароля на вход в программу настройки компьютера предотвращает изменение настроек компьютера (с помощью служебной программы настройки компьютера (F10)) до того, как будет введен пароль.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузка**.
2. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. Выберите пункт **Security** (Безопасность), затем – **Setup Password** (Пароль программы настройки) и следуйте инструкциям на экране.
4. Перед выходом из программы выберите **File** (Файл) > **Save Changes and Exit** (Сохранить изменения и выйти).

Установка пароля на включение компьютера с помощью служебной программы настройки компьютера

Установка пароля на включение компьютера с помощью программы настройки компьютера предотвращает доступ к компьютеру при его включении, пока не будет введен пароль. После того как пароль установлен, программа настройки компьютера отображает пункт **Password Options** (Параметры защиты паролем) в меню **Security** (Безопасность). Среди параметров пароля можно выбрать **Password Prompt on Warm Boot** (Запрос пароля при перезагрузке). При включенном запросе на ввод пароля при перезагрузке пароль потребует вводиться при каждой перезагрузке компьютера.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузка**.
2. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. Выберите пункт **Security** (Безопасность), затем – **Power-On** (Включение) и следуйте инструкциям на экране.
4. Перед выходом из программы выберите **File** (Файл) > **Save Changes and Exit** (Сохранить изменения и выйти).

Ввод пароля на включение питания

Для ввода пароля на включение компьютера выполните следующие действия:

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузить компьютер**.
2. Когда на экране монитора появится значок ключа, введите текущий пароль и нажмите клавишу **Enter**.

 **ПРИМЕЧАНИЕ.** Вводите пароль внимательно; так как в целях безопасности вводимые знаки не отображаются на экране.

Если пароль введен неправильно, на экране появится значок сломанного ключа. Попробуйте еще раз. После трех неудачных попыток ввода пароля для продолжения придется выключить и снова включить компьютер.

Ввод пароля на доступ к программе настройки

Если система снабжена встроенным устройством безопасности, обратитесь к руководству *HP ProtectTools Security Manager Guide* на странице <http://www.hp.com>.

Если на компьютере был установлен пароль на доступ к программе настройки, каждый раз при запуске данной программы на экране будет появляться запрос на ввод этого пароля.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузка**.
2. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. Когда на экране монитора появится значок ключа, введите пароль настройки и нажмите клавишу **Enter**.

 **ПРИМЕЧАНИЕ.** Вводите пароль внимательно, так как в целях безопасности вводимые знаки не отображаются на экране.

Если пароль введен неправильно, на экране появится значок сломанного ключа. Попробуйте еще раз. После трех неудачных попыток ввода пароля для продолжения придется выключить и снова включить компьютер.

Изменение пароля на включение компьютера или на доступ к программе настройки

Если система снабжена встроенным устройством безопасности, обратитесь к руководству *HP ProtectTools Security Manager Guide* на странице <http://www.hp.com>.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузить компьютер**.

2. Для изменения пароля на включение компьютера перейдите к шагу 3.

Чтобы изменить пароль для входа в программу настройки компьютера, после включения компьютера, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. При появлении значка ключа введите текущий пароль, косую черту (/) или альтернативный разделитель, затем введите новый пароль, еще одну косую черту (/) или альтернативный разделитель и еще раз новый пароль в следующем порядке, как показано на рисунке:
текущий пароль / новый пароль / новый пароль

 **ПРИМЕЧАНИЕ.** Вводите пароль внимательно, так как в целях безопасности вводимые знаки не отображаются на экране.

4. Нажмите клавишу **Enter**.

Новый пароль действует с момента следующего включения компьютера.

 **ПРИМЕЧАНИЕ.** Дополнительные сведения об альтернативных разделителях см. в разделе [Национальные символы-разделители, используемые на клавиатуре на стр. 35](#). Пароль для включения компьютера и пароль настройки можно также изменять, используя параметры защиты программы настройки компьютера.

Удаление пароля на включение компьютера или пароля программы настройки

Если система снабжена встроенным устройством безопасности, обратитесь к руководству *HP ProtectTools Security Manager Guide* на странице <http://www.hp.com>.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузить компьютер**.

2. Для удаления пароля на включение компьютера перейдите к шагу 3.

Чтобы удалить пароль для входа в программу настройки компьютера, после включения компьютера, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. При появлении значка ключа введите текущий пароль, а затем косую черту или альтернативный разделитель, как показано ниже: текущий пароль /
4. Нажмите клавишу **Enter**.

 **ПРИМЕЧАНИЕ.** Дополнительные сведения об альтернативных разделителях см. в разделе [Национальные символы-разделители, используемые на клавиатуре на стр. 35](#). Пароль для включения компьютера и пароль настройки можно также изменять, используя параметры защиты программы настройки компьютера.

Национальные символы-разделители, используемые на клавиатуре

Каждая клавиатура разрабатывается в соответствии с конкретными требованиями соответствующей страны. Символы и знаки препинания, которые используются для изменения или удаления пароля, зависят от клавиатуры, которая поставляется вместе с компьютером.

Национальные символы-разделители, используемые на клавиатуре					
/	Арабский	-	Греческий	/	Русский
=	Бельгийский	.	Иврит	-	Словацкий
-	БГХЧСС*	-	Венгерский	-	Испанский
/	Бразильский	-	Итальянский	/	Шведский/Финский
/	Китайский	/	Японский	-	Швейцарский
-	Чешский	/	Корейский	/	Тайваньский
-	Датский	-	Латиноамериканский	/	Тайский
!	Французский	-	Норвежский	.	Турецкий
й	Французский (Канада)	-	Польский	/	Английский (США)
-	Немецкий	-	Португальский		
* для Боснии-Герцеговины, Хорватии, Черногории, Сербии и Словении					

Сброс паролей

Если пароль будет забыт, доступ к компьютеру станет невозможен. Для получения сведений о процедуре сброса паролей обратитесь к *Руководству по устранению неполадок*.

Если система снабжена встроенным устройством безопасности, обратитесь к руководству *HP ProtectTools Security Manager Guide* на странице <http://www.hp.com>.

Блокировка дисков (DriveLock)

Блокировка дисков (DriveLock) – это предусмотренное отраслевым стандартом средство защиты, которое предотвращает несанкционированный доступ к данным на жестких дисках с интерфейсом ATA. Блокировка дисков DriveLock включена в качестве дополнительного средства в программу настройки компьютера. Это средство доступно только в случае обнаружения жестких дисков, поддерживающих набор команд ATA Security. Средство блокировки дисков предназначено для тех клиентов компании Hewlett-Packard, которые в первую очередь заинтересованы в обеспечении безопасности данных. Для таких клиентов затраты на жесткий диск и потеря хранимых на нем данных несопоставимы с тем ущербом, который они могут

понести в случае несанкционированного доступа к содержимому диска. Чтобы, с одной стороны, обеспечить безопасность такого уровня, а с другой стороны, дать приемлемое решение в случае, когда забыт пароль, в средстве блокировки применяется схема с использованием двух паролей. Один пароль должен быть установлен и использован системным администратором, а другой обычно устанавливается и используется конечным пользователем. Однако если оба пароля забыты, нет никакой возможности разблокировать диск. Поэтому можно безопасно использовать блокировку диска, только скопировав данные с жесткого диска в корпоративную информационную систему или регулярно создавая резервные копии. В случае утраты паролей блокировки диска жесткий диск непригоден для дальнейшего использования. Для тех пользователей, которые не относятся к описанной выше категории клиентов, это может оказаться неоправданным риском. Для тех же пользователей, кто относится к упомянутой категории, такой риск может быть вполне обоснован характером данных, хранимых на жестком диске.

Использование функции DriveLock

При обнаружении нескольких жестких дисков, поддерживающих набор команд ATA Security, в меню Security (безопасность) программы настройки компьютера появится команда DriveLock (Блокировка диска). Здесь предусмотрен ряд параметров, позволяющих устанавливать главный пароль и включать блокировку диска. Чтобы включить блокировку диска, необходим пользовательский пароль. Поскольку начальная настройка блокировки диска обычно выполняется системным администратором, главный пароль должен быть установлен первым. Компания Hewlett-Packard рекомендует системным администраторам устанавливать главный пароль в любом случае, собираются они или не собираются включать блокировку диска. Это даст системным администраторам возможность изменять параметры блокировки диска, если им потребуется впоследствии заблокировать диск. После того как установлен главный пароль, системный администратор может включить блокировку диска или оставить ее отключенной.

Если в системе имеется заблокированный жесткий диск, в ходе проверки POST будет запрошен пароль для снятия блокировки устройства. Если был установлен пароль на включение компьютера и он соответствует пользовательскому паролю на разблокировку устройства, в ходе проверки POST не будет запрашиваться ввод пароля. В противном случае пользователь должен будет ввести пароль блокировки диска. При «холодной» (аппаратной) перезагрузке может использоваться как главный, так и пользовательский пароль. При «теплой» (программной) перезагрузке необходимо ввести пароль, который был введен для разблокирования диска во время предшествовавшей процедуры «холодной» загрузки. У пользователя есть две попытки для ввода правильного пароля. Если ни одна из попыток при «холодной» загрузке не будет успешной, проверка POST будет продолжена, но диск останется недоступным. Если при программной перезагрузке или перезапуске из Windows ни одна из попыток не будет успешной, проверка POST будет остановлена, появится сообщение о необходимости отключения и повторного включения питания.

Приложения DriveLock

Лучше всего использовать средства защиты жесткого диска в корпоративной среде. Системный администратор отвечает за настройку жестких дисков, для которых, помимо всего прочего, будет установлен главный пароль блокировки диска и временный пароль пользователя. В случае, если пользователь забудет пользовательский пароль или оборудование будет передано другому сотруднику, всегда можно использовать главный пароль для переустановки пользовательского пароля и получения доступа к жесткому диску.

Компания Hewlett-Packard рекомендует тем системным администраторам, которые решили включить блокировку диска, разработать также корпоративную политику по установке и эксплуатации главных паролей. Это необходимо для того, чтобы предотвратить возникновения ситуаций, когда сотрудники намеренно или непреднамеренно устанавливают оба пароля на

блокировку диска перед тем, как уйти из компании. В таких случаях жесткий диск окажется полностью непригодным к использованию, и его придется заменить. Аналогично при отсутствии главного пароля системные администраторы могут оказаться лишены доступа к жесткому диску и не смогут выполнять обычную проверку наличия несанкционированного программного обеспечения, а также другие функции по контролю и поддержке.

Пользователям, у которых нет особых требований к безопасности данных, компания Hewlett-Packard не рекомендует включать блокировку диска. К этой категории относятся частные лица и те пользователи, которые, как правило, не держат на жестком диске секретные данные. Для этих пользователей потенциальная потеря жесткого диска в случае, если они забудут оба пароля, значит гораздо больше, чем те данные, для защиты которых предназначено средство блокировки диска. Доступ к программе настройки и средству блокировки диска может быть закрыт с помощью пароля программы настройки. Указав пароль для программы настройки и не сообщая его пользователям, системные администраторы могут предотвратить включение пользователями блокировки диска.

Датчик снятия крышки

Датчик снятия крышки, имеющийся на некоторых моделях, представляет собой сочетание программной и аппаратной технологии, способной предупреждать о снятии крышки или боковой панели компьютера. В следующей таблице описаны три существующих уровня защиты.

Таблица 11-2 Датчик снятия крышки — уровни защиты

Уровень	Параметр	Описание
Уровень 0	Disabled (отключен)	Датчик снятия крышки (Smart Cover Sensor) отключен (по умолчанию).
Уровень 1	Notify User (уведомление пользователя)	Во время перезагрузки компьютера на экране отображается сообщение о том, что была снята крышка или боковая панель компьютера.
Уровень 2	Setup Password (пароль для программы настройки)	Во время перезагрузки компьютера на экране отображается сообщение о том, что была снята крышка или боковая панель компьютера. Чтобы продолжить, необходимо ввести пароль для программы настройки.

ПРИМЕЧАНИЕ. Эти параметры можно изменить с помощью программы настройки компьютера. Для получения дополнительных сведений о настройке компьютера см. *Руководство по использованию служебной программы настройки компьютера (F10)*.

Установка уровня защиты датчика снятия крышки

Чтобы установить уровень защиты датчика снятия крышки, выполните следующие действия.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузка**.
2. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.



ПРИМЕЧАНИЕ. Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. Выберите **Security** (Безопасность) > **Smart Cover** (Крышка компьютера) > **Cover Removal Sensor** (Датчик снятия крышки) и установите необходимый уровень безопасности.
4. Перед выходом из программы выберите **File** (Файл) > **Save Changes and Exit** (Сохранить изменения и выйти).

Блокировка крышки

Блокировка крышки компьютера (Smart Cover Lock) представляет собой управляемый программными средствами замок, имеющийся на некоторых компьютерах Hewlett-Packard. Это устройство предотвращает несанкционированный доступ ко внутренним компонентам. Компьютер поставляется со снятой блокировкой Smart Cover Lock.

- △ **ПРЕДУПРЕЖДЕНИЕ.** Для обеспечения максимального уровня безопасности при блокировке крышки следует убедиться, что установлен пароль для входа в программу настройки компьютера. Пароль для входа в программу настройки компьютера препятствует несанкционированному доступу к ней.

📝 **ПРИМЕЧАНИЕ.** Блокировка крышки (Smart Cover Lock) имеется не на всех компьютерах.

Включение блокировки крышки.

Чтобы активировать и включить блокировку крышки, выполните следующие шаги.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузка**.
2. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

📝 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. Выберите **Security** (Безопасность) > **Smart Cover** (Крышка компьютера) > **Cover Lock** (Блокировка крышки) и установите параметр **Lock** (Включена).
4. Перед выходом из программы выберите **File** (Файл) > **Save Changes and Exit** (Сохранить изменения и выйти).

Выключение блокировки крышки.

1. Включите или перезагрузите компьютер. В операционной системе Windows выберите **Пуск > Завершение работы > Перезагрузка**.
2. Чтобы войти в программу настройки компьютера, после его включения, но до загрузки операционной системы нажмите клавишу **F10**. Можно нажать клавишу **Enter**, чтобы пропустить заставку.

📝 **ПРИМЕЧАНИЕ.** Если своевременно не нажать клавишу **F10**, для входа в программу придется повторно перезагружать компьютер и нажимать клавишу **F10** до загрузки операционной системы.

3. Выберите **Security** (Безопасность) > **Smart Cover** (Крышка компьютера) > **Cover Lock** (Блокировка крышки) > **Unlock** (Отключена).
4. Перед выходом из программы выберите **File** (Файл) > **Save Changes and Exit** (Сохранить изменения и выйти).

Использование аварийного ключа блокировки крышки

Если при включенной блокировке крышки (Smart Cover Lock) ввод пароля для разблокирования невозможен, для открытия крышки компьютера необходим аварийный ключ. Этот ключ может потребоваться в следующих ситуациях:

- Отключение электроэнергии
- Сбой при запуске

- Сбой компонента компьютера (например, процессора или блока питания)
- Забыт пароль

△ **ПРЕДУПРЕЖДЕНИЕ.** Аварийный ключ блокировки компьютера — это специализированное средство, которое можно приобрести в компании HP. Будьте готовы — приобретите этот ключ у уполномоченного представителя или в обслуживающей фирме до того, как он вам понадобится.

Для получения аварийного ключа выполните одно из следующих действий.

- Обратитесь к уполномоченному перепродавцу Hewlett-Packard или в ремонтную службу.
- Позвоните по телефону (список телефонных номеров содержится в документе о предоставлении гарантии).

Для получения дополнительных сведений об использовании аварийного ключа блокировки крышки см. *Справочное руководство по работе с оборудованием*.

Замок с тросиком

На задней панели некоторых моделей компьютера установлен замок с тросиком, обеспечивающий физическую защиту компьютера.

Для получения инструкций с рисунками см. *Справочное руководство по работе с оборудованием*.

Технология идентификации по отпечаткам пальцев

Устраняя необходимость ввода паролей конечными пользователями, технология идентификации по отпечаткам пальцев (HP Fingerprint Identification Technology) повышает сетевую безопасность, упрощает процедуру входа в систему и снижает затраты на управление корпоративными компьютерными сетями. Доступная по цене, эта технология предназначена не только для организаций, использующих высокие технологии и имеющих повышенный уровень секретности.

 **ПРИМЕЧАНИЕ.** Поддержка технологии идентификации по отпечаткам пальцев варьируется в зависимости от модели.

Уведомление о сбоях и восстановлению

Средства уведомления о сбоях и восстановлениях совмещают передовые аппаратные и программные технологии и позволяют предотвратить потерю важных данных и свести к минимуму время вынужденного простоя оборудования.

Если компьютер подключен к сети, управляемой с помощью программы HP Client Manager, уведомление о сбое отправляется приложению управления сетью. С помощью программы HP Client Manager также можно удаленно планировать выполнение программ диагностики, обеспечивая их автоматический запуск на всех управляемых ПК и создание сводного отчета о проверках, закончившихся сбоями.

Система защиты диска

Система защиты диска (DPS, Drive Protection System) – это диагностическое средство, встроенное в жесткие диски некоторых настольных компьютеров Hewlett-Packard. Система DPS

предназначена для обнаружения неполадок, которые могут привести к негарантийной замене жесткого диска.

При сборке компьютеров HP каждый устанавливаемый жесткий диск проверяется с помощью DPS, и на него записываются специальные нестираемые данные. При каждом применении DPS результаты проверки записываются на жесткий диск. Службы технической поддержки могут использовать эти данные для определения причины запуска проверки DPS. Для получения сведений об использовании DPS обратитесь к *Руководству по устранению неполадок*.

Помехозащищенный блок питания

Встроенный помехозащищенный блок питания повышает надежность работы компьютера при наличии помех в сети питания. Этот блок питания выдерживает импульсные помехи амплитудой до 2000 вольт без каких-либо сбоев в работе компьютера или потери данных.

Датчик температуры

Датчик температуры представляет собой программно-аппаратную функцию, следящую за внутренней температурой компьютера. Эта функция отображает предупреждающее сообщение при превышении нормального диапазона, что дает пользователю время принять меры прежде, чем будут повреждены внутренние компоненты или утеряны данные.

△ **ПРЕДУПРЕЖДЕНИЕ.** Повышение температуры может привести к повреждению компьютера или потере данных.

Указатель

- А**
Аварийный ключ, заказ 39
- Б**
Безопасность
 блокировка дисков (DriveLock) 35
 блокировка крышки 38
 датчик снятия крышки 38
 замок с тросиком 40
 параметры 27
 пароль 31
 средства, таблица 28
 технология идентификации по отпечаткам пальцев 40
 ProtectTools Security Manager 7
Блок питания,
 помехозащищенный 41
Блокировка дисков (DriveLock) 35
Блокировка крышки
 аварийный ключ 39
 блокировка 39
 разблокировка 39
Блокировка крышки, заказ аварийного ключа 39
- В**
Ввод
 пароль на включение компьютера 33
 пароль настройки 33
Веб-узел Subscriber's Choice 14
Веб-узлы
 Агент HP Client Automation 3
 Безопасность профессиональных настольных компьютеров HP 8
 загрузка драйверов и программных средств 20
 Загрузка BIOS 15
 каталог HP Client Catalog для Microsoft SMS 10
 пакет Altiris Client Management Suite 10
 поддержка программного обеспечения 25
 служебная программа Proactive Change Notification 14
 технология Intel vPro 11
 Удаленная перезапись ПЗУ 15
 Флэш-ПЗУ 15
 центр HP Client Automation 8
 HP Client Automation Center 9
 HP Client Management Interface 6
 HP Client Manager 3
 HP Client Manager компании Symantec 10
 HP Softpaq Download Manager 6
 HP Support 11
 HP System Software Manager 7
 HPQFlash 16
 Subscriber's Choice 14
Включение блокировки крышки 39
Восстановление программного обеспечения 2
Выключение блокировки крышки 39
- Д**
Датчик снятия крышки
 параметр 38
 уровни защиты 38
Датчик температуры 41
Диагностические средства для жестких дисков 40
Диск, защита 40
Диспетчер клиентов компании Symantec 9
Доступ к компьютеру, контроль 27
- Ж**
Жесткие диски, диагностические средства 40
- З**
Загрузочное устройство
 создание 20
 USB-устройство флэш-памяти 20
Заказ аварийного ключа 39
Замок с тросиком 40
Защита жестких дисков 40
- И**
Изменение пароля 34
Изменения, уведомление 13
Интернет-адреса. См. раздел Веб-узлы
- К**
Клонирование, программные средства 2
Кнопка питания (двухпозиционная) 24
Кнопка питания, настройка 24
Контроль доступа к компьютеру 27

Н

Настройка

- копирование на несколько компьютеров 19
- копирование на один компьютер 18
- начальная 2

Настройка кнопки питания 24

Настройка компьютера, копирование 18

Национальные символы-разделители, используемые на клавиатуре 35

Начальная настройка 2

О

Образ предварительно установленного программного обеспечения 2

Операционные системы, поддержка по смене 25

Отраслевые стандарты 26

П

Пароль

- безопасность 31
- включение 32, 33
- изменение 34
- настройка 32, 33
- сброс 35
- удаление 34

Пароль на включение компьютера

- ввод 33
- изменение 34
- параметр 32
- удаление 34

Пароль настройки

- ввод 33
- изменение 34
- удаление 34

Помехозащищенный блок питания 41

Предзагрузочная среда выполнения (PXE) 4

Программное обеспечение восстановления 2
диспетчер HP Client Manager компании Symantec 9

диспетчер HP System Software Manager 6

интеграция 2

каталог HP Client Catalog для продуктов Microsoft System Center и SMS 10

пакет Altiris Client Management Suite 10

развертывание 2

система защиты диска 40

служебная программа Proactive Change Notification (PCN) 13

средства обновления и управления 5

средства отслеживания 27

Технология удаленного управления 10

удаленная установка системы 4

HP Client Automation Starter, Standard Edition и Enterprise Edition 8

HP Client Management Interface 5

HP ProtectTools Security Manager 7

Verdiem Surveyor 13

Р

Развертывание, программные средства 2

Разделители, таблица 35

Режим аварийного восстановления загрузочного блока 17

Режим аварийного восстановления, загрузочный блок 17

С

Сброс паролей 35

Служебная программа HPQFlash 15

Служебная программа Proactive Change Notification (PCN) 13

Смена операционной системы, поддержка 25

Средства отслеживания активов 27

Т

Температура внутри компьютера 41

Температура, внутри компьютера 41

Технология идентификации по отпечаткам пальцев 40

Технология удаленного управления 10

У

Уведомление о сбоях и восстановлению 40

Уведомление об изменениях 13

Удаление пароля 34

Удаленная перезапись ПЗУ 15

Удаленная установка 4

Удаленная установка системы 4

Устаревшие решения 14

Ф

Флэш-ПЗУ 15

А

Altiris

пакет Client Management Suite 10

В

BIOS

режим аварийного восстановления загрузочного блока 17
служебная программа HPQFlash 15
удаленная перезапись ПЗУ 15

С

Client Management Interface 5

Н

HP

диспетчер клиентов компании Symantec 9
интерфейс управления клиентом 5

каталог Client Catalog для
продуктов Microsoft System
Center и SMS 10
Client Automation Starter,
Standard Edition и Enterprise
Edition 8
ProtectTools Security
Manager 7
System Software Manager 6
HP Client Automation Enterprise
Edition 8
HP Client Manager 3

P

ProtectTools Security Manager 7
PXE (Предзагрузочная среда
выполнения) 4

S

Setup password (пароль
программы настройки)
параметр 32
System Software Manager 6

U

USB-устройство флэш-памяти,
загрузочное 20, 22

V

Verdiem Surveyor 13