Технический документ

Обеспечьте соблюдение политик безопасности сети и данных

Рекомендации по применению мер безопасности к парку устройств печати

Содержание

Несоблюдение политик безопасности может нанести бизнесу существенный ущерб

Помимо крупных штрафов и судебных издержек брешь в системе безопасности может привести к снижению прибыли и потере деловой репутации. При разработке плана обеспечения безопасности необходимо помнить о том, что общий уровень безопасности сети зависит от того, насколько надежно защищено ее самое слабое звено. Устройства печати и обработки изображений подвержены тем же рискам, что и ПК. Именно поэтому критически важно установить устройства и решения, отвечающие политикам безопасности, чтобы защитить коммерческую информацию от внешних и внутренних угроз.

В чем заключаются риски?

Невыполнение нормативных требований приводит к значительным убыткам, к которым относятся штрафы, потеря бизнеса, испорченная репутация и групповые иски.

Незащищенные или недостаточно защищенные устройства вывода представляют собой отличную мишень для киберпреступников. Представители компаний, опрошенные Ponemon, заявили, что в среднем на каждую неделю 2016 года приходилось по две атаки, что на 23 % больше по сравнению с прошлым годом, а годовые потери от них составили в среднем 9,5 млн долларов[1]. Только в прошлом году было скомпрометировано более 4 млрд элементов данных по всему миру, что на 400 % больше, чем в предыдущие два года[2].

Хотя многие ИТ-отделы принимают комплексные меры безопасности в отношении компьютеров и сетей, устройства печати и обработки изображений зачастую остаются без внимания. В то же время принтеры могут использоваться для проникновения в сеть, поэтому обеспечение их безопасности является не менее важной задачей. 26% серьезных утечек данных, о которых сообщили руководители ИТ-отделов, были связаны с открытым доступом к устройствам печати[3].

Чтобы противостоять растущей угрозе, правительства многих стран внедряют жесткие меры обеспечения безопасности, требующие от компаний лучше защищать данные клиентов. Новый европейский общий регламент по защите данных — один из ключевых нормативных документов, который вступит в силу в 2018 году. В нем выдвигаются повышенные требования в области защиты данных. Поэтому целесообразно защитить каждое устройство с доступом к вашей корпоративной сети: от ПК до смартфонов и планшетов. Новый документ затрагивает не только страны ЕС: международные компании, использующие данные граждан ЕС, также должны организовать свою работу согласно этому документу. Компании будут обязаны сообщать об утечке данных в течение 72 часов с момента обнаружения. Для этого будет необходимо отслеживать и оценивать состояние каждого устройства. Если проверка на соответствие обнаружит незамеченную или не отраженную в отчете утечку данных, компанию ждет штраф до 20 млн долларов или 4 % годового оборота.

Общие меры безопасности для соблюдения политик безопасности

Обеспечение политик безопасности и требований законодательства является нетривиальной задачей. К счастью, компания Center for Internet Security (CIS) составила перечень общих мер безопасности, упрощающих применение рекомендаций по защите от киберпреступности. Этот перечень включает 20 конкретных действий, направленных на пресечение кибератак. (Подробные сведения см. по адресу https://www.cisecurity.org/critical-controls.cfm.) Данные меры безопасности соответствуют общепризнанным стандартам, таким как PCI-DSS, ISO 27001, рекомендации US CERT, HIPAA, FFIEC и NIST. Данные меры безопасности не заменяют другие стандарты, но часто используются в корпоративной среде для эффективной реализации политик безопасности.

Меры безопасности CIS определяют порядок выполнения небольшого количества действий, что позволяет добиться ощутимых результатов. Эти меры позволяют эффективно противодействовать наиболее распространенным схемам атак, приведенным в ведущих отчетах об угрозах безопасности. В разработке участвовала большая группа экспертов — в том числе из ведущих мировых компаний, занимающихся судебной экспертизой и расследованием киберпреступлений. Кроме того, данный перечень постоянно обновляется по мере появления новых угроз и типов атак.

Используйте перечень мер безопасности CIS для разработки корпоративных политик безопасности и соблюдения нормативных требований. В данном информационном документе приводятся рекомендуемые действия для каждой из 20 мер безопасности, позволяющие надежно защитить ваши принтеры, данные и документы в рамках более общего плана обеспечения безопасности. Пункты 4, 6, 8, 12, 13 и 15 нацелены на защиту данных и мониторинг активности в соответствии с требованиями нового европейского общего регламента по защите данных.

Критически важные меры безопасности CIS и рекомендуемые действия

CSC 1: инвентаризация авторизованных и неавторизованных устройств

Мера безопасности: активное администрирование (инвентаризация, отслеживание и устранение проблем) всех устройств в сети с целью предоставления доступа только авторизованным устройствам и блокировки неавторизованных и неподконтрольных устройств.

Рекомендация: убедитесь, что все печатающие устройства в сети находятся под контролем и соответствуют требованиям политики безопасности. Эффективное средство управления безопасностью печати позволяет обнаруживать и отслеживать все сетевые устройства и устройства, подключенные к ПК.

CSC 2: инвентаризация авторизованного и неавторизованного ПО

Мера безопасности: активное администрирование (инвентаризация, отслеживание и устранение проблем) всего программного обеспечения в сети с целью установки и выполнения только авторизованного ПО и запрета установки и выполнения неавторизованного и неподконтрольного ПО.

Рекомендация: убедитесь, что загруженные в устройства печати и обработки изображений микропрограммы и решения обновлены, подписаны электронной подписью и являются подлинными. Выбирайте печатающие устройства со встроенными средствами защиты BIOS и микропрограммами, гарантирующими загрузку только подлинного программного кода. Для своевременной установки обновлений микропрограмм в масштабах всей организации используются решения для управления парком устройств. Программное обеспечение (как серверное, так и пользовательское) должно быть подписано электронной подписью, подтверждающей его подлинность.

CSC 3: защищенные настройки оборудования и программного обеспечения на мобильных устройствах, ноутбуках, рабочих станциях и серверах

Мера безопасности: разработка, развертывание и активное администрирование (отслеживание, формирование отчетов и устранение проблем) защищенных настроек ноутбуков, серверов и рабочих станций в рамках строгих процедур управления конфигурацией и изменениями, не позволяющих злоумышленникам воспользоваться уязвимыми службами и настройками.

Рекомендация: при настройке сетевых устройств — в том числе принтеров — необходимо выбирать безопасные параметры. Рекомендуется разработать и развернуть единую политику безопасности для всего парка печатающих устройств и своевременно устранять все обнаруженные несоответствия. Контрольные списки безопасности (например, NIST) и службы рекомендаций по вопросам безопасности позволят вам спроектировать и внедрить комплексную политику безопасности печати. Эффективное средство управления безопасностью печати позволит автоматизировать процедуры создания, развертывания, оценки параметров устройств и устранения несоответствия параметров заданным значениям в масштабах всего парка оборудования. Многофункциональные устройства (МФУ) корпоративного класса поддерживают более 250 параметров безопасности, поэтому автоматизация соответствующих процедур настройки позволит существенно сэкономить время.

CSC 4: постоянное выявление и устранение рисков

Мера безопасности: постоянный сбор информации, анализ полученных данных и выполнение процедур по выявлению рисков, их устранению и сведению к минимуму возможностей для проведения атаки со стороны злоумышленников.

Рекомендация: системы управления информационной безопасностью и событиями безопасности (SIEM), например ArcSight, Splunk и SIEMonster, отслеживают активность в сети в режиме реального времени и уведомляют администраторов о подозрительных происшествиях. Отслеживать печатающие устройства так же важно, как и ПК — убедитесь, что ваши принтеры поддерживают возможность отправки сообщений в журнал событий системы SIEM.

Выбирайте печатающие устройства, обнаруживающие атаки в режиме реального времени и автоматически восстанавливающие работоспособность, что гарантирует максимальную продолжительность бесперебойной работы оборудования при минимальном вмешательстве со стороны ИТ-отдела.

Чтобы снизить риски, воспользуйтесь средством управления безопасностью парка устройств, которое автоматически обнаруживает новые принтеры и принудительно применяет к ним настройки корпоративной политики безопасности при подключении к сети. Запланируйте регулярные процедуры анализа инфраструктуры и устранения несоответствий, чтобы обеспечить соблюдение требований политики безопасности в масштабах всего парка устройств.

CSC 5: контролируемое применение прав администратора

Мера безопасности: постоянное отслеживание использования, назначения и изменения прав администратора для компьютеров, сетей и приложений; своевременное пресечение их ненадлежащего либо избыточного применения.

Рекомендация: выбирайте печатающие устройства и решения, поддерживающие возможности аутентификации пользователей и контроля доступа к отдельным функциям в зависимости от должностных обязанностей сотрудника, чтобы настраивать оборудование могли только ИТ-специалисты и уполномоченные лица. Задайте пароли администраторов для всего парка устройств с помощью ПО для управления безопасностью.

CSC 6: ведение, мониторинг и анализ журналов аудита

Мера безопасности: ведение журналов аудита и анализ полученных данных с целью обнаружения атак и устранения их последствий.

Рекомендация: печатающие устройства должны поддерживать возможность записи в системный журнал сообщений о подозрительных происшествиях, чтобы специалисты по безопасности могли выявлять и устранять проблемы. Выбирайте устройства, поддерживающие возможность отправки сообщений в решения для управления безопасностью парком устройств и системы SIEM — это позволит осуществлять мониторинг в режиме реального времени и создавать отчеты для проведения аудита и соблюдения иных нормативных требований.

CSC 7: защита электронной почты и браузера

Мера безопасности: сведение к минимуму возможностей злоумышленников по манипуляции поведением сотрудников с помощью мошеннических сообщений в браузерах и по электронной почте.

Рекомендация: МФУ часто подключают к Интернету, например для отправки отсканированных документов по электронной почте. Убедитесь, что передаваемые по почте сообщения шифруются, что гарантирует защиту конфиденциальных данных. Разверните устройства и решения, поддерживающие возможности аутентификации пользователей и контроля доступа к ресурсам оборудования (например, к веб-серверу и электронной почте) в зависимости от должностных обязанностей сотрудника. Создайте для МФУ список «Надежные сайты», в который будут входить только те сайты, на которые можно заходить с данного устройства. Интегрируйте различные методы аутентификации (например, по ПИН-коду или персональному идентификационному коду, LDAP и Kerberos) с Active Directory для повышения уровня безопасности и эффективности администрирования. Печатающие устройства, подключенные к сети, должны оснащаться встроенными средствами защиты от вирусов и иных вредоносных программ, а микропрограмма должна регулярно обновляться для поддержки новейших средств безопасности.

CSC 8: защита от вредоносных программ

Мера безопасности: контроль установки, распространения и выполнения вредоносного ПО в масштабах всей организации; использование средств автоматизации для оперативного обновления систем безопасности, сбора данных и проведения корректирующих мероприятий.

Рекомендация: выбирайте печатающие устройства, поддерживающие загрузку только проверенного кода с электронной подписью и оснащенные встроенными средствами защиты от вредоносных программ, которые постоянно отслеживают состояние памяти устройства, а в случае атаки выполняют перезагрузку. Эффективное решение по управлению безопасностью инфраструктуры печати автоматически оценивает параметры устройств и устраняет обнаруженные несоответствия в масштабах всего парка оборудования. Также следует убедиться в том, что все программные решения для управления печатью подписаны электронной подписью, гарантирующей их подлинность.

CSC 9: ограничение использования сетевых портов, протоколов и служб

Мера безопасности: контроль (отслеживание, ограничение функциональности и устранение проблем) использования портов, протоколов и служб на сетевых устройствах для сведения к минимуму возможностей злоумышленников по использованию уязвимостей.

Рекомендация: если это не сделано по умолчанию, отключите неиспользуемые порты и небезопасные протоколы (например, FTP и Telnet), с помощью которых злоумышленники могут получить доступ к устройству. Сэкономьте время ИТ-специалистов и сократите риски, развернув средство управления безопасностью печати, которое будет автоматически поддерживать параметры устройств в соответствии с корпоративной политикой безопасности в масштабах всего парка оборудования. Ограничьте доступ к функциям и настройкам устройств с помощью паролей администратора, средств аутентификации и механизмов контроля доступа на основе ролей.

CSC 10: возможности восстановления данных

Мера безопасности: резервное копирование критически важной информации по надежной методологии, позволяющей восстановить данные в экстренной ситуации.

Рекомендация: в настоящее время данная мера безопасности к устройствам печати не применима.

CSC 11: защищенные конфигурации сетевых устройств, в том числе брандмауэров, маршрутизаторов и коммутаторов

Мера безопасности: разработка, развертывание и активное администрирование (отслеживание, формирование отчетов и устранение проблем) защищенных конфигураций инфраструктурных сетевых устройств в рамках строгих процедур управления конфигурацией и изменениями, не позволяющих злоумышленникам воспользоваться уязвимыми службами и настройками.

Рекомендация: при настройке сетевых устройств — в том числе принтеров — необходимо выбирать безопасные параметры. Эффективное средство управления безопасностью печати позволит автоматизировать процедуры создания, развертывания, оценки параметров устройств и устранения несоответствия параметров заданным значениям в масштабах всего парка оборудования — сэкономив тем самым время ИТ-специалистов.

CSC 12: защита периметра сети

Мера безопасности: контроль (в том числе ограничение и пресечение) информационных потоков, передаваемых по сетям с различными уровнями доверия; особо пристальное внимание к данным, которые могут поставить под угрозу систему безопасности.

Рекомендация: шифруйте передаваемые данные (задания печати и сканирования, отправляемые на принтер или с принтера) и данные, хранящиеся на жестком диске устройства. Выбирайте печатающие устройства и решения, поддерживающие возможности аутентификации пользователей и контроля доступа к отдельным функциям в зависимости от должностных обязанностей сотрудника; в этом случае только авторизованные лица смогут отправлять задания сканирования по электронной почте или отправлять файлы в облачные хранилища. Создайте для устройства список «Надежные сайты», чтобы предотвратить доступ к вредоносным сайтам. Разверните защищенные решения для мобильной печати, чтобы предоставить пользователям удобные возможности печати документов с мобильных устройств без ущерба для безопасности сети.

CSC 13: защита данных

Мера безопасности: предотвращение утечки данных, сведение к минимуму последствий утечки данных и обеспечение целостности и неприкосновенности конфиденциальной информации.

Рекомендация: шифруйте передаваемые данные (задания печати и сканирования, отправляемые на принтер или с принтера) и данные, хранящиеся на жестком диске устройства. Разверните решения для печати с авторизацией, чтобы исключить ситуацию, когда конфиденциальные документы остаются в лотке принтера без присмотра. Обеспечьте надежное уничтожение данных, хранящихся на жестких дисках устройств, перед возвратом арендованного либо перед утилизацией списанного оборудования.

CSC 14: контроль доступа по принципу минимальной необходимости

Мера безопасности: контроль доступа к критически важным активам (например, к информации, ресурсам и системам) в соответствии с формальным определением минимального уровня доступа к данным активам для конкретных сотрудников, компьютеров и приложений; пресечение ненадлежащего использования активов и устранение проблем с безопасностью.

Рекомендация: выбирайте печатающие устройства и решения, поддерживающие возможности аутентификации пользователей и контроля доступа к отдельным функциям в зависимости от должностных обязанностей сотрудника. Интегрируйте различные методы аутентификации (например, по ПИН-коду или персональному идентификационному коду, LDAP и Kerberos) с Active Directory для повышения уровня безопасности и эффективности администрирования. Решения для печати с авторизацией позволяют защитить конфиденциальные документы от попадания в руки злоумышленников.

CSC 15: контроль доступа к беспроводным сетям

Мера безопасности: контроль доступа к беспроводным сетям, точкам доступа и беспроводным клиентским системам, пресечение ненадлежащего использования оборудования и устранение проблем с безопасностью.

Рекомендация: эффективное средство управления безопасностью печати позволит автоматизировать процедуры развертывания и оценки параметров устройств — в том числе параметров беспроводной связи — и устранения несоответствия параметров заданным значениям в масштабах всего парка оборудования. Воспользуйтесь решениями для контроля доступа, чтобы ограничить доступ к отдельным функциям устройств, например возможностям отправки отсканированных документов по электронной почте, в зависимости от должностных обязанностей сотрудников. Разверните защищенные решения для мобильной печати, чтобы предоставить пользователям удобные возможности печати документов с мобильных устройств без ущерба для безопасности сети. Например, если устройство поддерживает одноранговое беспроводное соединение, это позволяет сотрудникам отправлять документы на печать напрямую, без подключения к корпоративной сети.

CSC 16: контроль учетных записей

Мера безопасности: активное администрирование учетных записей на протяжении всего жизненного цикла — от создания до удаления, включая отслеживание активных и неактивных учетных записей — чтобы свести к минимуму возможности злоумышленников для атаки через уязвимости в учетных записях.

Рекомендация: выбирайте печатающие устройства и решения, поддерживающие возможности аутентификации пользователей и контроля доступа к отдельным функциям в зависимости от должностных обязанностей сотрудника. Интегрируйте методы аутентификации с Active Directory, чтобы обеспечить централизованное управление и повысить уровень безопасности. Регулярно просматривайте учетные записи пользователей, отключайте неиспользуемые записи, отслеживайте действия пользователей с помощью решений для мониторинга. Шифруйте имена пользователей и учетные данные, как передаваемые по сети, так и хранящиеся на устройствах. Консультанты по вопросам безопасности помогут вам разработать комплексный план обеспечения безопасности печати, чтобы свести риски к минимуму. Специалисты также помогут вам управлять системой безопасности, в том числе с помощью средств мониторинга и контроля учетных записей.

CSC 17: оценка навыков информационной безопасности и обучение персонала

Мера безопасности: определение конкретных знаний и навыков, необходимых для обеспечения безопасности организации; разработка и внедрение интегрированного плана оценки, выявления и устранения брешей в системе безопасности, включающего разработку корпоративных политик безопасности, организационное планирование, обучение персонала и информационно-просветительские программы в соответствии с должностными обязанностями каждого сотрудника.

Рекомендация: высококвалифицированные консультанты по вопросам безопасности печати помогут вам оценить риски для безопасности, разработать комплексную политику безопасности и план обеспечения безопасности и внедрить необходимые процедуры и технологии. В рамках отдельных услуг по обеспечению безопасности также предусмотрено внешнее управление системой безопасности печати с соблюдением нормативных требований.

CSC 18: безопасность приложений

Мера безопасности: управление безопасностью приложений собственной разработки и приобретенного программного обеспечения на протяжении всего жизненного цикла с целью предотвращения, выявления и устранения уязвимостей в системе безопасности.

Рекомендация: при разработке решений для печати строго придерживайтесь методологий безопасности. Выбирайте программные решения с электронной подписью, гарантирующей их подлинность.

CSC 19: управление инцидентами

Мера безопасности: защита хранящейся в организации информации, а также деловой репутации путем разработки и развертывания эффективной инфраструктуры реагирования на инциденты (включая разработку планов действий, определение ролей сотрудников, обучение персонала, налаживание коммуникаций и надзор).

Рекомендация: включите в план реагирования на инциденты инфраструктуру печати.

CSC 20: испытания на проникновение и отработка действий злоумышленников

Мера безопасности: проверка надежности всех аспектов системы безопасности организации (технологий, процедур и персонала) путем имитации действий злоумышленника.

Рекомендация: при проведении испытаний на проникновение обязательно проверяйте инфраструктуру печати. Регулярно проверяйте инфраструктуру печати на наличие уязвимостей и корректируйте план обеспечения безопасности в соответствии с выявленными недостатками.

Сделайте следующий шаг

Внедрение приведенных в данном документе рекомендаций позволит вам повысить безопасность инфраструктуры печати и обеспечить соблюдение нормативных требований. Требуется помощь? Воспользуйтесь услугами по управлению безопасностью печати, чтобы разработать политику безопасности и внедрить в организации необходимые процедуры и технологии обеспечения безопасности печатающих устройств, документов и данных.

Приложение A. Услуги и решения HP по обеспечению безопасности печати

Средства безопасности, встроенные в устройства HP, а также ведущие в отрасли программные решения и услуги помогут вам обеспечить соблюдение политик безопасности и надежно защитить коммерческую информацию от внешних угроз.

Встроенные средства безопасности принтеров и МФУ HP Enterprise обеспечивают надежную защиту от вредоносных программ и автоматически обнаруживают атаки с последующим восстановлением работоспособности устройства. Средства безопасности HP обеспечивают обнаружение угроз в режиме реального времени, автоматический мониторинг работоспособности устройств печати и встроенную проверку целостности программного обеспечения, что позволяет пресекать атаки на самом раннем этапе[4]. (Позволяет соблюсти рекомендации CSC 2, 4, 6 и 8.) hp.com/go/PrintersThatProtect

Решения HP Access Control поддерживают целый ряд методов аутентификации и средств контроля доступа на основе ролей, что позволяет устранить потенциальные бреши в системе безопасности, а также вести учет использования принтеров. (Позволяет соблюсти рекомендации CSC 5, 7, 10, 12, 13, 14, 15 и 16.) hp.com/go/hpac

Средства шифрования и **решения HP JetAdvantage для электронного документооборота** обеспечивают надежную защиту данных, хранящихся на устройствах HP Enterprise и передаваемых по сети между печатающими устройствами и облачными хранилищами. (Позволяет соблюсти рекомендации CSC 12 и 13.) hp.com/go/upd, hp.com/go/documentmanagement

Решения HP для печати с авторизацией обеспечивают надежную защиту конфиденциальных документов: задания печати хранятся на защищенном сервере, в облачном хранилище или на ПК. Чтобы получить напечатанные документы, пользователь должен пройти проверку подлинности на любом удобном устройстве. (Позволяет соблюсти рекомендации CSC 10, 13 и 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

Решение HP JetAdvantage Connect предоставляет пользователям удобные возможности мобильной печати непосредственно со смартфонов и планшетов без ущерба для безопасности корпоративной сети. (Позволяет соблюсти рекомендации CSC 12 и 15.) hp.com/go/JetAdvantageConnect

Принтеры HP поддерживают возможность отправки событий в системы SIEM, например ArcSight, Splunk и SIEMonster. Ваши специалисты по информационной безопасности могут легко отслеживать состояние устройств печати в рамках более широкой ИТ-инфраструктуры и своевременно принимать необходимые меры. (Позволяет соблюсти рекомендации CSC 4 и 6.)

HP JetAdvantage Security Manager — это единственное в отрасли решение для обеспечения безопасности инфраструктуры печати на основе политик[5]. Данное решение позволяет развернуть единую политику безопасности в масштабах всего парка устройств, автоматизировать процедуру устранения несоответствия параметров устройств заданным значениям, устанавливать и обновлять уникальные сертификаты и формировать отчеты, подтверждающие соблюдение нормативных требований. Технология Instant-On, реализованная в данном решении, автоматически настраивает новые устройства в соответствии с корпоративной политикой безопасности сразу же при их подключении к сети либо после перезагрузки. (Позволяет соблюсти рекомендации CSC 1, 2, 3, 4, 5, 6, 8, 9, 11 и 15.) hp.com/go/securitymanager

Услуги HP по аутсорсингу и управлению инфраструктурой печати обеспечивают самую надежную в отрасли систему безопасности печати[6]. Обеспечение безопасности печати может оказаться весьма нетривиальной задачей. Положитесь на специалистов HP, которые обеспечат эффективное управление вашей инфраструктурой печати с помощью комплексных решений, охватывающих сотрудников компании, бизнес-процессы и требования политик безопасности. (Позволяет соблюсти рекомендации CSC 2, 3, 12, 16, 17, 18 и 19.) hp.com/go/SecureMPS

В рамках профессиональных услуг HP по обеспечению безопасности печати эксперты по безопасности помогут вам оценить вашу инфраструктуру печати, развернуть политики безопасности и поддерживать план обеспечения безопасности в актуальном состоянии. Специалисты HP также могут взять на себя обязанности по обеспечению политики безопасности к безопасности печати в вашей организации. (Позволяет соблюсти рекомендации CSC 2, 3, 12, 16, 17 и 19.) hp.com/go/SecureMPS

Примечания

[1] Исследование Ponemon по заказу HPE: «2016 Cost of Cyber Crime Study & the Risk of Business Innovation» («Потери в результате кибератак и уровень риска бизнес-инноваций в 2016 году»), 2016.

[2] Отчет RiskBased Security «The 2016 Year End Data Breach QuickView» («Краткий обзор фактов утечки данных в 2016 году»), январь 2017.

[3] 26,2% опрошенных сталкивались с серьезными проблемами в системе безопасности, требовавшими срочного устранения, и в более чем 26,1% случаев эти атаки и потери были связаны с печатающими устройствами. Опрос IDC «Безопасность ИТ-инфраструктур и систем печати — 2015», #US40612015, сентябрь 2015 г.

[4] Для устройств HP Enterprise, представленным в начале 2015 г.; по данным анализа встроенных средств безопасности конкурирующих принтеров аналогичного класса, проведенного компанией HP в 2016 г. Только HP предоставляет набор средств безопасности, обеспечивающих проверку целостности на уровне BIOS и поддерживающих возможности самовосстановления. Для активации функций безопасности может потребоваться установка пакета обновления FutureSmart. Список совместимых устройств см. по адресу hp.com/go/PrintersThatProtect. Дополнительные сведения см. по адресу hp.com/go/printersecurityclaims.

[5] Решение HP JetAdvantage Security Manager приобретается отдельно. Дополнительные сведения см. по адресу hp.com/go/securitymanager. Утверждение сделано по данным внутренних исследований HP предложений конкурентов (сравнительный анализ решений для обеспечения безопасности устройств, январь 2015 г.) и отчета о решении HP JetAdvantage Security Manager 2.1 независимой лаборатории Buyers Laboratory LLC, февраль 2015 г.

[6] Рассматривались средства обеспечения безопасности устройств, документов и иных данных, предоставляемые ведущими поставщиками услуг по управлению ресурсами печати. По данным анализа услуг безопасности, программных решений для обеспечения безопасности и администрирования и встроенных средств безопасности для конкурирующих принтеров аналогичного класса, проведенного компанией HP в 2015-2016 гг. Дополнительные сведения см. по адресам hp.com/go/MPSsecurityclaims и hp.com/go/mps.

Подпишитесь на информационные бюллетени HP
hp.com/go/getupdated

Поделиться с коллегами

4AA6-8821RUE, Июнь 2017 г., ред. 1