

## Toshiba EasyGuard Carefree Mobile Computing

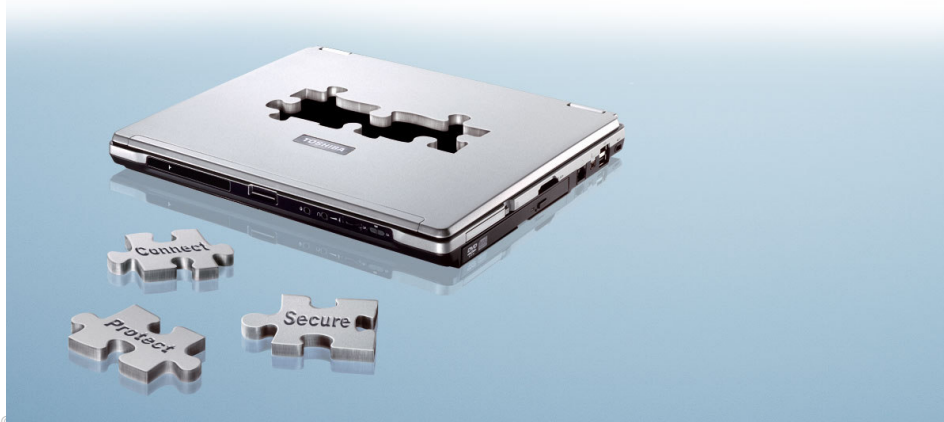


Toshiba EasyGuard — это наилучший способ обеспечения безопасности данных, самая современная системная защита и максимальная легкость подключения. Относящийся к новейшему поколению достижений в области вычислительной техники, этот системный пакет включает в себя технологии, обеспечивающие оптимальное 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



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 бит XD (Execute Disable Bit)?

Бит XD (Execute Disable Bit) — это системная функция, при наличии и активизации которой процессор ноутбука способен различать коды, которые исполнять можно, от кодов, представляющих собой опасность для компьютера.



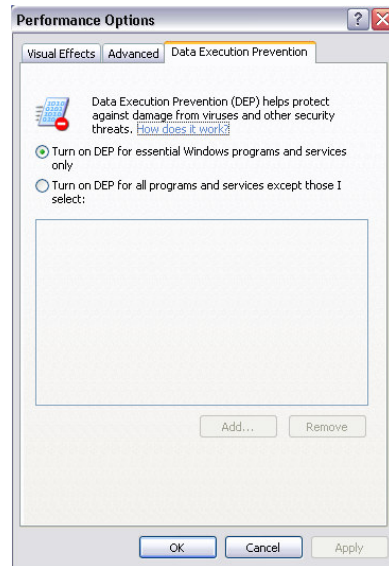
Если программный "червь" пытается установить свой код в буфер, процессор отключает выполнение кода, предупреждая дальнейшее распространение инфицирующей программы. Иными словами, даже если на ноутбуке установлена инфицированная программа, она не может причинить вреда до тех пор, пока она не будет выполнена процессором. Защита, при которой системный процессор отключает исполнение кода, называется также DEP (Data Execution Protection).

## Что такое аппаратная защита DEP и как она работает?

Защита DEP (Data Execution Protection) может быть либо аппаратной, при которой необходима ее поддержка оборудованием, либо программной, для которой нужна дополнительная проверка исключений; специального оборудования при этом не требуется. (Для аппаратной защиты DEP необходим процессор, на котором исполняется соответствующая функция, установленная корпорацией Intel для Execute Disable Bit.)

При защите DEP все адреса в памяти процессора помечаются как неисполняемые, если только в этих адресах не содержится в явном виде исполняемый код. При некоторых разновидностях атак на систему безопасности предпринимаются попытки ввести исполняемый код из неисполняемых адресов памяти. Защита DEP помогает предотвратить подобные атаки, перехватывая эти попытки и инициируя исключения. Кроме того, система DEP с помощью процессора помечает адреса памяти атрибутом, показывающим, что код, содержащийся в этих адресах, не должен исполняться. В операционной системе Windows XP SP 2 это исключение распознается, после чего исполнение указанного кода запрещается.

В 32-разрядной версии Windows (начиная с Windows XP SP 2) применяется функция Execute Disable Bit в виде, установленном корпорацией Intel, если процессор ноутбука работает в расширенном режиме PAE (Physical Address Extension).



## Конфигурации защиты DEP для Windows XP SP2

- ▶ **Opt-in (принять):** Защита DEP включена по умолчанию для отдельных системных и программных приложений, которые могут ее «принять», и доступна на компьютерах с процессорами, предназначенными для аппаратной защиты DEP. Служба технической поддержки может включить защиту DEP для дополнительных приложений.
- ▶ **Opt-out (отклонить):** Защита DEP включена по умолчанию для всех процессов. Пользователь может вручную создать список приложений, не поддерживающих DEP, используя окно «Свойства системы».
- ▶ **Всегда включена:** Полный охват всей системы и всех процессов включенной защитой DEP. «Отклонить» использование DEP невозможно.
- ▶ **Всегда выключена:** Защита DEP в системе отсутствует.

## Краткие сведения о функциях защиты и их преимуществах

- ▶ **Бит XD (Execute Disable Bit)** Предотвращение вирусных атак, провоцирующих переполнение буфера, путем придания процессору компьютера способности отличать код, который следует исполнять, от кода, который не должен исполняться
- ▶ **Защита DEP (Data Execution Protection)** Процесс, позволяющий системному процессору отключать исполнение кода для предотвращения негативных последствий от деятельности вирусов или для препятствования распространению программ - "червей"
- ▶ **Четыре настройки DEP** Гибкость применения

