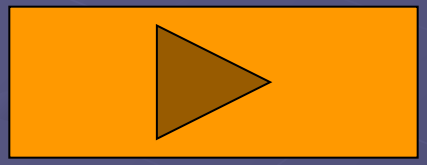
Получение навыков криптографической защиты данных на примере программного продукта PGPdisk

Цель: Научиться пользоваться технологией криптографической защиты данных на примере PGPdisk

Начать показ слайдов



По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

Теоретическая часть

PGPdisk - удобное в работе приложение кодирования, которое дает возможность Вам выделить область из дискового пространства для того, чтобы сохранять ваши конфиденциальные данные. Это зарезервированное место используется, чтобы создать файл названный *томом PGPdisk*.

Хотя это отдельный файл, том PGPdisk действует подобно жесткому диску и Вы можете использовать это пространство для хранения Ваших файлов и приложений. Когда том PGPdisk демонтирован, его содержимое хранится в зашифрованном файле и недоступно, пока том не смонтирован. Файл содержащий том PGPdisk может быть сохранен на любом дисководе в вашей системе.

Когда том PGPdisk смонтирован, он появляется как пустой дисковод в окне Windows Explorer, так что Вы можете начать работать с ним немедленно.

ЗАПУСК PGPdisk

1. Щелкните по значку PGPtray.
2. Выберете пункт PGPdisk.

Команды Меню PGPdisk:

- **Mount Disk: монтирует указанный том PGPdisk при условии правильного ввода пароля;**
- **New Disk: создает новый том PGPdisk при помощи Мастера;**
- **Edit Disk: открывает Редактор PGPdisk, где Вы можете выполнить административные задачи с томом PGPdisk;**
- **Unmount All Disks: демонтирует все существующие тома PGPdisk и хранит их в зашифрованном формате.**

РАБОТА С PGPdisk В WINDOWS EXPLORER

Вы можете использовать Windows Explorer чтобы выполнить некоторые операции PGPdisk:

- **Монтирование тома PGPdisk;**
- **Демонтирование тома PGPdisk;**
- **Создание, копирование, перемещение, и удаление файлов и папок, сохраненных на вашем томе PGPdisk;**
- **Запуск Редактора PGPdisk.**

Чтобы *смонтировать том PGPdisk в Windows Explorer* необходимо:

1. Найти зашифрованный файл тома, который Вы хотите смонтировать, в окне Windows Explorer.
2. Щелкнуть правой кнопкой мыши на имени зашифрованного файла тома.
3. Выбрать PGP—>Mount PGPdisk.
4. Ввести пароль и нажать кнопку OK.

Чтобы *демонтировать том PGPdisk в Windows Explorer* необходимо:

1. Найти зашифрованный файл тома, который Вы хотите демонтировать, в окне Windows Explorer.
2. Щелкнуть правой кнопкой мыши на имени зашифрованного файла тома.
3. Выбрать PGP—>Unmount PGPdisk.

СОЗДАНИЕ НОВОГО ТОМА PGPdisk

Чтобы создать новый том PGPdisk:

1. Выполните команду Пуск-> Программы-> PGP-> PGPdisk.

2. Мастер PGPdisk появляется на вашем экране. Прочтите вводную информацию.

3. Нажмите на кнопку Next. В появившемся диалоговом окне укажите местоположение и размер из нового тома.

4. Нажмите кнопку Browse, чтобы указать папку для хранения вашего тома PGPdisk или примите заданное по умолчанию местоположение.

-Windows NT: C:\WINNT\Profiles\{Name of Current User}\Personal

-Windows 2000: C:\Documents and Settings\{Name of Current User}\My Documents

- Windows XP: C:\Documents and Settings\{Name of Current User}\My Documents

5. Укажите объем, который Вы хотите зарезервировать для нового тома (PGPdisk Size field). Для ввода используйте только целые числа. Количество свободного дискового пространства для выбранного диска показывают поля Size.

6. Указать единицы измерения объема нового тома PGPdisk: Кбайт, Мбайт или Гбайт. Вы можете создать том любого размера большего чем 100 кбайт. Максимально допустимый размер для тома PGPdisk зависит от вашей версии Windows и размера вашего жесткого диска.

7. Нажмите кнопку Advanced Options, чтобы определить, где и как Вы хотите установить ваш PGPdisk.
Появится диалоговое окно Options.

8. Выберете желательные варианты:

а) On a drive letter. Выберите имя диска, где Вы хотите смонтировать ваш новый том PGPdisk.

б) As a directory on an NTFS volume. Эта опция доступна только для систем Windows 2000/XP. Выберете эту опцию, если Вы хотите установить ваш новый том PGPdisk как каталог в разделе файловой системы NTFS.

в) Choose an encryption algorithm. Выберите алгоритм кодирования, который Вы хотите использовать, чтобы защитить ваши данные:

- **CAST5 Cipher Algorithm (128-bit). Это алгоритм кодирования военного класса, который имеет гарантированную способность противостоять несанкционированному доступу.**
- **Twofish Cipher Algorithm (256-bit). Это один из пяти алгоритмов, который Национальный Институт Стандартов и Технологии (NIST) США предложил для стандарта кодирования AES.**

г) Choose a filesystem format. Определите формат файловой системы для нового тома PGPdisk:

д) Mount at startup. Выберете эту опцию, чтобы монтировать том PGPdisk при запуске системы. При этом необходимо указывать пароль каждый раз при запуске.

9. Закройте диалоговое окно, нажав кнопку OK.

10. Нажмите кнопку Next.

11. Выберете метод защиты для вашего нового тома PGPdisk:

а) Public key. Защита тома PGPdisk открытым ключом.

б) Passphrase. Защита тома при помощи пароля.

12. Нажмите кнопку Next. Полоса прогресса указывает, какой объем тома PGPdisk был инициализирован и отформатирован.

13. Нажатие на кнопку Next монтирует ваш PGPdisk.

14. Нажмите кнопку Finish, чтобы начать работать с вашим новым томом PGPdisk. Ваш том PGPdisk появляется в окне Windows Explorer.

МОНТИРОВАНИЕ ТОМА PGPdisk

Когда Вы создаете новый том, программа PGPdisk автоматически монтирует его и Вы может начать использовать его, чтобы хранить ваши файлы. Когда Вы готовы засекретить содержание тома, Вы должны демонтировать его. Как только том демонтирован, его содержание становится защищенным в зашифрованном файле и содержимое тома остается недоступным пока Вы еще раз не смонтируете его.

Есть несколько способов монтирования тома PGPdisk:

- **Найдите файл тома PGPdisk в Windows Explorer. Щелкните правой кнопкой мыши по нему и выберите PGP—>Mount PGPdisk.**
- **В PGPtray, выберите PGPdisk—>Mount Disk.**
- **В Редакторе PGPdisk, нажмите кнопку Mount или выберите Mount в меню File.**

Смонтированный том PGPdisk появляется как диск в окне Windows Eplorer.

ИСПОЛЬЗОВАНИЕ СМОНТИРОВАННОГО ТОМА PGPdisk

Вы можете создать, копировать, перемещать, и удалять файлы и папки на томе PGPdisk также, как Вы обычно делаете в любом другом разделе. Однако при этом, кто-либо еще также имеет доступ к данным, сохраненным в томе. Только когда Вы демонтируете том данные станут недоступными.

***Предостережение*: Зашифрованный файл, связанный с каждым томом может быть удален средствами операционной системы. Поэтому, необходимо сохранить резервную копию зашифрованного файла в недоступном месте.**

ДЕМОНТИРОВАНИЕ ТОМА PGPdisk

Если Вы хотите блокировать содержимое тома, Вы должны демонтировать его.

Есть несколько способов демонтировать том:

- **В Windows Explorer щелкните правой кнопкой мыши на PGPdisk файле, и выберите PGP—> Unmount PGPdisk.**
- **В Редакторе PGPdisk, щелкните кнопкой Unmount или выберите Unmount в меню File.**
- **В PGPtray, выберите PGPdisk—>Unmount All Disks.**
- **Нажмите клавиши Ctrl-Shift-U чтобы демонтировать все тома PGPdisks.**

Предостережение: Вы можете потерять данные, если Вы демонтируете том PGPdisk, который содержит открытые файлы. Если Вы выберете опции Allow forcible unmounting of PGPdisks with open files и Don't ask before forcibly unmounting a PGPdisk в окне PGP Options, то Вы не будете получать предупреждение перед демонтированием тома, который содержит открытые файлы.

Практическая часть

1) **Выполните настройку PGPdisk.**
2) **Зашифруйте любые данные.**

Результат: Выполнив работу, вы получите навыки шифрования данных с использованием программного продукта PGPdisk.