

# BitLocker: новое средство защиты данных в Windows Server 2008

**Андрей Бирюков**

Информация всегда нуждается в защите. В этой статье я опишу основные возможности, установку и настройку BitLocker.

## Суть проблемы

Современные информационные системы, в частности серверы и приложения, располагают множеством различных средств для защиты информации, таких как разграничение доступа для пользователей и групп, списки доступа Access Control Lists, межсетевые экраны, антивирусы и прочее. Все эти средства при грамотной настройке могут быть вполне эффективны против проникновения хакера, однако они практически бесполезны при банальном хищении физического устройства. К примеру, при ненадлежащей работе охраны из серверной могут украсть сервер, содержащий конфиденциальную информацию, или, что гораздо более распространено, могут украсть ноутбук у сотрудника, находящегося в командировке, с не менее критичными для бизнеса данными. На новостных порталах периодически появляются сообщения о том, что у сотрудника той или иной компании украли ноутбук, в результате чего были похищены конфиденциальные данные миллионов пользователей. А далее существует множество способов, как обойти защиту на похищенном устройстве. В простейшем случае можно воспользоваться загрузочным диском Knopix или аналогичной LiveCD-системой и считать конфиденциальные данные на файловом уровне, или же подключить жесткий диск вторым в компьютер под управлением Windows.

Для решения данной проблемы нужно использовать шифрование. Существует множество решений от различных компаний. Большинство этих решений предназначено для крупных предприятий и отвечают определенным требованиям к средствам криптографической защиты, предъявляемым российским законодательством. Для государственных предприятий и банков только такие средства криптографической защиты могут использоваться для шифрования. Однако для небольших частных организаций нет необходимости использовать столь громоздкие и дорогие средства шифрования. Альтернативой им может стать BitLocker – новое средство шифрования данных в Windows Server 2008 и Vista.

Продукт является логическим продолжением такого известного средства защиты, имевшегося в предыдущих версиях Windows, как шифрующей файловой системы EFS (Encrypted File System). Однако в отличие от дан-

ного средства BitLocker позволяет шифровать разделы Windows целиком, а также контролировать целостность системных файлов до запуска операционной системы, тем самым предотвращая внедрение вредоносного кода (например, rootkit) на этапе загрузки. Для реализации данного функционала требуется аппаратная поддержка, о которой мы поговорим позже. Также работа BitLocker абсолютно прозрачна для пользователя и не занимает много системных ресурсов. Помимо файлов, BitLocker также шифрует реестр, файлы спящего режима и подкачки. В качестве алгоритма шифрования здесь используется AES с 128-битным ключом по умолчанию, который при необходимости можно увеличить до 256 бит. Также следует отметить, что BitLocker входит в состав операционной системы и соответственно не требует никаких дополнительных расходов на покупку.

## Установка

BitLocker не устанавливается по умолчанию, поэтому утилиту необходимо доустановить. Сделать это можно следующим образом. Установив диск с дистрибутивом Windows Server 2008, выберите Server Management, затем

нужно добавить опцию Add feature (см. рис. 1).

В открывшемся списке выбираем BitLocker (см. рис. 2). После успешной установки необходимо перегрузить сервер.

Но на этом предварительные действия не заканчиваются. Наибольшей эффективности от использования BitLocker можно добиться, если плата поддерживает технологию Trusted Platform Module (TPM). Данная функция является программно-аппаратным решением, позволяющим использовать более мощные средства защиты информации и шифрования. TPM обычно устанавливается на материнскую плату компьютера или ноутбука и взаимодействует с операционной системой с помощью аппаратной шины. Компьютеры с TPM могут создавать криптографические ключи и шифровать, причем расшифровать данные ключи можно будет только на машине с установленным TPM. Этот процесс часто называют wrapping (завертывание) ключа, то есть это дополнительное средство защиты, предназначенное только для хранения. Каждый TPM имеет свой корневой Root wrapping key, называемый также Storage Root Key (SRK), который хранится в самом TPM. Еще одной отличительной особенностью TPM является то, что данные ключи не хранятся в памяти операционной системы, а хранятся в специальном аппаратном разделе. Это также позволяет защитить ключ от дискредитации. Основным недостатком данной технологии является ее аппаратная зависимость, что существенно сужает ее область применения, так как далеко не все оборудование поддерживает TPM.

Для включения TPM необходимо запустить консоль управления tpm.msc. В открывшемся окне нужно выбрать Initialize TPM. Далее запустится инициализация TPM. Затем вам будет предложено указать пароль владельца TPM owner password. Затем необходимо перезагрузиться и в процессе перезагрузки произвести реконфигурацию BIOS. После перезагрузки необходимо снова запустить TPM Initialization Wizard. В открывшемся окне создайте новый пароль владельца TPM и сохраните файл с паролем на сменный носитель, который, естественно, нужно хранить в безопасном месте. Затем наж-

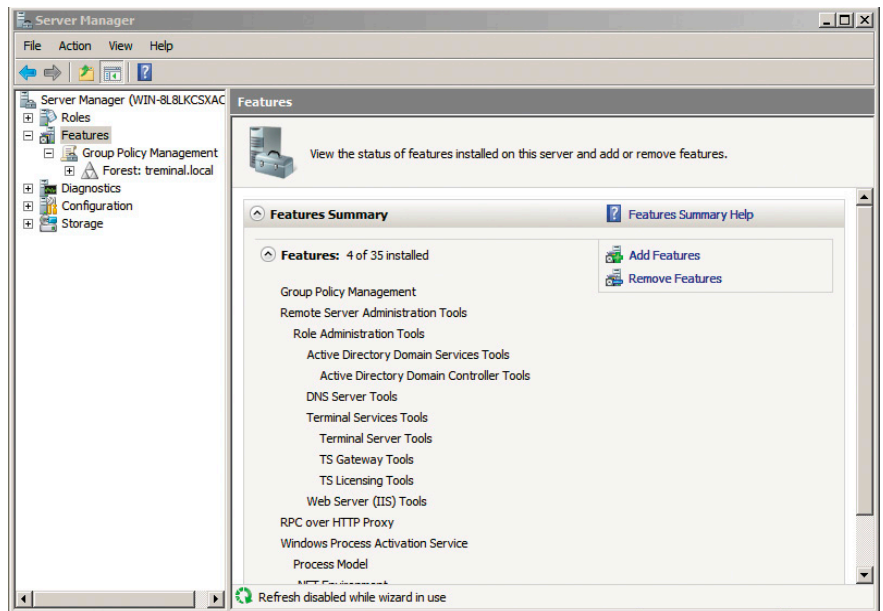


Рисунок 1. Меню добавления опций

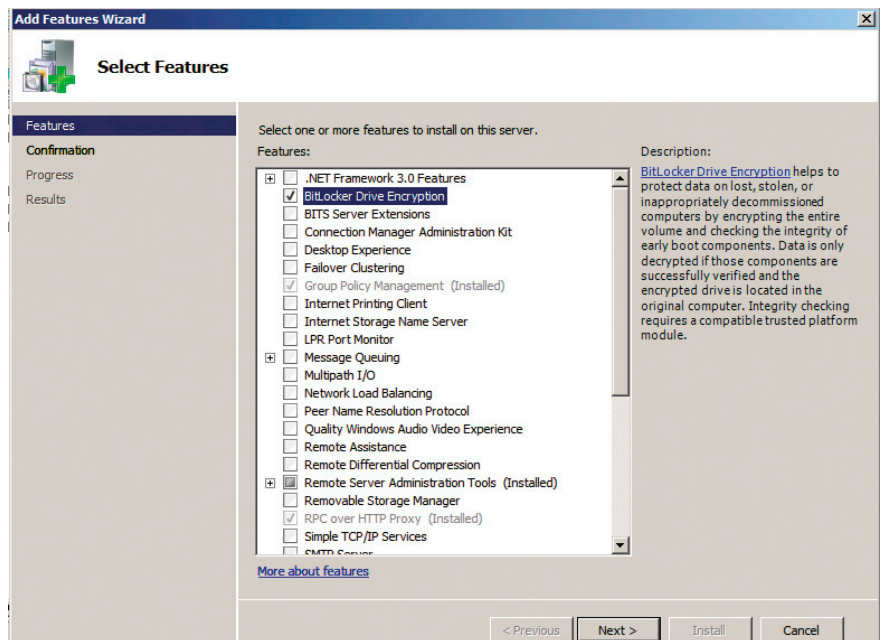


Рисунок 2. Выбор опции для установки BitLocker

мите Initialize. На этом настройку TPM мы завершаем, однако далее я еще вернусь к описанию работы с TPM.

## Включение и настройка

Следующий этап – это непосредственное включение BitLocker. Хочу отметить, что наличие TPM является желательным условием для функционирования BitLocker, так что крайне желательно иметь в сети хотя бы один сервер, поддерживающий данное оборудование.

Для запуска BitLocker нужно зайти в Control Panel, далее раздел Security, и BitLocker. На странице BitLocker Drive

Encryption, выберите Turn On BitLocker для выбранного диска. В разделе Save the recovery password необходимо выбрать один из трех способов сохранения. Пароль можно сохранить на USB drive, либо в папку, или же распечатать (см. рис. 3).

Думаю, сохранение на переносной носитель является наиболее безопасным вариантом. Следует пояснить, о каком пароле для восстановления идет речь. Данный пароль может потребоваться в случае, когда, к примеру, системный раздел вашего сервера поврежден и вам необходимо скопировать зашифрованные

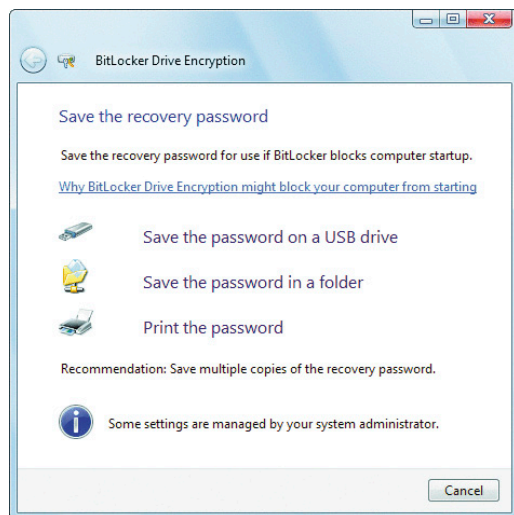


Рисунок 3. Сохранение пароля восстановления

данные в другое место, но предварительно их необходимо расшифровать. Сделать это можно с помощью recovery Password.

Затем запускаем BitLocker, нажав Run BitLocker System Check. После этого вы можете наблюдать процесс шифрования содержимого выбранного диска. После окончания шифрования ваши данные будут доступны только после загрузки системы. В случае каких-либо сбоев при загрузке системы BitLocker перейдет в режим восстановления, и зашифрованные данные станут доступны только после ввода пароля для восстановления.

## Варианты реализации

Итак, мы рассмотрели наиболее оптимальный и рекомендованный пример использования BitLocker. Однако в отличие от своего предшественника EFS (Encrypted File System) здесь появился целый ряд новых функций и возможностей. Рассмотрим более подробно некоторые из них.

Прежде всего необходимо рассмотреть ситуацию с применением

BitLocker на рабочих станциях, аппаратные компоненты которых не поддерживают TPM. Думаю, в ближайшее время это будет наиболее распространенный способ развертывания BitLocker, так как вряд ли платы с поддержкой TPM широко используются в офисных серверах и рабочих станциях.

Если ваш компьютер не поддерживает TPM, то Windows вам не даст выполнить те действия по настройке BitLocker, которые я приводил ранее. Для того чтобы включить BitLocker, вам потребу-

ется USB-носитель и наличие в BIOS возможности загрузки с него. Далее выполните следующие действия: запустите gpedit.msc, затем выберите Group Policy Object Editor, Administrative Templates, Windows Components. После этого выберите шифрование диска BitLocker Encryption. Дважды щелкните настройку «Установка панели управления: включить параметры запуска». В открывшемся окне выберите вариант «Разрешить использование BitLocker без совместимого TPM» и нажмите «OK». Теперь вместо TPM можно использовать ключ запуска. Теперь достаточно обновить политику безопасности с помощью команды «groupupdate.exe /force».

Еще один важный момент, на который следует обратить внимание, – это правильная настройка томов. Для работы BitLocker требуется, чтобы активный раздел был не зашифрован. Это необходимо для считывания загрузочного сектора, диспетчера загрузки и загрузчика Windows (эти компоненты защищаются средствами проверки целостности системы, о кото-

рых я уже упоминал выше). Поскольку другие компоненты Windows могут нуждаться во временном доступе к активному разделу, корпорация Microsoft рекомендует отводить ему не меньше 1,5 ГБ, к тому же многие программы при установке могут доставлять свои компоненты в активный раздел. Также не помешает настроить разрешения NTFS, чтобы пользователи не смогли случайно или специально записать данные на этот том.

Сама операционная система Windows будет установлена на другой, больший том, который можно зашифровать. Если установка Windows производится на новый компьютер, можно вручную настроить тома в соответствии с инструкциями, приведенными в «Пошаговом руководстве шифрования дисков Windows BitLocker» на странице Microsoft Technet [1].

Для подготовки системы можно использовать средство подготовки диска для BitLocker. Это средство берет на себя все заботы по настройке дисков. Оно доступно в нескольких редакциях Windows Vista, а также Windows 2008. Подробные инструкции по использованию этого средства см. в статье базы знаний [2]. Средство подготовки автоматически уменьшает размер тома (если он один), создает второй раздел, делает его активным, вносит все необходимые изменения в конфигурацию и переносит загрузочные файлы в нужное место. После настройки томов включить BitLocker не составляет труда. Для этого в разделе «Security» панели управления щелкните значок шифрования дисков BitLocker.

## Заключение

Итак, в этой статье мы рассмотрели новое средство защиты информации в Windows Server 2008 – BitLocker. Данная утилита позволяет существенно увеличить защищенность данных, хранящихся на ваших серверах и рабочих станциях, так что она будет полезна системным администраторам.

1. <http://technet.microsoft.com/en-us/windowsvista/aa905065.aspx> – страница BitLocker в Microsoft TechNet.
2. <http://support.microsoft.com/kb/930063> – Description of the BitLocker Drive Preparation Tool.



Рисунок 4. Шифрование диска с помощью BitLocker