Стандарт FIPS 140-2 и технология самошифрования

Маркетинговый бюллетень

Вопросы и ответы

Что такое FIPS 140-2?

FIPS (федеральный стандарт по обработке информации) 140-2 — это государственный стандарт США, описывающий требования к шифрованию и связанным с ним мерам безопасности в ИТ-продуктах, которые используются для обработки данных класса «sensitive but unclassified» (конфиденциальные, но не секретные).

Проверка на соответствие стандарту FIPS 140-2 — это программа тестирования и сертификации, удостоверяющая соответствие продуктов требованиям стандарта FIPS 140-2. Национальный институт стандартов и технологий США (NIST) утвердил программу проверки модулей шифрования для проверки продуктов на соответствие требованиям стандарта.

Какие требования определяет стандарт FIPS 140-2?

Стандарт определяет использование в продуктах надежных методик безопасности, включая утвержденные алгоритмы и методы стойкого шифрования. Кроме того, стандарт описывает работу пользователей и процессов для использования продуктов, а также правила проектирования модулей и компонентов для безопасного взаимодействия с другими системами.

Почему шифрование необходимо?

Жесткие диски постоянно выводятся из эксплуатации (возвращаются по гарантии, на ремонт или по истечении аренды, устанавливаются для использования в другие системы или продаются), они могут быть утеряны или украдены. Если незащищенные данные выходят из-под контроля владельца и попадают в чужие руки, компания может потерять прибыль, лишиться своего положения на рынке и утратить доверие клиентов. Компания также может подвергнуться судебному преследованию за нарушение законов о защите конфиденциальности данных. Это может повлечь крайне тяжелые последствия для любой организации, особенно для предприятий малого и среднего бизнеса.

Стандарт FIPS 140-2 и технология самошифрования

По оценкам компании Seagate, каждый день за пределы центров обработки данных перемещается приблизительно 50 000 жестких дисков с терабайтами данных. По оценкам компании IBM, 90% жестких дисков, возвращенных по гарантии, содержат данные, которые можно прочитать. Ведущие отраслевые исследовательские организации, такие как институт Ponemon, считают, что ущерб от утечки данных возрастает с каждым годом. Величина такого ущерба в 2008 году составляла в среднем 6,6 миллионов долларов, или 202 доллара на каждую единицу информации, вышедшую из-под контроля[1].

По данным института Ponemon, на 81% ноутбуков хранятся конфиденциальные данные, а 10% всех ноутбуков бывают утеряны или украдены за время своего использования. Кроме того, только в аэропортах США количество утерянных или украденных ноутбуков достигает 12 тыс. еженедельно. Средний ущерб для бизнеса при пропаже ноутбука, содержащего конфиденциальные, но незашифрованные данные, достигает 50 тыс. долларов. В исключительных случаях размер ущерба может достигать 1 миллиона долларов[2].

Какие уровни предусмотрены стандартом FIPS 140-2?

Стандарт FIPS 140-2 определяет 4 уровня безопасности. В ходе проверки соответствия стандарту FIPS 140-2 указывается уровень безопасности, которому соответствует продукт.

- Уровень 1 обычно используется только для программных продуктов шифрования и предполагает весьма ограниченные требования к безопасности. Все компоненты должны быть профессионального уровня, не должно быть различных грубых нарушений безопасности.
- Для уровня 2 требуется аутентификация на основе ролей. (Индивидуальная проверка подлинности пользователей не требуется.) Также требуется способность обнаруживать физическое проникновение — для этого применяются физические замки или пломбы, защищающие от несанкционированного вскрытия.
- Уровень 3 добавляет требование устойчивости к физическому проникновению, разборке или модификации систем, что значительно затрудняет попытки добыть информацию. При обнаружении проникновения устройство должно быть способно стереть важнейшие параметры безопасности.

  Уровень 3 также предусматривает стойкое шифрование, управление ключами, аутентификацию на основе личных данных пользователей, физическое и логическое разделение интерфейсов, при помощи которых важные параметры безопасности вводятся в систему и выводятся из нее.
- Уровень 4 требует усовершенствованной защиты от проникновения. Этот уровень предназначен для продуктов, работающих в физически незащищенной среде.

Какой уровень стандарта FIPS 140-2 имеет компания Seagate?

Жесткие диски Seagate® с самошифрованием сертифицированы на соответствие стандарту FIPS 140-2 уровня 2.

Зачем компания Seagate прошла сертификацию по стандарту FIPS 140-2 уровня 2?

Организациям всех видов все чаще требуется шифрование хранящихся данных для защиты от утери или кражи. Сертификация по стандарту FIPS 140-2 уровня 2 подтверждает высокое качество и безопасность продуктов, гарантирует всем покупателям, что жесткие диски Seagate с самошифрованием по стандарту FIPS соответствуют федеральным требованиям США для продуктов в области безопасности.

Как узнать, соответствует ли мое устройство хранения данных Seagate стандарту FIPS-2?

В каждом устройстве, соответствующем стандарту FIPS 140-2, используются физические механизмы защиты для обнаружения физического проникновения. Если ваше устройство хранения данных соответствует стандарту FIPS-2, на нем должна присутствовать защитная наклейка.

Как настроить диск Seagate с самошифрованием по стандарту FIPS для соответствия стандарту FIPS-2?

Сведения о настройке устройства, соответствующего стандарту FIPS 140-2, см. в документе «Политика безопасности» на веб-сайте «Список проверенных модулей» Института NIST по адресу http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm. Подробная процедура инициализации устройства описана в разделе «Инициализация модуля безопасности» документа «Политика безопасности».

На какие типы продуктов распространяется стандарт FIPS 140-2?

Стандарт FIPS 140-2 применяется ко всем продуктам, выполняющим хранение или передачу конфиденциальных данных. В частности, стандарт касается оборудования, например, модулей шифрования, жестких дисков, флэш-накопителей и других съемных носителей информации. Также стандарт распространяется на программные продукты, шифрующие данные во время их передачи или хранения.

[1] Институт Ponemon, 2008 *Annual Study: U.S. Cost of a Data Breach*, февраль 2009 г., www.ponemon.org, приводится по тексту в статье *Data-breach costs rising, study finds*, Эллен Месмер (Ellen Messmer), Network World, 2 февраля 2009 г.

[2] Исследование компании Intel: Stolen Laptops Cost to Business; журнал eWeek, 23 апреля 2009 г.; исследование института Ponemon, апрель 2009 г.

Стандарт FIPS 140-2 и технология самошифрования

Действительно ли нужен такой уровень безопасности? Разве пароля операционной системы недостаточно?

Меры безопасности операционной системы, такие как ввод пароля, можно легко обойти: для этого достаточно извлечь жесткий диск из компьютера и подключить его к другому компьютеру. Даже хранение паролей жестких дисков с интерфейсом ATA в BIOS компьютера являются уязвимым, если использовать его с обычными жесткими дисками, а не с жесткими дисками Seagate с самошифрованием. Шифрование данных на жестких дисках или других носителях информации является надежным способом защиты данных.

Какие организации или компании должны выполнять нормы стандарта FIPS 140-2?

В США, согласно требованию Национального института стандартов и технологий (NIST), все федеральные учреждения должны использовать продукты, сертифицированные по стандарту FIPS 140-2 уровня 2, для защиты данных класса *sensitive but unclassified* (конфиденциальные, но не секретные) в компьютерных системах и системах связи (включая системы голосовой связи)[3]. В Канаде, согласно требованию Управления защиты связи (CSE), федеральные учреждения должны использовать модули шифрования, сертифицированные по стандарту FIPS 140-2 уровня 2, для защиты данных класса *Protected Information* (защищенные данные) (типа A или B) в компьютерных системах и системах связи (включая системы голосовой связи). Соответствие стандарту FIPS 140 необходимо для того, чтобы продукт с шифрованием был указан в списке продуктов, отвечающих требованиям по ИТ-безопасности правительства Канады[3]. В Великобритании Группа по безопасности связи и электронного оборудования (Communications-Electronics Security Group) рекомендует использовать модули шифрования, сертифицированные по стандарту FIPS 140[4].

Компании во всем мире, работающие по контракту с федеральными государственными учреждениями США, Канады и Великобритании, в которых требуется шифрование по стандарту FIPS 140-2, также обязаны соблюдать требования этого стандарта. Коммерческие компании, особенно в области финансов, здравоохранения, образования и инфраструктуры (национальной безопасности), во всем мире все чаще требуют соблюдения стандарта FIPS 140-2. Таким компаниям необходимы самые надежные стандарты защиты данных. Компании признают надежность сертификации по стандарту FIPS 140-2, используют его для шифрования своих данных и выбирают в качестве основного стандарта безопасности.

www.seagate.com

Что необходимо для получения сертификата FIPS 140-2?

Для получения сертификата FIPS 140-2 продукт должен соответствовать установленным стандартам по конструкции и изготовлению и должен быть проверен и утвержден одной из 13 независимых лабораторий, аккредитованных Национальным институтом стандартов и технологий (NIST).

Какой из стандартов FIPS 140 действует в настоящее время?

Публикации FIPS серии 140 представляют собой набор стандартов безопасности, касающихся требований к модулям шифрования. Стандарт FIPS 140-1 был выпущен в 1994 году, но ему на смену пришел стандарт FIPS 140-2, который был выпущен в 2001 году и используется в настоящее время. FIPS 140-3 — это новая версия стандарта, ее разработка началась в 2005 году. Черновой вариант этого стандарта вышел в декабре 2009 года, но еще не применялся для проверки продуктов.

Существует ли список продуктов, проверенных на соответствие стандарту FIPS 140-2?

Национальный институт стандартов и технологий (NIST) поддерживает список всех коммерческих продуктов, проверенных на соответствие стандарту FIPS 140-2.

См.: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

[3] http://csrc.nist.gov/groups/STM/cmvp/index.html

[4] www.cesg.gov.uk/

FIPS 140-2 Inside

СЕВЕРНАЯ И ЮЖНАЯ АМЕРИКА Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, +1 408 658 10 00
АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, +65 6485 3888
ЕВРОПА, БЛИЖНИЙ ВОСТОК И АФРИКА Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00

© Seagate Technology LLC, 2013. Все права защищены. Отпечатано в США. Seagate, Seagate Technology и логотип Wave являются зарегистрированными товарными знаками компании Seagate Technology LLC в США и других странах. Логотип FIPS — знак сертификации Национального института стандартов и технологий США (NIST). Он не подразумевает одобрения продукта Институтом NIST либо правительством США или Канады. Прочие товарные знаки или зарегистрированные товарные знаки являются собственностью соответствующих владельцев. Экспорт и реэкспорт программных и аппаратных продуктов с технологиями шифрования может находиться в ведении Бюро промышленности и безопасности Министерства торговли США (дополнительную информацию см. на веб-узле www.bis.doc.gov). Импорт и использование таких технологий за пределами США могут быть ограничены. Компания Seagate оставляет за собой право изменять ассортимент и характеристики своих продуктов без предварительного уведомления. MB605.2-1302RU, февраль 2013 г.