

## Toshiba EasyGuard Carefree Mobile Computing

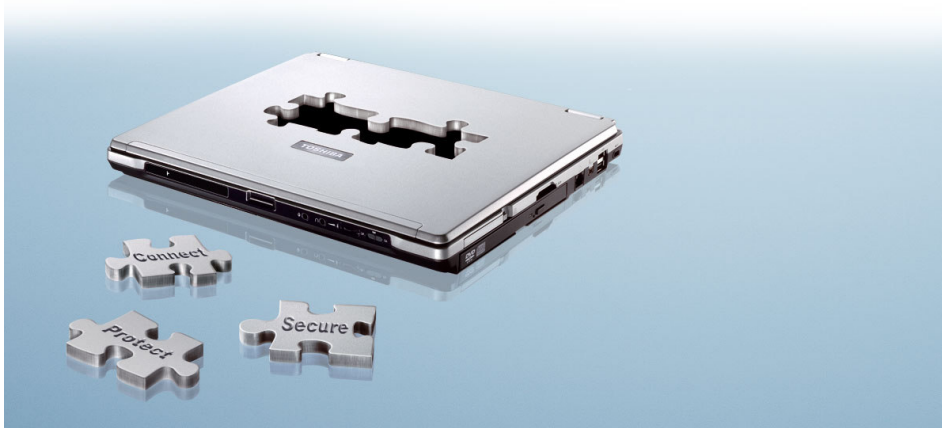


Toshiba EasyGuard — это наилучший способ обеспечения безопасности данных, самая современная системная защита и максимальная легкость подключения. Относящийся к новейшему поколению достижений в области вычислительной техники, этот системный пакет включает в себя технологии, обеспечивающие оптимальное подключение и безопасность, а также последние разработки специалистов Toshiba, направленные на защиту от случайных сбоев, и современное программное обеспечение, устраняющее какие бы то ни было проблемы при эксплуатации мобильных компьютерных устройств.

### Три ключевых элемента обеспечения надежной работы мобильных компьютерных устройств

Отвечая на растущую потребность в совершенствовании средств защиты данных и обеспечении легкости подключения, мы предлагаем систему Toshiba EasyGuard, характерные особенности которой могут быть разделены на три ключевые группы:

**Безопасность** — Функции, повышающие безопасность компьютера и хранящихся в нем данных



© Toshiba Europe GmbH, 2005. Специалисты Toshiba при подготовке данного документа к публикации приложили все необходимые усилия для обеспечения адекватности приведенной в нем информации, однако сведения о спецификациях изделий, их конфигурации, ценах и наличии систем, компонентов или опций в определенных регионах могут быть изменены без предварительного уведомления. Для получения новейшей информации, имеющей отношение к Вашему компьютеру, а также для того, чтобы быть в курсе последних достижений в области программного обеспечения и аппаратных средств, посетите web-сайт Toshiba по адресу: [www.toshiba-europe.com](http://www.toshiba-europe.com).

### Механические средства защиты и устранение неполадок

Средства защиты, предусмотренные в конструкции ноутбуков и программная диагностика для увеличения времени эксплуатации устройств

### Подключение

Функции и программные средства, обеспечивающие простое и надежное подключение по проводным и беспроводным каналам

### Что такое модуль TPM?

Модуль TPM (Trusted Platform Module) — микросхема защищенной памяти, в которой хранятся уникальная пара ключей PKI (Public Key Infrastructure) и учетные данные. Иными словами, это идеальный "сейф", в котором можно держать ключи от зашифрованных данных. Модуль TPM, малый контроллер обеспечения безопасности, был разработан в соответствии с промышленными стандартами, подготовленными организацией TCG (Trusted Computing Group); он обеспечивает соответствие стандарту обеспечения безопасности компьютерных платформ.



### Как работает модуль TPM

Большинство современных решений в области защиты информации являются программными, поэтому они не обеспечивают должную степень защиты и уязвимы для физического доступа и/или атак хакеров. Модуль TPM, в противоположность этому, является как аппаратным, так и программным средством обеспечения безопасности. Он включен в последовательность



Модуль TPM - решение, разработанное компанией Infineon, включает в себя защитную микросхему и программное обеспечение, формирующее более безопасную подсистему компьютерных платформ.

загрузки компьютера, а также интегрирован с операционной системой. Хотя модуль TPM физически отделен от основного процессора, он, тем не менее, связан с материнской платой ноутбука.

Основой этого решения является аппаратное защищенное хранилище данных. После создания системными программами ключа или сертификата шифрованных данных эти ключи или сертификаты изолируются в модуле TPM. Сохраняемая информация позволяет при необходимости идентифицировать платформу и удостовериться в ее целостности, а также передать пользователю и его партнерам (например, поставщикам онлайн-информации) сведения о состоянии аппаратной и программной среды. Сведения предоставляется на основе уникальной платформы, уникальность которой, в свою очередь, обеспечивается ключами, хранящимися в модуле TPM.

Каждой микросхеме TPM присвоен индивидуальный номер, однако пользователь идентифицируется не по этому номеру, а по ключам и идентификационным кодам, хранящимся в модуле TPM. В результате модуль TPM может противостоять несанкционированному доступу и атакам хакеров, защищая сохраняемые в нем ключи и учетные данные.

Наивысший уровень защиты может быть достигнут при использовании двойной системы идентификации, при которой модуль TPM применяется как для идентификации платформы, так и для идентификации пользователя по ключу USB или по метке SD. Такая идентификация может осуществляться только раздельно, поскольку, например, метка SD не может храниться в модуле TPM.

## Какие приложения можно использовать совместно с модулем TPM?

- ▶ Шифрование файлов и папок
  - Система шифрования файлов Windows EFS
  - Виртуальный шифрованный диск (личный защищенный диск)
- ▶ Защищенная электронная почта
  - Версии Outlook, Outlook Express и Netscape Communicator, в которых поддерживаются функции цифровой подписи и шифрования почты.
- ▶ Защита Интернета
  - в Internet Explorer и Netscape Communicator с поддержкой протоколов защиты (SSL)
- ▶ Другие приложения
  - Виртуальные частные сети (VPN)
  - Разовые пароли (например, RSA SecurID)
  - Идентификация клиента

## Краткие сведения о функциях и преимуществах модуля TPM

- ▶ Модуль TPM (Trusted Platform Module) Защита секретных данных, шифрование и цифровая подпись для обеспечения конфиденциальности и безопасности информации пользователя
- ▶ Аппаратно-программное решение Способность противостоять логическим и физическим атакам на защищенные ключи и учетные данные
- ▶ Соответствие стандартам (например, TCG) Возможность использования функции на различных платформах