

# Безопасность

## Руководство пользователя

© Copyright 2008 Hewlett-Packard  
Development Company, L.P.

Windows является товарным знаком  
корпорации Майкрософт,  
зарегистрированным в США.

Информация, содержащаяся в  
настоящем документе, может быть  
изменена без предварительного  
уведомления. 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 ошибки  
или опечатки, которые могут содержаться  
в настоящем документе.

Третье издание: июнь 2008 г.

Номер документа: 463798-253

### **Уведомление о продукте**

В данном руководстве описываются  
функции, являющиеся общими для  
большинства моделей. Некоторые  
функции на вашем компьютере могут  
быть недоступны.

---

# Содержание

## 1 Защита компьютера

### 2 Использование паролей

Установка паролей Windows .....	4
Установка паролей в программе настройки компьютера .....	5
Пароль администратора для доступа к BIOS .....	6
Управление паролем администратора для доступа к BIOS .....	6
Ввод пароля администратора для доступа к BIOS .....	7
Использование пароля DriveLock, устанавливаемого в программе настройки компьютера .....	8
Установка пароля DriveLock .....	8
Ввод пароля DriveLock .....	9
Изменение пароля DriveLock .....	9
Снятие защиты DriveLock .....	10
Использование автоматической защиты DriveLock, устанавливаемой в программе настройки компьютера .....	11
Ввод пароля для автоматической защиты DriveLock .....	11
Снятие автоматической защиты DriveLock .....	11

### 3 Использование функций безопасности программы настройки компьютера

Устройства безопасности .....	13
Просмотр сведений о системе в программе настройки компьютера .....	15
Использование идентификаторов компьютера в программе настройки компьютера .....	16

## 4 Использование антивирусного программного обеспечения

## 5 Использование брандмауэра

## 6 Установка критических обновлений системы безопасности

## 7 Использование диспетчера безопасности HP ProtectTools (только на некоторых моделях)

## 8 Установка замка с тросиком



# 1 Защита компьютера

 **ПРИМЕЧАНИЕ.** Средства безопасности предназначены для ограничения возможностей злоумышленников. Эти средства защиты не устраняют полностью угрозу ненадлежащего использования или кражи компьютера.

**ПРИМЕЧАНИЕ.** Этот компьютер поддерживает CompuTrace, безопасную интерактивную службу отслеживания и восстановления, доступную в некоторых регионах. Если компьютер украден, CompuTrace может обнаружить его, когда злоумышленник выйдет в сеть Интернет. Чтобы использовать CompuTrace, необходимо приобрести программное обеспечение и подписаться на эту услугу. Для получения сведений о заказе программного обеспечения CompuTrace посетите веб-узел HP по адресу <http://www.hpshopping.com>.

Средства обеспечения безопасности, предоставляемые с компьютером, помогают защитить компьютер, личные сведения и данные от различных опасностей. То, каким образом используется компьютер, определяет необходимость использования тех или иных средств безопасности.

ОС Windows® предлагает определенные средства обеспечения безопасности. Дополнительные средства обеспечения безопасности перечислены в таблице ниже. Большинство из них можно настроить в программе настройки компьютера.

Опасность	Функция безопасности
Несанкционированное использование компьютера	Диспетчер безопасности HP ProtectTools, а также пароль, смарт-карта и/или устройство считывания отпечатков пальцев.
Несанкционированный доступ к программе настройки компьютера (f10)	Пароль администратора для доступа к BIOS в программе настройки компьютера*
Несанкционированный доступ к содержимому жесткого диска	Установка пароля DriveLock в программе настройки компьютера*
Несанкционированный запуск с оптического диска, дискеты или загрузка через внутренний сетевой адаптер	Функция Boot options (Параметры загрузки) в программе настройки компьютера*
Несанкционированный доступ к учетным данным пользователя в Windows	Диспетчер безопасности HP ProtectTools
Несанкционированный доступ к данным	<ul style="list-style-type: none"><li>• Брандмауэр</li><li>• Обновления Windows</li><li>• Шифрование диска для HP ProtectTools</li></ul>
Несанкционированный доступ к параметрам программы настройки компьютера и другим идентификационным сведениям системы	Пароль администратора для доступа к BIOS в программе настройки компьютера*

---

**Опасность****Функция безопасности**

---

Кража компьютера

Гнездо для замка с тросиком (используется для поставляемого дополнительно замка с тросиком)

---

\*Программа настройки компьютера относится к числу предварительно установленных служебных программ на основе ПЗУ, которую можно использовать, даже когда операционная система не работает или не загружается. Для переходов и выбора пунктов в программе настройки компьютера можно использовать указывающее устройство (сенсорную панель, указку или мышь USB) или клавиатуру.

---

---

## 2 Использование паролей

В большинстве функций безопасности используются пароли. Установив пароль, запишите его и храните в безопасном месте отдельно от компьютера. Обратите внимание на следующие замечания.

- Пароль к программе настройки и пароль DriveLock устанавливаются в программе настройки компьютера. Управление ими осуществляется через BIOS системы.
- В программе настройки компьютера можно включить использование пароля встроенной системы безопасности, являющегося паролем диспетчера безопасности HP ProtectTools, после чего он будет выполнять функцию пароля BIOS помимо своих обычных функций для HP ProtectTools. Для использования пароля встроенной системы безопасности необходима дополнительная микросхема встроенной системы безопасности.
- Пароли Windows устанавливаются только в операционной системе Windows.
- Если забыт пароль администратора для доступа к BIOS, установленный в программе настройки компьютера, для доступа к программе можно использовать HP SpareKey.
- Если забыты оба пароля DriveLock (пользовательский и главный), защищенный паролями жесткий диск окончательно блокируется и больше не может использоваться.

В программе настройки компьютера и в операционной системе Windows можно использовать одни и те же пароли. Кроме того, можно использовать один и тот же пароль для нескольких функций в программе настройки компьютера.

Советы по созданию и хранению паролей:

- при создании пароля учитывайте требования конкретной программы;
- запишите пароль и храните его в надежном месте отдельно от компьютера;
- не храните пароль в файле на компьютере.

В следующей таблице приведен список часто используемых паролей администратора BIOS и операционной системы Windows, а также описания их функций.

# Установка паролей Windows

Пароли Windows	Функция
Пароль администратора*	Ограничение доступа к учетным данным администратора Windows.
Пароль пользователя*	Ограничение доступа к учетной записи пользователя в Windows.

\*Для получения сведений об установке пароля администратора Windows или пароля пользователя Windows выберите **Пуск > Справка и поддержка**.

## Установка паролей в программе настройки компьютера

Пароли администратора для доступа к BIOS	Функция
Пароль администратора для доступа к BIOS	Ограничение доступа к программе настройки компьютера.
Главный пароль DriveLock	Ограничение доступа ко внутреннему жесткому диску, защищенному функцией DriveLock. Он также используется для удаленной защиты DriveLock. Этот пароль устанавливается в разделе DriveLock Passwords (Пароли DriveLock) в ходе включения функции.
Пользовательский пароль DriveLock	Ограничение доступа ко внутреннему жесткому диску, защищенному функцией DriveLock, пароль устанавливается в разделе DriveLock passwords (Пароли DriveLock) в ходе включения функции.
Пароль встроенной системы безопасности TPM	<p>Если этот пароль используется как пароль администратора BIOS, он ограничивает доступ к данным на компьютере при включении, перезагрузке и выводе компьютера из спящего режима.</p> <p>Для поддержки данной функции безопасности необходима дополнительная микросхема встроенной системы безопасности.</p>

## Пароль администратора для доступа к BIOS

Пароль администратора для доступа к BIOS в программе настройки компьютера защищает параметры настройки и сведения о системе, установленные в ней. После того, как установлен этот пароль, его необходимо вводить при доступе к программе настройки компьютера и внесении изменений с ее помощью.

Обратите внимание на следующие характеристики пароля администратора для доступа к BIOS.

- Этот пароль не связан с паролем администратора Windows, хотя оба пароля могут быть одинаковыми.
- Пароль при установке, вводе, смене или удалении не отображается.
- Пароль следует вводить при помощи тех же клавиш, при помощи которых он был установлен. Например, пароль администратора для доступа к BIOS, установленный с помощью цифровых клавиш клавиатуры, не опознается, если его ввести с помощью клавиш встроенной цифровой панели.
- Пароль может иметь длину до 32 символов и состоять из букв и цифр. Регистр букв не учитывается, если обратное не назначено администратором.

## Управление паролем администратора для доступа к BIOS

Пароль администратора для доступа к BIOS устанавливается, изменяется и удаляется в программе настройки компьютера.

Чтобы установить или изменить этот пароль в программе настройки компьютера, выполните следующие действия.

1. Включите или перезагрузите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **Change Password** (Изменить пароль) и нажмите клавишу **enter**.
4. При появлении запроса укажите текущий пароль.
5. При появлении запроса укажите новый пароль.
6. При появлении запроса еще раз введите новый пароль для подтверждения.
7. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

Изменения начинают действовать после перезагрузки компьютера.

Чтобы удалить этот пароль в программе настройки компьютера, выполните следующие действия.

1. Включите или перезагрузите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **Change Password** (Изменить пароль) и нажмите клавишу **enter**.
4. При появлении запроса укажите текущий пароль.
5. При появлении запроса на ввод нового пароля оставьте поле пустым и нажмите клавишу **enter**.
6. Прочитайте предупреждение. Чтобы продолжить, выберите **YES** (Да).
7. При появлении запроса на повторный ввод нового пароля оставьте поле пустым и нажмите клавишу **enter**.
8. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

Изменения начинают действовать после перезагрузки компьютера.

## Ввод пароля администратора для доступа к BIOS

При появлении запроса **BIOS administrator password** (Пароль администратора для доступа к BIOS) введите пароль (при помощи тех же клавиш, при помощи которых он был установлен) и нажмите клавишу **enter**. После трех неудачных попыток ввода пароля администратора для доступа к BIOS необходимо перезапустить компьютер, чтобы попытаться ввести пароль еще раз.

# Использование пароля DriveLock, устанавливаемого в программе настройки компьютера

△ **ПРЕДУПРЕЖДЕНИЕ.** Во избежание необратимой блокировки жесткого диска, защищенного функцией DriveLock, запишите главный и пользовательский пароли DriveLock и храните их в безопасном месте отдельно от компьютера. Если забыты пароли DriveLock, жесткий диск блокируется, и использовать его будет невозможно.

Функция DriveLock предотвращает несанкционированный доступ к содержимому жесткого диска. Функцию DriveLock можно использовать только для внутренних жестких дисков компьютера. После установки для жесткого диска защитной функции DriveLock необходимо вводить пароль DriveLock при обращении к жесткому диску. Чтобы иметь возможность обращаться к жесткому диску с использованием паролей DriveLock, диск должен быть установлен в компьютере или в усовершенствованном репликаторе портов.

Чтобы использовать функцию DriveLock для защиты диска, нужно настроить главный и пользовательский пароли в программе установки компьютера. При использовании функции DriveLock обратите внимание на следующие замечания.

- Если для защиты диска используется функция DriveLock, доступ к нему может быть осуществлен только после ввода пользовательского или главного пароля.
- Пользовательский пароль должен знать тот человек, который ежедневно работает с защищенным жестким диском. Главный пароль должен знать системный администратор или пользователь.
- Пользовательский и главный пароли могут совпадать.
- Удалить пользовательский или главный пароль можно, только сняв с диска защиту DriveLock. Защита функцией DriveLock может быть снята с диска только с помощью главного пароля.

## Установка пароля DriveLock

Чтобы установить или изменить пароль DriveLock в программе настройки компьютера, выполните следующие действия.

1. Включите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **DriveLock passwords** (Пароли DriveLock) и нажмите клавишу **enter**.
4. С помощью указывающего устройства выберите жесткий диск, который нужно защитить.  
— или —  
С помощью клавиш со стрелками выберите жесткий диск, который нужно защитить, и нажмите клавишу **enter**.
5. Прочитайте предупреждение. Чтобы продолжить, выберите **YES** (Да).
6. Укажите главный пароль в полях **New password** (Новый пароль) и **Verify new password** (Подтверждение нового пароля) и нажмите клавишу **enter**.

7. Укажите пользовательский пароль в полях **New password** (Новый пароль) и **Verify new password** (Подтверждение нового пароля) и нажмите клавишу **enter**.
8. Чтобы подтвердить защиту выбранного диска функцией DriveLock, введите DriveLock в поле подтверждения и нажмите клавишу **enter**.

 **ПРИМЕЧАНИЕ.** При подтверждении DriveLock учитывается регистр.

9. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

Изменения начинают действовать после перезагрузки компьютера.

## Ввод пароля DriveLock

Убедитесь, что жесткий диск установлен в компьютер (а не в дополнительную станцию расширения и не во внешний отсек MultiBay).

При появлении запроса **DriveLock Password** (Пароль DriveLock), введите пароль пользователя или главный пароль (с помощью тех же клавиш, которые использовались при установке пароля) и нажмите клавишу **enter**.

После двух неудачных попыток ввода пароля необходимо перезапустить компьютер, чтобы попытаться ввести пароль еще раз.

## Изменение пароля DriveLock

Чтобы изменить пароль DriveLock в программе настройки компьютера, выполните следующие действия.

1. Включите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **DriveLock passwords** (Пароли DriveLock) и нажмите клавишу **enter**.

4. С помощью указывающего устройства выберите внутренний жесткий диск.

— или —

С помощью клавиш со стрелками выберите внутренний жесткий диск и нажмите клавишу **enter**.

5. С помощью указывающего устройства или клавиш со стрелками выберите пароль, который нужно изменить.

6. Укажите текущий пароль в поле **Old password** (Старый пароль), укажите новый пароль в полях **New password** (Новый пароль) и **Verify new password** (Подтверждение нового пароля) и нажмите клавишу **enter**.
7. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

Изменения начинают действовать после перезагрузки компьютера.

## Снятие защиты DriveLock

Чтобы снять защиту DriveLock в программе настройки компьютера, выполните следующие действия.

1. Включите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **DriveLock password** (Пароль DriveLock) и нажмите клавишу **enter**.
4. С помощью указывающего устройства или клавиш со стрелками выберите внутренний жесткий диск и нажмите клавишу **enter**.
5. С помощью указывающего устройства или клавиш со стрелками выберите **Disable protection** (Отключить защиту).
6. Введите главный пароль и нажмите клавишу **enter**.
7. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

Изменения начинают действовать после перезагрузки компьютера.

# Использование автоматической защиты DriveLock, устанавливаемой в программе настройки компьютера

Если на компьютере работают несколько пользователей, можно установить пароль для автоматической защиты DriveLock. При установке пароля для автоматической защиты DriveLock происходит создание главного и пользовательского паролей DriveLock случайным образом. Когда какой-либо пользователь проходит проверку учетных данных, эти же пароли DriveLock используются для разблокирования диска.

 **ПРИМЕЧАНИЕ.** Для доступа к функции автоматической защиты DriveLock требуется пароль администратора BIOS.

## Ввод пароля для автоматической защиты DriveLock

Чтобы включить пароль для автоматической защиты DriveLock в программе настройки компьютера, выполните следующие действия.

1. Включите или перезагрузите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **Automatic DriveLock** (Автоматическая защита DriveLock) и нажмите клавишу **enter**.
4. С помощью указывающего устройства или клавиш со стрелками выберите внутренний жесткий диск и нажмите клавишу **enter**.
5. Прочитайте предупреждение. Чтобы продолжить, выберите **YES** (Да).
6. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

## Снятие автоматической защиты DriveLock

Чтобы снять защиту DriveLock в программе настройки компьютера, выполните следующие действия.

1. Включите или перезагрузите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **Automatic DriveLock** (Автоматическая защита DriveLock) и нажмите клавишу **enter**.
4. С помощью указывающего устройства или клавиш со стрелками выберите внутренний жесткий диск и нажмите клавишу **enter**.

5. С помощью указывающего устройства или клавиш со стрелками выберите **Disable protection** (Отключить защиту).
6. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

---

## 3 Использование функций безопасности программы настройки компьютера

### Устройства безопасности

Можно включить или отключить системные устройства с помощью следующих меню в программе настройки компьютера.

- Boot Options (Параметры загрузки)
- Device Configurations (Настройка устройств)
- Built-In Device Options (Параметры встроенных устройств)
- Port Options (Параметры портов)

Чтобы отключить или снова включить системное устройство в программе настройки компьютера, выполните следующие действия.

1. Включите или перезагрузите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите **esc**, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **System Configuration** (Настройка системы) > **Boot Options** (Параметры загрузки) или **System Configuration** (Настройка системы) > **Device Configurations** (Настройка устройств), или **System Configuration** (Настройка системы) > **Built-In Device Options** (Параметры встроенных устройств), или **System Configuration** (Настройка системы) > **Port Options** (Параметры портов).
4. Нажмите клавишу **enter**.
5. Чтобы отключить параметр, с помощью указывающего устройства выберите **Disabled** (Отключено) рядом с параметром.  
— или —  
С помощью клавиш со стрелками выберите **Disabled** (Отключено) рядом с параметром и нажмите клавишу **enter**.
6. Чтобы снова включить параметр, с помощью указывающего устройства выберите **Enabled** (Включено) рядом с параметром.

— или —

С помощью клавиш со стрелками выберите **Enabled** (Включено) рядом с параметром и нажмите клавишу **enter**.

7. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

Изменения начинают действовать после перезагрузки компьютера.

# Просмотр сведений о системе в программе настройки компьютера

При просмотре сведений о системе в программе настройки компьютера пользователь получает два типа сведений о системе:

- Идентификационные сведения о модели компьютера и об аккумуляторных батареях.
- Технические характеристики процессора, оперативной и кэш-памяти, ПЗУ, видеокарты и контроллера клавиатуры.

Чтобы просмотреть эти общие сведения о системе в программе настройки компьютера, выполните следующие действия.

1. Включите или перезагрузите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **File (Файл) > System Information (Сведения о системе)** и нажмите клавишу **enter**.

---

 **ПРИМЕЧАНИЕ.** Для предотвращения несанкционированного доступа к этим сведениям необходимо установить пароль администратора для доступа к BIOS в программе настройки компьютера.

---

## Использование идентификаторов компьютера в программе настройки компьютера

Пункт меню System IDs (Идентификаторы компьютера) в программе настройки компьютера позволяет ввести и просмотреть инвентарный номер компьютера и сведения о владельце.

 **ПРИМЕЧАНИЕ.** Для предотвращения несанкционированного доступа к этим сведениям необходимо установить пароль администратора для доступа к BIOS в программе настройки компьютера.

Для управления этой функцией в программе настройки компьютера выполните следующие действия.

1. Включите или перезагрузите компьютер и нажмите клавишу **esc**, когда в нижней части экрана появится сообщение «Press the ESC key for Startup Menu» (Нажмите esc, чтобы открыть меню запуска).
2. Нажмите клавишу **f10**, чтобы войти в программу настройки BIOS.
3. С помощью указывающего устройства или клавиш со стрелками выберите **Security** (Безопасность) > **System IDs** (Идентификаторы компьютера) и нажмите клавишу **enter**.
4. С помощью указывающего устройства или клавиш со стрелками выберите **Notebook Asset Tag** (Инвентарный номер портативного компьютера) или **Notebook Ownership Tag** (Сведения о владельце портативного компьютера) и укажите эту информацию.
5. По окончании нажмите клавишу **enter**.
6. Чтобы сохранить изменения и выйти из программы настройки компьютера, щелкните **Save** (Сохранить) в нижнем левом углу и следуйте указаниям на экране.

— или —

С помощью клавиш со стрелками выберите **File** (Файл) > **Save changes and exit** (Сохранить изменения и выйти), а затем нажмите клавишу **enter**.

Изменения начинают действовать после перезагрузки компьютера.

---

## 4 Использование антивирусного программного обеспечения

При работе с электронной почтой, сетью или при подключении к Интернету компьютер может подвергнуться воздействию компьютерных вирусов. Компьютерные вирусы способны повредить операционную систему, установленные и служебные программы или привести к их неправильной работе.

Антивирусное программное обеспечение способно обнаружить и уничтожить большинство вирусов, а также устранить вызванные ими неполадки. Необходимо обновлять антивирусное программное обеспечение, чтобы защититься от вновь появляющихся вирусов.

На данном компьютере предварительно установлено либо предварительно загружено антивирусное программное обеспечение McAfee Total Protection.

Если антивирусное программное обеспечение предварительно установлено, выберите **Пуск > Все программы > McAfee > Managed Services** (Управляемые службами) > **Total Protection** (Полная защита).

Если программное обеспечение предварительно загружено, выберите **Пуск > Все программы > HP Software Setup** (Установка программного обеспечения HP) и следуйте экранным инструкциям по загрузке программного обеспечения **McAfee Total Protection**.

Чтобы получить дополнительную информацию о компьютерных вирусах, введите слово **вирусы** в окне поиска в центре справки и поддержки.

---

## 5 Использование брандмауэра

При работе с электронной почтой, сетью или при подключении к Интернету существует возможность несанкционированного доступа посторонних лиц к компьютеру, личным файлам и сведениям о пользователе. Брандмауэр, установленный на данном компьютере, обеспечивает конфиденциальность. На данном компьютере предварительно установлено антивирусное программное обеспечение McAfee Total Protection. Чтобы открыть это программное обеспечение, выберите **Пуск > Все программы > McAfee > Managing Services (Управление службами) > Total Protection** (Полная защита).

В число функций брандмауэра входит регистрация и создание отчетов о работе в сети, а также автоматическое наблюдение за всем входящим и исходящим трафиком. Для получения дополнительных сведений обратитесь к инструкциям производителя программного обеспечения. Эти инструкции можно найти на прилагаемом к программному обеспечению компакт-диске или на веб-узле производителя.

---

 **ПРИМЕЧАНИЕ.** При некоторых обстоятельствах брандмауэр может блокировать доступ к Интернет-играм, оказывать помехи выводу на печать или совместному использованию файлов в сети либо блокировать вложения в электронные сообщения, получаемые из надежных источников. Чтобы временно решить эту проблему, отключите брандмауэр, выполните требуемую задачу, а затем снова включите брандмауэр. Чтобы полностью решить эту проблему, перенастройте брандмауэр нужным образом и отрегулируйте политики и параметры других систем обнаружения вторжений. Для получения дополнительных сведений обратитесь к администратору сети или в отдел ИТ.

---

---

## 6 Установка критических обновлений системы безопасности

---

△ **ПРЕДУПРЕЖДЕНИЕ.** Корпорация Майкрософт выполняет отправку уведомлений о критических обновлениях. Чтобы защитить компьютер от брешей в системе безопасности и компьютерных вирусов, устанавливайте все критические обновления Майкрософт, как только появляется уведомление о их наличии.

---

Обновления операционной системы и другого программного обеспечения могут быть выпущены уже *после* отгрузки компьютера. Чтобы убедиться, что все доступные обновления установлены, необходимо следовать приведенным ниже рекомендациям.

- Запускать службу Windows Update каждый месяц для установки последнего программного обеспечения, выпущенного корпорацией Майкрософт.
- Получать обновления по мере их появления с веб-узла корпорации Майкрософт по ссылке на обновления в центре справки и поддержки.

---

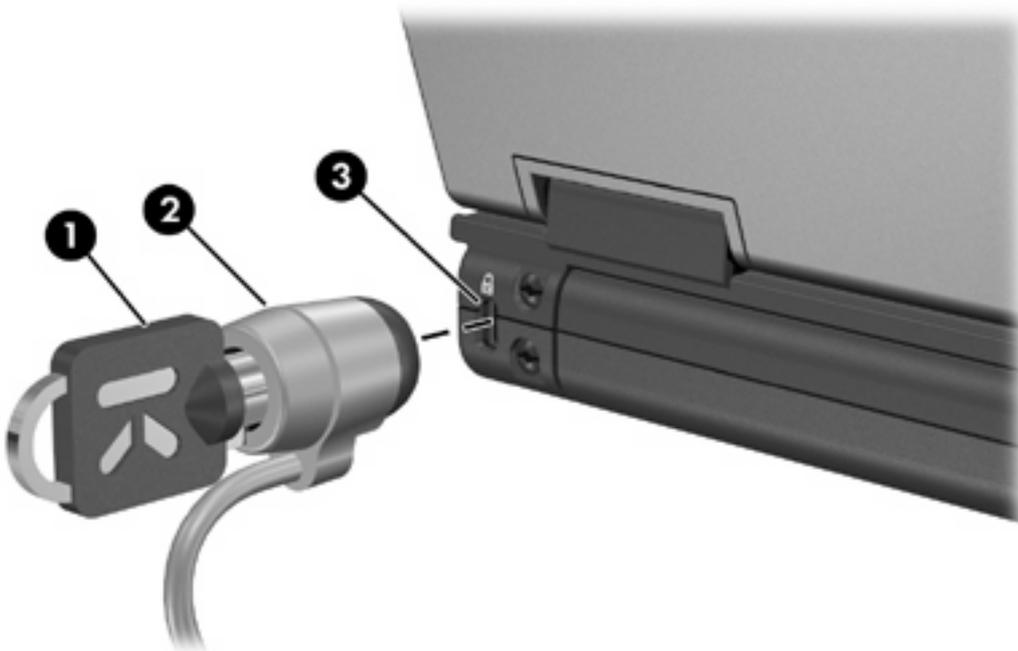
## 7 Использование диспетчера безопасности HP ProtectTools (только на некоторых моделях)

На некоторых моделях компьютеров установлен диспетчер безопасности HP ProtectTools. Доступ к данному программному обеспечению предоставляется на панели управления Windows. Функции безопасности этой программы помогают защитить компьютер, сети и важные данные от несанкционированного доступа. Для получения дополнительных сведений см. справку HP ProtectTools.

## 8 Установка замка с тросиком

 **ПРИМЕЧАНИЕ.** Замок с тросиком — это средство защиты, однако он не может помешать ненадлежащему использованию или краже компьютера.

1. Оберните тросик замка вокруг надежно закрепленного объекта.
2. Вставьте ключ (1) в замок (2).
3. Вставьте замок с тросиком в гнездо (3) на компьютере и закройте замок ключом.



 **ПРИМЕЧАНИЕ.** Ваш компьютер может отличаться от изображенного на рисунках, приведенных в данной главе. Расположение гнезда замка с тросиком может различаться в зависимости от модели компьютера.

---

# Указатель

## А

Автоматическая защита

- DriveLock, пароль  
ввод 11
- удаление 11

Антивирусное программное  
обеспечение 17

## Б

Безопасность, защита  
компьютера 1

Брандмауэр 18

## Д

Диспетчер безопасности HP  
ProtectTools 20

## З

Замок с тросиком 21

Защита устройств 13

## К

Критические обновления,  
программное обеспечение 19

## П

Пароли

- администратор 4
- администратор BIOS 6
- пользователь 4
- DriveLock 8

Пароль администратора 4

Пароль пользователя 4

Пароль DriveLock

- ввод 9
- изменение 9
- описание 8
- снятие 10
- установка 8

Программа настройки  
компьютера

- защита устройств 13
- пароль администратора для  
доступа к BIOS 6
- пароль DriveLock 8

Программное обеспечение  
антивирусное 17

- брандмауэр 18
- критические обновления 19

## Т

Тросик, безопасность 21

## М

McAfee Total Protection 17, 18

