Официальный технический документ

HP Sure Start

Автоматическая защита и восстановление на уровне BIOS

Май 2018 г.

Содержание

Введение

HP Sure Start автоматически выполняет обнаружение, устранение и восстановление после атаки или повреждения BIOS, без привлечения ИТ-специалистов и практически без прерывания работы пользователей. При каждом включении компьютера HP Sure Start автоматически проверяет целостность кода BIOS, обеспечивая защиту компьютера от атак злоумышленников. После того, как компьютер готов к работе, функция обнаружения вторжений во время выполнения выполняет непрерывный мониторинг памяти. В случае атаки компьютер может выполнить самовосстановление с помощью изолированной «золотой копии» BIOS менее чем за минуту.

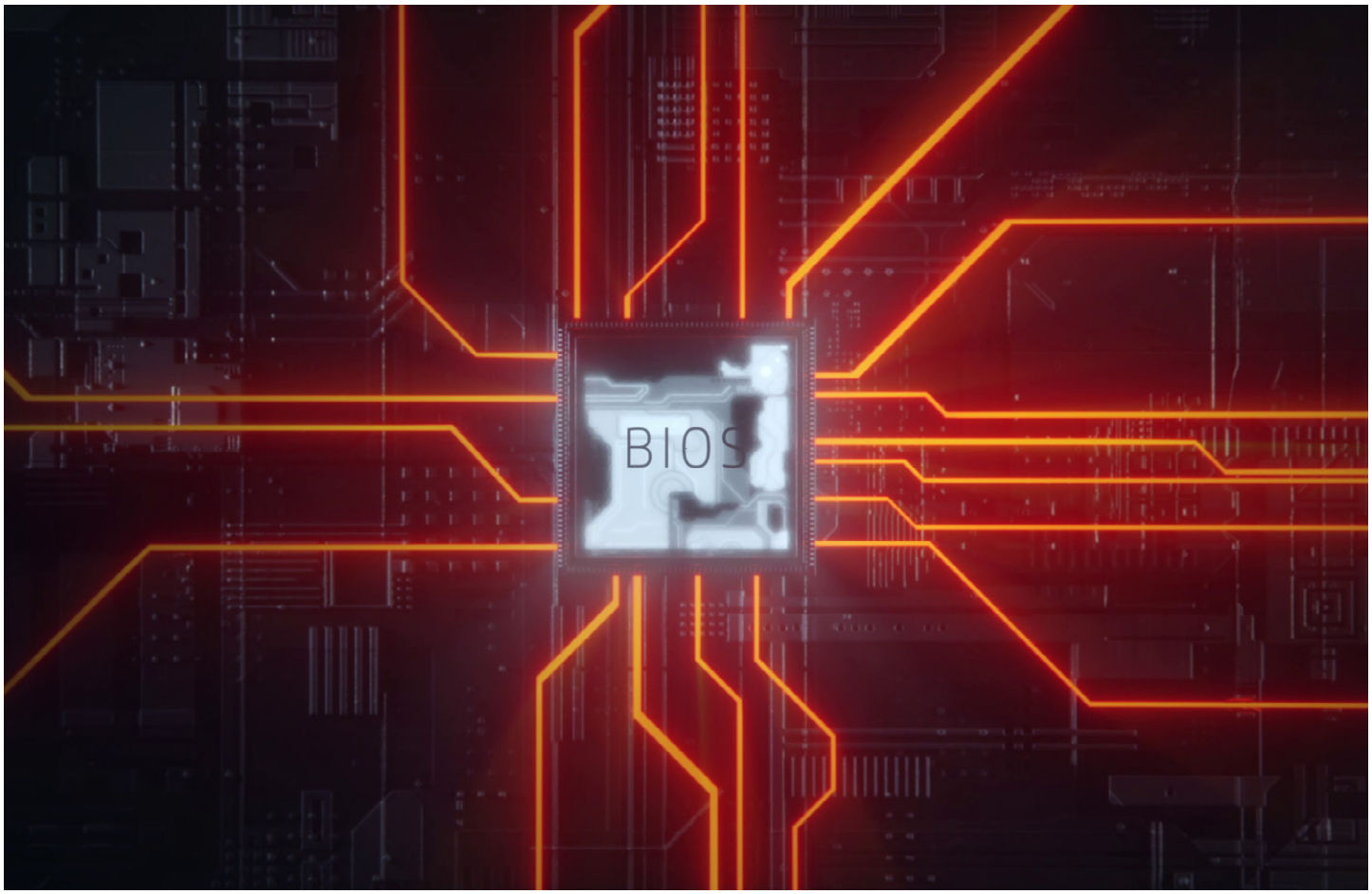
Почему важно обеспечить защиту BIOS?

В современном мире роль Интернета постоянно возрастает. Одновременно увеличивается частота и сложность кибер-атак, направленных против микропрограммного и аппаратного обеспечения клиентских устройств. Еще недавно инструменты и техники атак на микропрограммное обеспечение существовали только в теории и считались доступными только госструктурам. Однако оказалось, что эти инструменты и техники не только существуют, но доступны самым широким слоям общества.

Микропрограммное обеспечение устройства (или BIOS) является привлекательной мишенью для злоумышленников из-за потенциальных преимуществ, которые предоставляет нарушителю успешный взлом:

- Стойкость: микропрограммное обеспечение расположено в энергонезависимой памяти на монтажной плате, и его нельзя удалить путем простого стирания жесткого диска.
- Контроль: микропрограммное обеспечение связано с самым высоким уровнем доступа, оно находится за пределами домена ОС, что дает вредоносному ПО возможность действовать независимо от ОС.
- Скрытность: микропрограммное обеспечение занимает область памяти, абсолютно недоступную для операционной системы и системного ПО; поэтому оно не сканируется и не обнаруживается антивирусными программами.
- Сложность восстановления: все перечисленное выше делает восстановление после заражения такого типа практически невозможным без обращения к техническому обслуживанию, которое включает замену системной платы.

Идеальное решение для защиты устройств от данного типа атак разработано на основе аппаратного обеспечения с использованием принципов «киберустойчивости». Согласно этим принципам, предвидеть и предотвратить каждую потенциальную атаку чрезвычайно сложно, если не невозможно. Идеальное решение не только обеспечивает усовершенствованную защиту от вредоносного ПО, но также включает в себя аппаратные функции обнаружения успешной атаки и восстановления после нее.



HP Sure Start обеспечивает превосходную защиту микропрограммного обеспечения

HP Sure Start — это уникальная, революционная технология HP, обеспечивающая усовершенствованную защиту микропрограммного обеспечения и отказоустойчивость для компьютеров HP. Она использует аппаратное применение посредством HP Endpoint Security Controller (HP ESC), обеспечивая защиту BIOS, качество которой значительно превышает отраслевые стандарты, и гарантирует загрузку только подлинной HP BIOS. Кроме того, при попытке взлома BIOS, микропрограммного обеспечения или исполняемого кода System Management Mode (SMM) BIOS, HP Sure Start обеспечивает их восстановление с использованием защищенной резервной копии.

Обзор функций HP Sure Start

- Применение подлинного микропрограммного обеспечения ядра платформы HP и защита от взлома: аппаратное применение системной загрузки через HP Endpoint Security Controller обеспечивает загрузку только подлинного и немодифицированного микропрограммного обеспечения HP и HP BIOS
- Мониторинг состояния микропрограммного обеспечения и соответствия нормативно-правовым требованиям: регистрация событий, связанных с состоянием микропрограммы, через изолированный HP Endpoint Security Controller; представляет состояние микропрограммного обеспечения платформы вместе с любыми отклонениями от нормы, которые могут указывать на предотвращенные атаки
- Самовосстановление: автоматическое исправление повреждений HP BIOS и микропрограммного обеспечения HP с помощью их изолированных резервных копий в HP Endpoint Security Controller
- Защита настройки BIOS: расширяет защиту кода BIOS с помощью HP Endpoint Security Controller, включая резервное копирование HP ESC и проверку целостности всех параметров BIOS, заданных администратором или пользователями
- Функция Runtime Intrusion Detection: непрерывный мониторинг критически важного кода BIOS в памяти во время выполнения (SMM) без остановки работы ОС
- Безопасность ключей защищенной загрузки: значительно улучшает защиту баз данных и ключей, хранящихся в BIOS, которые критически важны для целостности функции защищенной загрузки ОС, в отличие от стандартной реализации UEFI BIOS
- Защищенное хранилище: HP Sure Start использует надежные криптографические методы для хранения параметров BIOS, учетных данных пользователей и других настроек в аппаратном обеспечении HP Endpoint Security Controller для защиты целостности, обнаружения вторжений и обеспечения конфиденциальности этих данных
- Защита микропрограммного обеспечения Intel® Management Engine: усовершенствованные защита и восстановление микропрограммного обеспечения Intel Management Engine
- Удобство управления: администраторы могут управлять возможностями HP Sure Start с помощью подключаемого модуля Manageability Integration Kit (MIK) для Microsoft® System Center Configuration Manager (SCCM)

Обзор дополнительных возможностей каждого поколения HP Sure Start представлен в Приложении A на странице 11.

Сертификация средства безопасности сторонними организациями

Аппаратное обеспечение HP Endpoint Security Controller, используемое в HP Sure Start, прошло оценку безопасности сторонней организацией и получило сертификат, подтверждающий, что оно обеспечивает аппаратное применение только авторизованного микропрограммного обеспечения для запуска на целевом компьютере.[1]

Гарантия заявленной работы решения является решающим фактором при выборе продуктов для обеспечения безопасности. Поскольку репутация качества распространяется быстро и повсеместно, компания HP подвергла внутренние механизмы HP Endpoint Security Controller проверке и тестированию в независимой аккредитованной лаборатории, чтобы подтвердить заявленные рабочие характеристики решения на основании общедоступных критериев, методологии и процессов.

«Киберустойчивое» исполнение

Решение HP Sure Start не только обеспечивает усовершенствованную защиту BIOS, превышающую требования отраслевого стандарта — оно также разработано на аппаратной основе таким образом, чтобы обеспечивать беспрецедентную киберустойчивость платформы, гарантируя восстановление BIOS даже в случае взлома или разрушительной атаки. Бизнес-компьютеры HP с технологией HP Sure Start превосходят требования проекта руководства Национального института стандартов и технологий США (National Institute of Standards

Technology, NIST) по отказоустойчивости микропрограммного обеспечения платформы (специальное издание 800-193), которое представляет собой одну из основных государственных мер по официальному оформлению требований к киберустойчивым платформам.

Модели с поддержкой HP Sure Start

Решение HP Sure Start впервые появилось на рынке в 2014 г. С тех пор компания HP усовершенствовала Sure Start и расширила ассортимент продуктов, поддерживающих эту технологию. HP Sure Start поддерживается всеми продуктами линейки 2018 Elite, включая планшеты, ноутбуки, настольные компьютеры и моноблоки (All-in-One, AIO). Технология HP Sure Start 4-го поколения доступна на продуктах HP Elite и HP Pro 600, оснащенных процессорами AMD® или Intel 8-го поколения.

Обзор архитектуры и возможностей

HP Sure Start состоит из двух основных архитектурных компонентов:

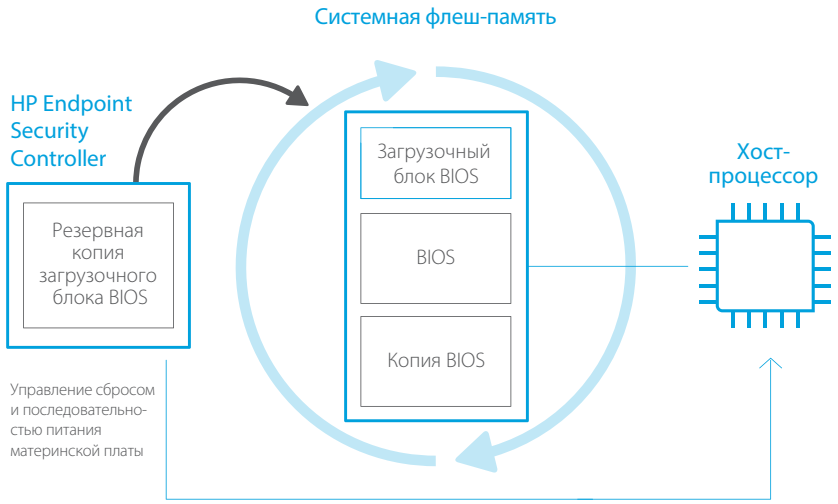
- **HP Endpoint Security Controller** выполняет микропрограммное обеспечение HP Sure Start
- **HP Sure Start BIOS** работает в сочетании с аппаратным и микропрограммным обеспечением HP Endpoint Security Controller

Проверка целостности микропрограммного обеспечения — основа HP Sure Start

HP Endpoint Security Controller (HP ESC) — это первое устройство в системе, которое выполняет микропрограммное обеспечение при включении питания системы задолго до загрузки системы. В числе функций HP ESC — мониторинг кнопки питания системы и управление последовательностью запуска выполнения хост-процессора при нажатии кнопки питания.

При подаче питания на платформу (до включения системы), HP ESC проверяет, является ли его собственное микропрограммное обеспечение оригинальным кодом HP, прежде чем загружать и выполнять этот код.
Для проверки целостности аппаратное обеспечение HP ESC использует стандартные надежные криптографические методы. В методе используется открытый ключ RSA HP 2048 бит, хранящийся во внутренней постоянной памяти только для чтения. Таким образом, HP ESC является встроенным аппаратным «корнем доверия» (Root of Trust, RoT) платформы, который используется для проверки микропрограммного обеспечения и HP BIOS перед их выполнением. Этот аппаратный «корень доверия» обеспечивает защиту от атак с заменой микропрограммы, независимо от их метода развертывания, являясь основой безопасности платформы HP.

Рисунок 1. Процесс проверки целостности микропрограммы.



На рисунке 1 представлен процесс проверки целостности микропрограммного обеспечения. После того как HP ESC выполняет проверку подлинности и запускает выполнение микропрограммного обеспечения HP Sure Start, эта микропрограмма использует те же надежные криптографические операции для проверки целостности загрузочного блока BIOS системной флеш-памяти. Если он является единым, но недействительным, HP ESC заменяет содержимое флеш-памяти системы на собственную копию загрузочного блока HP BIOS, хранящуюся в изолированной энергонезависимой памяти (Non-Volatile Memory, NVM), которая специально предназначена для HP ESC.

HP Sure Start гарантирует, что микропрограммное обеспечение и код BIOS, выполняемый на HP ESC и хост-процессоре, — это код, предназначенный компанией HP для данного устройства.

Примечание. Проверка целостности загрузочного блока системной флеш-памяти, как и любые необходимые действия по восстановлению, выполняемые HP ESC, осуществляются, пока хост-процессор выключен. Поэтому, с точки зрения пользователя данная операция целиком осуществляется до включения системы, в спящем режиме или режиме гибернации.

Загрузочный блок BIOS системной флеш-памяти является основанием HP BIOS. HP ESC обеспечивает процесс, при котором загрузочный блок BIOS является первым кодом, который ЦП выполняет после сброса. После того, как HP ESC определит, что загрузочный блок BIOS содержит подлинный код HP, система загружается обычным способом.

HP ESC также выполняет проверку целостности кода загрузочного блока системной флеш-памяти при каждом выключении системы или ее переводе в спящий режим или режим гибернации. Поскольку в каждом из этих режимов процессор выключен и для возобновления работы процессор должен заново выполнить код загрузочного блока BIOS, крайне важно каждый раз заново выполнять проверку целостности загрузочного блока BIOS для обнаружения попыток взлома.

Кроме того, для моделей HP на процессорах Intel технология HP Sure Start периодически (каждые 15 минут) проверяет целостность загрузочного блока BIOS в системной флеш-памяти во время работы системы.[2]

Целостность данных, уникальная для каждой системы

Совместная работа HP ESC и BIOS обеспечивает усовершенствованную защиту критически важных переменных, настроенных на заводе, которые уникальны для каждой системы и должны оставаться неизменными в течение всего срока службы конкретной платформы. На заводе резервная копия данных этой переменной сохраняется в энергонезависимой памяти HP ESC. Данная резервная копия доступна компоненту HP Sure Start BIOS только для чтения для выполнения проверки целостности данных при каждой загрузке. В случае изменения какого-либо параметра в общей флеш-памяти по сравнению с заводскими настройками, компоненты BIOS HP Sure Start автоматически восстановят системную флеш-память на основании резервной копии, предоставленной HP ESC.

Регион дескриптора

Для моделей HP на процессорах Intel решение HP Sure Start защищает регион дескриптора системной флеш-памяти. Регион дескриптора, являющийся уникальной отличительной характеристикой архитектуры Intel, содержит важные параметры конфигурации, которые отбираются логикой Intel Core™ при сбросе и затем используются для настройки логики Core. Регион дескриптора также включает в себя информацию о разделах для системной флеш-памяти, которая используется логикой Intel Core для установления расположения региона BIOS во флеш-памяти, а следовательно, и места, откуда процессор получает код для выполнения после восстановления. HP Sure Start выполняет мониторинг целостности этого региона и восстанавливает его заданную конфигурацию в случае взлома или повреждения.

Защита контроллера сети

Кроме того, для моделей HP на процессорах Intel решение HP Sure Start защищает настройки сетевого контроллера (NIC), хранящиеся в системной флеш-памяти. Условия эксплуатации у некоторых клиентов HP требуют законного изменения заводских настроек сетевого контроллера. Поэтому по умолчанию HP Sure Start не препятствует изменениям настроек сетевого контроллера. Вместо этого HP Sure Start поддерживает функцию, которая, если ее включить, предупреждает пользователя об изменениях настроек сетевого контроллера. Кроме того, HP Sure Start предоставляет способ восстановления заводских настроек сетевого контроллера. В число защищенных параметров входят MAC-адрес, параметры среды PXE (Pre-boot Execution Environment) и параметры протокола RPL (Remote Initial Program Load). Это восстановление возможно через резервную копию только для чтения, защищенную HP ESC

Защита настройки BIOS

Как было описано выше, HP Sure Start выполняет проверку целостности и подлинности кода HP BIOS. Поскольку данный код является статическим после создания компанией HP, цифровые подписи можно использовать для подтверждения обоих атрибутов кода. Однако являясь динамическими, с возможностью настройки пользователем, параметры BIOS создают дополнительные трудности для защиты. Цифровые подписи не могут создаваться компанией HP и использоваться аппаратным обеспечением HP Sure Start ESC для проверки этих параметров.

Функция защиты настройки BIOS HP Sure Start позволяет настроить систему таким образом, чтобы аппаратное обеспечение HP ESC использовалось для резервного копирования и проверки целостности всех параметров BIOS, предпочитаемых пользователем.

Если эта функция включена на платформе, все параметры политики, используемые BIOS, будут резервироваться, и проверка целостности будет выполняться при каждой загрузке для обеспечения отсутствия изменений параметров политики BIOS. При обнаружении изменений система использует резервную копию из защищенного хранилища HP Sure Start для автоматического восстановления определенных пользователем параметров.

При обнаружении попытки изменения параметров BIOS функция защиты настройки BIOS HP Sure Start генерирует событие для аппаратного обеспечения ESC HP Sure Start. Данное событие записывается в журнал аудита HP Sure Start, а локальный пользователь получает соответствующее уведомление от BIOS во время загрузки.

Защищенное хранилище HP Sure Start

Защищенное хранилище в аппаратном обеспечении HP Endpoint Security Controller предоставляет высочайший уровень безопасности данных и настроек BIOS/микропрограммы под защитой HP Sure Start. Защищенное хранилище HP Sure Start разработано для обеспечения конфиденциальности, целостности и обнаружения взлома даже в случае физической атаки, когда злоумышленник разбирает систему и устанавливает прямое соединение с энергонезависимым запоминающим устройством на монтажной плате.

Целостность данных

Целостность динамических данных, которые микропрограммное обеспечение сохраняет в энергонезависимой памяти и использует для контроля состояния различных возможностей, критически важна для обеспечения безопасности всей платформы. К динамическим данным относятся все параметры BIOS, которые подлежат изменению конечным пользователем или администратором устройства. В качестве примеров можно привести параметры загрузки, такие как функция защищенной загрузки, пароль администратора BIOS и связанные политики, контроль состояния доверенного платформенного модуля и параметры политики HP Sure Start.

Любая успешная атака, обходящая существующие ограничения доступа для предотвращения несанкционированных изменений этих параметров, может нарушить безопасность платформы. Например, рассмотрим сценарий, в котором злоумышленник вносит несанкционированные изменения в состояние защищенной загрузки, чтобы незаметно отключить ее. В этом сценарии платформа загрузит пакет программ rootkit злоумышленника до запуска ОС и совершенно незаметно для пользователя.

Стандартная UEFI BIOS применяет ограничения доступа, препятствующие несанкционированному изменению этих переменных, и HP использует их, как это принято в компьютерной индустрии.

Однако, учитывая риски для платформы, связанные с взломом этих механизмов, HP Sure Start предоставляет дополнительный уровень защиты, превышающий базовые требования отраслевого стандарта.

Параметры BIOS и другие динамические данные, используемые микропрограммным обеспечением для контроля состояния, защиту которого обеспечивает решение HP Sure Start, хранятся в изолированной энергонезависимой памяти HP Endpoint Security Controller, которая недоступна для ПО, выполняемого на хост-процессоре.

Кроме того, HP ESC создает и применяет уникальные показатели целостности при каждом сохранении элемента данных в этом хранилище на основе энергонезависимой памяти. Эти показатели целостности основаны на надежном криптографическом алгоритме (код проверки подлинности сообщений, использующий хеш-функции (HMAC), на основе хеширования SHA-256), привязанный к секрету, содержащемуся в HP ESC. Данный секрет является уникальным для каждого HP ESC: каждый контроллер генерирует уникальный показатель целостности при идентичном элементе.

Когда этот элемент данных считывается обратно из энергонезависимой памяти, HP ESC пересчитывает показатель целостности для этого элемента данных и сравнивает его с показателем целостности, примененным к данным. Любые несанкционированные изменения данных в хранилище энергонезависимой памяти приводят к несовпадению. С помощью этого метода HP ESC может выявить изменение элементов данных, хранящихся в энергонезависимой памяти.

Конфиденциальность данных

Для многих элементов данных, хранящихся на платформе, сохранение конфиденциальности является критически важным. В качестве примеров можно привести хеши пароля администратора BIOS, учетные данные пользователей и секреты, которые могут храниться микропрограммным обеспечением от имени пользователя для таких основанных на микропрограмме функций, как HP Sure Run и HP Sure Recovery.

При использовании стандартных методов UEFI BIOS защиту этих секретов обеспечить трудно, поскольку энергонезависимое хранилище, как правило, доступно для чтения ПО, выполняемым на хост-процессоре. Защищенное хранилище HP Sure Start обеспечивает гораздо более надежную защиту конфиденциальных данных, чем стандартное развертывание UEFI BIOS.

Помимо отдельного изолированного хранилища, метод HP Sure Start заключается в использовании аппаратного блока Advanced Encryption Standard (AES), содержащегося в HP ESC, для применения шифрования AES-256 ко всем конфиденциальным элементам данных, хранящимся в энергонезависимой памяти HP Sure Start, в дополнение к показателям целостности данных для этих элементов. Используемый ключ шифрования уникален для каждого HP ESC и никогда не покидает данный контроллер, поэтому данные, зашифрованные отдельным компонентом HP ESC, могут быть расшифрованы только тем же HP ESC.

Безопасность ключей защищенной загрузки

HP Sure Start предоставляет более усовершенствованную защиту баз данных ключей защищенной загрузки UEFI, которые сохраняются микропрограммным обеспечением, по сравнению с реализацией защищенной загрузки UEFI. Эти переменные критически важны для правильной работы функции защищенной загрузки UEFI, которая проверяет целостность и подлинность загрузчика ОС, прежде чем разрешить запуск загрузки.

HP Sure Start обеспечивает безопасность баз данных ключей защищенной загрузки UEFI, сохраняя мастер-копию в защищенном хранилище HP Sure Start. HP Sure Start отслеживает разрешенные изменения стандартных баз данных ключей защищенной загрузки UEFI, выполняемые ОС во время выполнения, а HP ESC применяет их к мастер-копии. Затем HP Sure Start использует мастер-копию в защищенном хранилище HP Sure Start для обнаружения и отклонения несанкционированных изменений стандартных баз данных ключей защищенной загрузки UEFI.

Эта возможность, включенная по умолчанию, поддерживается следующими базами данных:

- Signature database (db)
- Revoked signatures database (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) обновляется динамически операционной системой в среде выполнения

Функция Runtime Intrusion Detection (RTID)

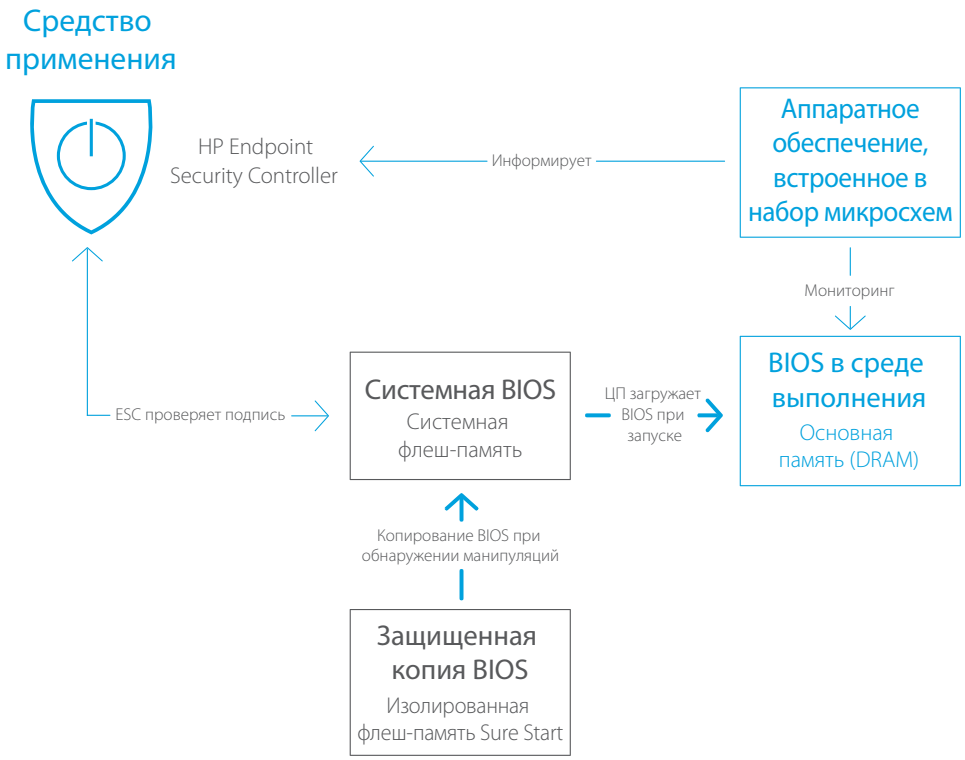
При каждой загрузке код BIOS запускает выполнение из флеш-памяти по фиксированному адресу. Это так называемый загрузочный код BIOS, предоставляющий предварительные возможности, необходимые до запуска ОС. Однако определенная часть BIOS остается в DRAM: она нужна для предоставления расширенных функций управления питанием, служб ОС и других независимых от ОС функций во время выполнения ОС. Этот код BIOS, называемый кодом System Management Mode (SMM), находится в специальной области DRAM, скрытой от ОС. В контексте функции Runtime Intrusion Detection HP Sure Start этот код называется также кодом «среды выполнения» BIOS. (Более подробно об SMM и его работе см. в Приложении Б на стр. 12).

Целостность кода SMM критически важна для безопасности клиентского устройства. HP Sure Start проверяет целостность кода BIOS HP SMM при запуске ОС. Функция Runtime Intrusion Detection предоставляет механизмы для обеспечения целостности кода SMM BIOS во время выполнения ОС путем добавления новых функций защиты и/или предоставления мер по обнаружению атак на этот код.

Архитектура Runtime Intrusion Detection

Функция RTID использует специализированное аппаратное обеспечение в наборе микросхем платформы для обнаружения отклонений в HP SMM BIOS среды выполнения. При обнаружении отклонений отправляется уведомление для HP Endpoint Security Controller, который в свою очередь выполняет действие, настроенное политикой, независимо от процессора.

Рисунок 2. Функция Runtime Intrusion Detection использует специализированное аппаратное обеспечение, встроенное в набор микросхем платформы для мониторинга кода SMM на наличие изменений.



Уведомления пользователей, журналы событий и управление политиками

Уведомления HP Sure Start для конечных пользователей

При нормальных условиях решение HP Sure Start неощутимо для пользователей. Операции восстановления выполняются автоматически с использованием настроек по умолчанию. Как правило, когда HP Sure Start обнаруживает проблему, для восстановления не требуется взаимодействия с конечными пользователями или ИТ-отделом.

Уведомления во время выполнения отображаются для пользователей в случае, если проблема с целостностью BIOS обнаружена функциями HP Sure Start Dynamic Protection или Runtime Intrusion Detection во время выполнения ОС. При обнаружении значительного события или принятии мер HP Sure Start отображает предупреждение в виде уведомления Windows® при следующей загрузке. Для просмотра уведомлений Windows необходимо приложение HP Notifications Software.

Журнал событий HP Sure Start

HP Endpoint Security Controller записывает критически важные события, связанные с кодом и данными микропрограммного обеспечения/BIOS, которые контролируются решением HP Sure Start. Эти события сохраняются в хранилище энергонезависимой памяти Sure Start. Эти события копируются из HP ESC в средство просмотра событий Windows при установке HP Notifications Software для упрощения доступа к этим событиям локального пользователя, а также предпочтительного агента управляемости клиента.

Следующие события запустят сбор всех событий приложением HP Notifications Software из подсистемы HP Sure Start, а также обеспечат добавление в средство просмотра событий Windows еще не записанных событий:

- Загрузка Windows
- Возобновление Windows из спящего режима/режима гибернации
- HP Sure Start с уведомлениями о событиях динамической защиты в среде выполнения
- HP Sure Start Runtime Intrusion Detection (RTID)

Приложение HP Notifications Software регистрирует события HP Sure Start в уникальном журнале событий приложения «HP Sure Start». В этот журнал включаются только события HP Sure Start. Путь средства просмотра событий Windows к событиям HP Sure Start: Служебные программы/Просмотр событий/Журналы приложений и служб/HP Sure Start.

Категории уровня средства просмотра событий Windows, связанные с событиями HP Sure Start, определены в таблице ниже.

Эти события добавляются в средство просмотра событий Windows в том порядке, в котором они генерируются HP Sure Start. Хронологически наиболее удаленные события в подсистеме HP Sure Start добавляются в средство просмотра событий Windows первыми, а самые недавние, наоборот, добавляются последними.

Временная метка каждой записи средства просмотра событий Windows — это время его добавления в журнал, а НЕ время возникновения данного события. Каждая запись Sure Start в средстве просмотра событий Windows включает подробные данные о событии, включая метку времени его фактического возникновения.

Примечание. События сохраняются в HP Endpoint Security Controller даже после копирования в средство просмотра событий Windows. Если очистить средство просмотра событий Windows, приложение HP Notifications Software заменит все записи HP Sure Start на следующее событие, вызывающее проверку журналов событий HP Sure Start.

Типы событий средства просмотра событий Windows HP Sure Start

Уровень события	Определение
Информация	События, прогнозируемые в ходе нормальной работы (напр., обновление BIOS).
Предупреждение	Непредвиденные события, которые, однако, были полностью восстановлены HP Sure Start и не требуют вмешательства пользователя/администратора для обеспечения полноценной работы платформы. Такими событиями являются аномальные операции, которые пользователю/администратору следует изучить подробнее, особенно если такие события происходят на нескольких компьютерах.
Ошибка	События, для полного восстановления от которых требуется вмешательство в работу платформы администратора/службы HP.

Средства настройки политик HP Sure Start

По умолчанию HP BIOS включает и оптимизирует политики HP Sure Start для типичного пользователя. Поскольку решение HP Sure Start включено по умолчанию, типичному пользователю нет необходимости изменять параметры защиты HP Sure Start. Для продвинутых пользователей системная BIOS предоставляет возможности управления поведением HP Sure Start с помощью параметров политики в программе настройки BIOS (F10). Если не указано иное, эти параметры и функции расположены в разделе Security/BIOS Sure Start.

Примечание. Политики хранятся в энергонезависимой памяти HP ESC, которая закрыта для прямого доступа хост-процессора; поэтому для того, чтобы настройки Sure Start вступили в действие, требуется перезагрузка.

HP Sure Start предоставляет следующие параметры и функции:

- Проверка загрузочного блока при каждой загрузке
- Политика восстановления данных BIOS
- Восстановление конфигурации сетевого контроллера (только Intel)
- Запрос на подтверждение изменения конфигурации сетевого контроллера (только Intel)
- Динамическое сканирование загрузочного блока в среде выполнения (только Intel)
- Защита настроек BIOS HP Sure Start
- Безопасность ключей защищенной загрузки HP Sure Start
- Усовершенствованное обнаружение и предотвращение вторжений в среде выполнения микропрограммного обеспечения HP (только Intel)
- Обнаружение вторжений в среде выполнения микропрограммного обеспечения HP (только AMD)
- Политика событий безопасности HP Sure Start
- Уведомление о событии безопасности HP Sure Start при загрузке
- Блокировка версии BIOS
- Сохранение/восстановление главной загрузочной записи (master boot record, MBR) системного жесткого диска
- Сохранение/восстановление GPT системного жесткого диска
- Политика восстановления загрузочного сектора (MBR/GPT)

Verify Boot Block on Every Boot (Проверка загрузочного блока при каждой загрузке)

HP Sure Start всегда проверяет целостность загрузочного блока BIOS системной флеш-памяти перед возобновлением работы из спящего режима, режима гибернации или перед включением питания системы. Если задан параметр **enable** (вкл.), HP Sure Start будет также проверять целостность загрузочного блока при каждой «горячей перезагрузке» (перезапуск Windows). Можно рассмотреть компромиссный вариант более быстрой перезагрузки со снижением уровня защиты. По умолчанию для данной функции задана настройка **disable** (откл.).

BIOS Data Recovery Policy (Политика восстановления данных BIOS)

Если задан параметр **Automatic** (Автоматически), HP Sure Start при необходимости автоматически восстановит BIOS или уникальные данные компьютера. Если задан параметр **Manual** (Вручную), для продолжения исправления HP Sure Start потребуется специальное сочетание клавиш. В случае проблем с кодом загрузочного блока система не будет загружена, а на светодиодной панели системы замигает уникальная последовательность индикаторов. При возникновении проблем с уникальными данными компьютера на экране отобразится соответствующее сообщение. Требуемое сочетание клавиш и отображаемая последовательность индикаторов зависят от системы (ноутбук, настольный компьютер, планшет). Ручной режим пригодится пользователям, которые умеют проводить экспертизу содержимого системной флеш-памяти перед исправлением. Типичным пользователям ручной режим не рекомендуется. По умолчанию для данной функции задана настройка **Automatic** (Автоматически).

Network Controller Configuration Restore (Восстановление конфигурации сетевого контроллера) (только Intel)

Этот элемент управления доступен только в системах Intel. При его выборе HP Sure Start мгновенно восстанавливает заводскую конфигурацию сетевого контроллера по умолчанию.

Prompt on Network Controller Configuration Change (Запрос на подтверждение изменения конфигурации сетевого контроллера) (только Intel)

Этот параметр доступен только в системах Intel. HP предоставляет заводскую конфигурацию сетевого контроллера, включая MAC-адрес. Если для этой функции задана настройка **enable** (вкл.), система осуществляет мониторинг конфигурации сетевого контроллера и отображает запрос подтверждения в случае, если пользователь меняет заводскую конфигурацию. По умолчанию для данной функции задана настройка **disable** (откл.).

Dynamic Runtime Scanning of Boot Block (Динамическое сканирование загрузочного блока в среде выполнения) (только Intel)

Этот параметр доступен только в системах Intel. По умолчанию задано значение **enable** (вкл.), при котором HP Sure Start выполняет периодические проверки целостности загрузочного блока BIOS во время работы ОС. Если задана настройка **disable** (откл.), HP Sure Start проверяет целостность только перед загрузкой или возобновлением работы из спящего режима или режима гибернации.

HP Sure Start BIOS Setting Protection (Защита настройки BIOS HP Sure Start)

По умолчанию для политики защиты настройки BIOS задана настройка **disabled** (откл.). Чтобы включить эту функцию, владелец/администратор клиентского устройства должен сначала настроить предпочтительные политики BIOS. Владельцу/администратору также нужно задать пароль администратора для настройки BIOS, который будет использоваться функцией защиты настройки BIOS HP Sure Start.

После этого значение политики защиты настройки BIOS должно измениться на «enabled» (вкл.). На этом этапе создается резервная копия всех параметров BIOS в защищенном хранилище HP Sure Start. С этого момента ни один параметр BIOS нельзя изменить ни локально, ни удаленно. При каждой загрузке выполняется проверка состояния параметров политики BIOS и, при обнаружении расхождений, параметры BIOS восстанавливаются из защищенного хранилища HP Sure Start.

Для изменения параметра BIOS потребуется предоставить пароль администратора BIOS, после чего защита настройки BIOS будет отключена и можно будет изменить параметры BIOS.

HP Sure Start Secure Boot Keys Protection (Безопасность ключей защищенной загрузки HP Sure Start)

На заводе для данной функции по умолчанию задана настройка **enable** (вкл.), и HP Sure Start обеспечивает усовершенствованную защиту баз данных и ключей защищенной загрузки, используемых BIOS для проверки целостности и подлинности загрузчика ОС, прежде чем запускать его при загрузке. Если задана настройка **disable** (откл.), используется только стандартная защита переменной защищенной загрузки UEFI и резервные копии не сохраняются в подсистеме HP Sure Start.

Enhanced HP Firmware Runtime Intrusion Prevention and Detection (Усовершенствованное обнаружение и предотвращение вторжений во время выполнения микропрограммного обеспечения HP) (только Intel) и HP Firmware Runtime Intrusion Detection (Обнаружение вторжений во время выполнения (Runtime Intrusion Detection, RTID) микропрограммного обеспечения HP) (только AMD)

По умолчанию для функции RTID задана настройка **enabled** (вкл.) для всех платформ, поставляемых с завода HP. Чтобы начать использовать HP Sure Start RTID, конечные пользователи/администраторы не должны включать или иным способом выполнять «развертывание» данной функции.

При необходимости владелец/администратор платформы может задать для функции RTID настройку **disable** (откл.).

HP Sure Start Security Event Policy (Политика событий безопасности HP Sure Start)

Данный параметр политики BIOS указывает, какое действие будет выполняться при обнаружении решением HP Sure Start атаки или попытки атаки во время выполнения ОС. Существуют три возможные конфигурации этой политики.

- **Log event only** (Только регистрация событий): При выборе этой настройки HP ESC регистрирует события обнаружения, которые можно просмотреть по следующему пути: Журналы приложений и служб/HP Sure Start в средстве просмотра событий Microsoft Windows.[3]
- **Log event and notify user** (Регистрация событий и отправка уведомлений пользователям): Эта настройка задана по умолчанию. При выборе этой настройки HP ESC регистрирует события обнаружения, которые можно просмотреть по следующему пути: Журналы приложений и служб/HP Sure Start в средстве просмотра событий Microsoft Windows. Кроме того, для пользователя отображается запрос в Windows, сообщающий о произошедшем событии.[4]
- **Log event and power off system** (Регистрация событий и выключение системы): При выборе этой настройки HP ESC регистрирует события обнаружения, которые можно просмотреть по следующему пути: Журналы приложений и служб/HP Sure Start в средстве просмотра событий Microsoft Windows. Кроме того, для пользователя отображается запрос в Windows о произошедшем событии и о том, что сейчас произойдет выключение системы.

Уведомление о событии безопасности HP Sure Start при загрузке

Этот параметр политики BIOS задает, должен ли локальный пользователь подтверждать предупреждения и сообщения об ошибке HP Sure Start, которые отображаются в случае необходимости перезагрузки системы, прежде чем продолжится перезагрузка. Если задана настройка по умолчанию **Require Acknowledgement** (Требуется подтверждение), система останавливается и отображается сообщение об ошибке. Для продолжения загрузки локальный пользователь должен нажать клавишу. Если задать настройку **Time out after 15 seconds** (Превышение лимита времени через 15 секунд), сообщение отобразится, но процесс загрузки продолжится автоматически через 15 секунд.

Lock BIOS Version (Блокировка версии BIOS)

В программе настройки BIOS (F10) эта функция находится на вкладке Main/Update System BIOS (Главное меню/Обновить системную BIOS).

Если задана настройка **disable** (откл.), можно обновить BIOS с помощью любого поддерживаемого процесса. Когда HP ESC обнаруживает допустимое обновление загрузочного блока в системной флеш-памяти, выполняется обновление резервной копии данного загрузочного блока.

Если задана настройка **enable** (вкл.), все средства обновления HP BIOS отказываются выполнять обновление BIOS. Кроме того, HP Sure Start защищает BIOS от попыток изменить версию BIOS путем удаления системной флеш-памяти несанкционированным способом. HP ESC записывает заблокированные версии BIOS. Если HP ESC обнаруживает изменение BIOS в системной флеш-памяти, HP ESC переписывает загрузочный блок BIOS, заменяя его на копию загрузочного блока HP ESC. Копия загрузочного блока HP ESC выполняет и восстанавливает оставшуюся часть правильной версии BIOS. По умолчанию для данной функции задана настройка **disable** (откл.).

Save/Restore MBR of System Hard Drive (Сохранение/восстановление главной загрузочной записи (master boot record, MBR) системного жесткого диска) и Save/Restore GPT of System Hard Drive (Сохранение/восстановление GPT системного жесткого диска)

В программе настройки BIOS (F10) данная функция расположена на вкладке Security/Hard Drive Utilities (Безопасность/Утилиты жесткого диска). Доступна одна из этих возможностей, в зависимости от типа разделов основного диска (GPT или MBR), который обнаружит решение HP Sure Start.

Если задана настройка **enable** (вкл.), HP Sure Start сохраняет защищенную резервную копию таблицы разделов MBR/GPT с основного диска и сопоставляет резервную копию с основной при каждой загрузке. При обнаружении отличий отображается запрос для пользователя, который может выбрать восстановление исходного состояния в соответствии с резервной копией или включение обнаруженных изменений в защищенную резервную копию. Можно также использовать функцию **Boot Sector (MBR/GPT) Recovery Policy** (Политика восстановления загрузочного сектора (MBR/GPT)) для удаления выбранного пользователем действия, в случае, если HP Sure Start обнаруживает противоречие.

Если задана настройка по умолчанию **disable** (откл.), HP Sure Start не предоставляет защиту MBR/GPT.

Boot Sector (MBR/GPT) Recovery Policy (Политика восстановления загрузочного сектора (MBR/GPT))

Если задана настройка по умолчанию **Local User Control** (Контроль локальным пользователем), в случае, когда решение HP Sure Start обнаруживает изменение в таблице разделов MBR/GPT, отображается запрос действия для пользователя. Если задана настройка **Recover in the event of corruption** (Восстановление в случае повреждения), HP Sure Start автоматически восстанавливает сохраненное состояние MBR/GPT при обнаружении отличий.

Удаленное управление средствами настройки политик HP Sure Start

По умолчанию политики HP Sure Start оптимизированы для типичного пользователя. Поскольку технология HP Sure Start включена по умолчанию, удаленный администратор не должен выполнять никаких действий для включения (или «развертывания») HP Sure Start. Если требуется изменить параметры политики HP Sure Start, удаленный администратор может использовать те же API Windows Management Instrumentation (WMI) или скрипты HP BIOS Configuration Utility, которые используются для управления политиками BIOS других платформ. Кроме того, администраторы могут выполнять удаленное управление функциями HP Sure Start с помощью подключаемого модуля Manageability Integration Kit (MIK) для Microsoft System Center Configuration Manager (SCCM).

Кроме того, администраторы могут выполнять удаленное управление функциями HP Sure Start и просматривать события HP Sure Start с помощью подключаемого модуля Manageability Integration Kit (MIK) для Microsoft System Center Configuration Manager (SCCM).

Заключение

HP Sure Start предоставляет следующие основные преимущества.

- **Непрерывная работа** — HP Sure Start обеспечивает непрерывность функционирования в случае атаки или случайного повреждения, устраняя простои, связанные с ожиданием визита ИТ/техподдержки.
- **Сокращение расходов** — способность HP Sure Start выполнять восстановление автоматически сокращает число обращений в ИТ службу поддержки и повышает производительность, что в конечном счете помогает сократить расходы на обслуживание платформы.
- **Спокойствие и уверенность** — HP Sure Start включает несколько функций обеспечения безопасности, совместимых с различными программными и аппаратными платформами.

Защита критически важного микропрограммного обеспечения BIOS от вредоносного ПО с помощью ведущих в отрасли функций обнаружения вторжений и автоматического восстановления микропрограммы, предоставляемых эксклюзивным решением HP Sure Start, которое доступно на некоторых моделях компьютеров HP Elite.

Приложение A — HP Sure Start, поколение за поколением

Решение HP Sure Start впервые появилось на рынке в 2014 г. С тех пор компания HP усовершенствовала Sure Start и расширила ассортимент продуктов, использующих эту технологию. В таблице ниже представлен обзор возможностей, которые добавлялись в решение с каждым новым поколением.

Поколение	Дата выпуска	Добавленные возможности
HP Sure Start	2014	• Обеспечение подлинности микропрограммного обеспечения и BIOS, с возможностью самовосстановления • Мониторинг микропрограммного обеспечения и проверка соответствия нормативно-правовым требованиям
HP Sure Start с Dynamic Protection	2015	• Поддержка средства просмотра событий Windows • Dynamic Protection (для некоторых продуктов Intel)
HP Sure Start 3-го поколения (для некоторых продуктов Intel)[5] HP Sure Start с функцией Runtime Intrusion Detection (для некоторых продуктов AMD)[6]	2017	• Функция Runtime Intrusion Detection • Защита настройки BIOS • Подключаемый модуль Manageability Integration Kit (MIK) для Microsoft SCCM
HP Sure Start 4-го поколения[7]	2018	• Защищенное хранилище: надежные криптографические методы для сохранения параметров BIOS, учетных данных пользователей и других настроек в аппаратном обеспечении HP Endpoint Security Controller с целью защиты целостности, обнаружения вторжений и обеспечения конфиденциальности этих данных • Безопасность базы данных защищенной загрузки: усовершенствованная защита баз данных и ключей, хранящихся в BIOS, которые критически важны для целостности функции защищенной загрузки ОС, в отличие от стандартной реализации UEFI BIOS • На платформах Intel — усовершенствованные защита и восстановление микропрограммного обеспечения Intel Management Engine • Сертификация средства безопасности HP Endpoint Security Controller сторонними организациями: тестирование независимой аккредитованной лабораторией для подтверждения заявленных основных рабочих характеристик аппаратного обеспечения HP ESC на основании общедоступных критериев, методологии и процессов.[1] • Бизнес-компьютеры HP с технологией HP Sure Start превосходят требования проекта руководства NIST по отказоустойчивости микропрограммного обеспечения платформы (специальное издание 800-193)

Приложение Б — Обзор System Management (SMM)

System Management Mode (SMM) — это стандартный отраслевой метод, используемый для функций расширенного управления питанием компьютера и других функций, независимых от ОС, во время выполнения ОС. Условия и реализация SMM рассчитаны на архитектуры x86, однако во многих современных вычислительных архитектурах используется аналогичная архитектурная концепция.

BIOS настраивает SMM во время загрузки. Код SMM вносится в основную память (DRAM), после чего BIOS использует специальные (фиксируемые) реестры конфигураций в наборе микросхем для блокировки доступа к этой области, если микропроцессор не выполняется в контексте SMM. В среде выполнения вход в режим SMM вызывается событиями. Набор микросхем запрограммирован на распознавание различных событий и превышений лимита времени. При возникновении такого события аппаратное обеспечение набора микросхем выставляет закрепление ввода System Management Interrupt (SMI). При следующей границе инструкции микропроцессор сохраняет все состояние и входит в режим SMM.

Когда микропроцессор входит в режим SMM, он выставляет закрепление вывода аппаратного обеспечения — SMI Active (SMIACT). Закрепление доставляет аппаратному обеспечению набора микросхем уведомление о том, что микропроцессор входит в режим SMM. SMI может быть выставлено в любое время, в режиме функционирования любого процесса, кроме самого SMM. Аппаратное обеспечение набора микросхем распознает сигнал SMIACT и перенаправляет все последующие циклы памяти в защищенную область памяти (иногда ее называют областью SMRAM), которая зарезервирована специально для SMM. Сразу после получения ввода SMI и выставления вывода SMIACT микропроцессор начинает сохранять все свое внутреннее состояние в эту защищенную область памяти.

После того как состояние микропроцессора сохранено в памяти SMRAM, специальный код обработчика SMM, который также хранится в SMRAM (он помещается туда системной BIOS во время загрузки), начинает выполняться в специальном рабочем режиме SMM. В этом режиме большая часть механизмов изоляции памяти и аппаратного обеспечения приостанавливается, и микропроцессор получает доступ практически ко всем ресурсам платформы, обеспечивая выполнение ими требуемых задач. Код SMM выполняет требуемую задачу, после чего микропроцессор должен вернуться в предыдущий рабочий режим. На этом этапе код SMM выполняет инструкцию «Return from System Management Mode» (RSM) для выхода из режима SMM. Инструкция RSM вызывает восстановление данных предыдущего внутреннего состояния микропроцессора на основании копии, которая была сохранена в SMRAM после входа в режим SMM. После завершения RSM полностью восстанавливается состояние микропроцессора, предшествующее событию SMI, и возобновляется выполнение предыдущей программы (ОС, приложений, гипервизора и т. д.) с того момента, когда был выполнен выход.

[1] Аппаратное обеспечение контроллера HP Sure Start сертифицировано по программе сертификации CSPN.

[2] Технология HP Sure Start с функцией Dynamic Protection доступна продуктах HP Elite, оснащенных процессорами Intel Core 6-го и последующих поколений.

[3] Для просмотра событий HP Sure Start в средстве просмотра событий Windows требуется установить приложение HP Notification Software.

[4] Для получения уведомлений требуется установить приложение HP Notification Software.

[5] Технология HP Sure Start 3-го поколения доступна на продуктах HP Elite, оснащенных процессорами Intel 7-го поколения.

[6] Технология HP Sure Start с функцией Runtime Intrusion Detection доступна на продуктах HP Elite, оснащенных процессорами AMD 7-го поколения.

[7] Технология HP Sure Start 4-го поколения доступна в продуктах HP Elite и HP Pro 600, оснащенных процессорами AMD или Intel 8-го поколения.

Дополнительная информация доступна на веб-сайте hp.com/go/computersecurity

4AA7-3172RUE, Май 2018 г.