*А.В. Человечкова, Е.Н. Полякова, Ю.В. Адаменко, Т.Р. Змызгова*

*Курганский государственный университет, г. Курган*
**УДК 004.056.55**

# СРЕДСТВА ШИФРОВАНИЯ В ОС GNU/LINUX

**Аннотация.** В данной статье рассматриваются различные средства шифрования данных, доступные в операционной системе GNU/Linux, проводится сравнение и анализ работы представленных средств шифрования. Отражается актуальность представленной операционной системы.

**Ключевые слова:** шифрование, данные, разделы, GNU/Linux, безопасность информации.

GNU/Linux — операционная система, обладающая внушительным количеством встроенных средств обеспечения безопасности и архитектурой, позволяющей обеспечить распределение доступа пользователей к файлам. Изначально она была разработана как серверная, и на соответствующем сегменте рынка она занимает лидирующие позиции. Кроме того, уже долгое время ходят слухи о том, что государство собирается переводить бюджетные учреждения на дистрибутивы этой системы, что делает информацию о её защите ещё более актуальной.

Как было отмечено выше, GNU/Linux обладает средствами, которые позволяют ограничить доступ несанкционированных пользователей к каким-либо файлам, командам или устройствам. Тем не менее, в случае загрузки ПК с другой системы через внешний носитель или мультибут, либо в случае изъятия жёсткого диска, данные можно скопировать, игнорируя внутрисистемные политики безопасности. Во избежание утечек подобного рода используется шифрование файлов или целых разделов.

GNU/Linux предоставляет широкий арсенал средств шифрования, в данной статье будут рассмотрены четыре из них:

- VeraCrypt
- KGpg
- EncFS
- zuluCrypt

Каждое из представленных средств является бесплатным и свободно распространяемым ПО с открытым исходным кодом. Рассмотрим каждое из них.

**VeraCrypt**

VeraCrypt — форк TrueCrypt, созданный в 2013 году Моурниром Идрасси, основателем IDRIX, и поддерживаемый им же по сей день. Этот продукт содержится в репозиториях большинства дистрибутивов GNU/Linux и может быть установлен через консоль или графический пакетный менеджер.

VeraCrypt предоставляет возможности моментального шифрования с применением алгоритмов AES, Serpent, Twofish, Camellia, Кузнечик, а также их комбинаций, криптографические хэш-функции RIPEMD-160, SHA-256, SHA-512, Стрибог и Whirlpool. Поддерживает каскадное шифрование, позволяя создавать скрытые разделы внутри зашифрованных.

Для генерации ключа шифрования системного раздела VeraCrypt использует 327661 итерацию, для шифрования отдельных файлов или разделов диска используется 655331 итерацию для хэш-функции RIPEMD-160 и 500000 итераций для SHA-2 и Whirlpool. Это, конечно, замедляет работу программы, но при этом делает зашифрованные ей файлы крайне устойчивыми к атаке прямым перебором.

Для улучшения производительности в VeraCrypt реализована поддержка параллельной работы на многоядерных и многопроцессорных

системах и использование аппаратного ускорения шифрования, доступного на процессорах, реализующих набор инструкций AES-NI.

Программа имеет графический интерфейс пользователя и создаёт в панели задач значок для удобного управления подключёнными разделами. Также она удобна в настройке и имеет иллюстрированную документацию для новичков, FAQ и официальный форум поддержки. Есть мастер для выполнения большинства стандартных задач (рис.1).

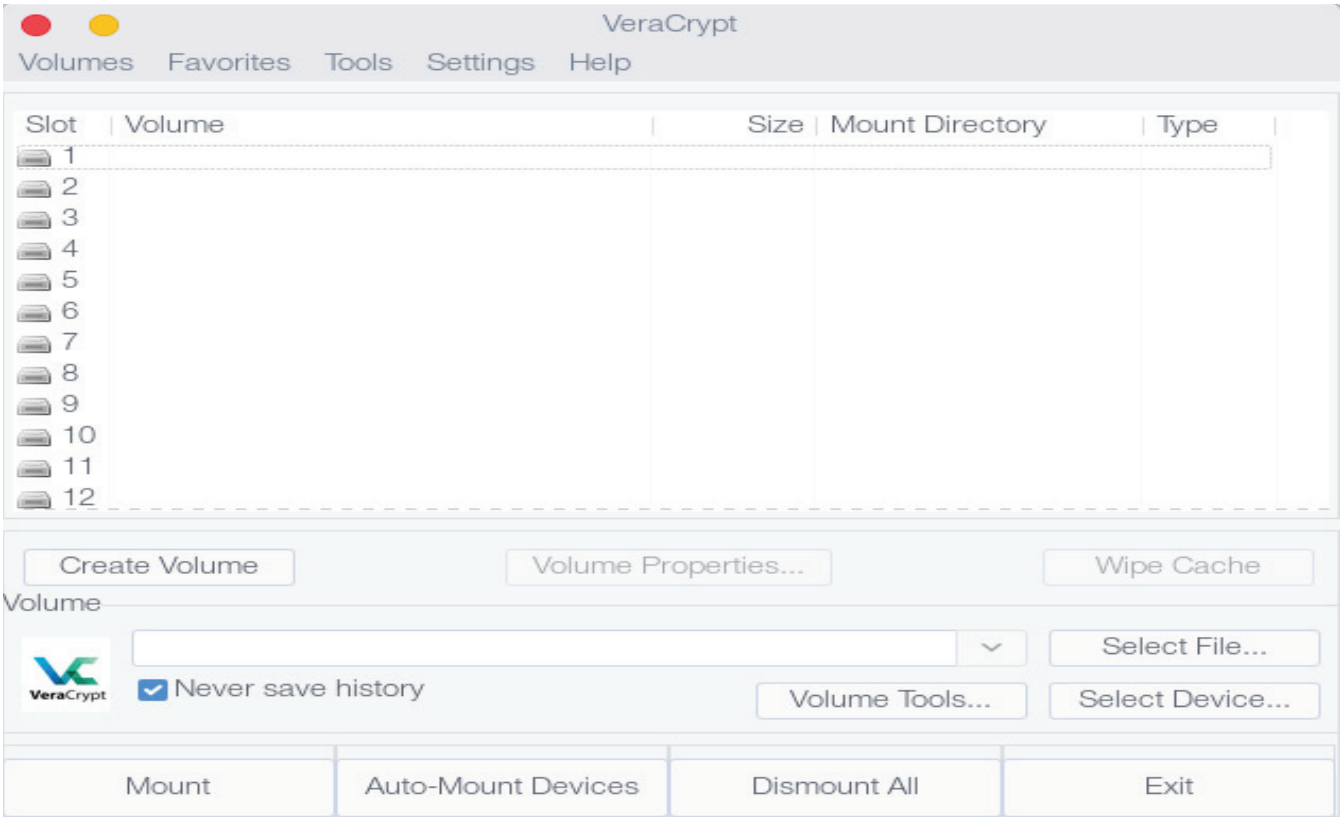


*Рис. 1.* Графический интерфейс VeraCrypt

**KGpg**

KGpg — графический фронтэнд для GnuPG, разрабатываемый Сообществом для графического окружения KDE Plasma. Программа реализует большую часть функционала GPG и поддерживает алгоритмы шифрования AES, CAST5, 3DES, Twofish, Blowfish, Camellia, а также

IDEA с помощью плагина, алгоритмы электронной подписи ElGamal, DSA, RSA и хеш-функции MD5, SHA-1, SHA-2, RIPEMD-160 и TIGER.

KGpg предоставляет возможность создания электронной подписи и шифрования файлов при её помощи. Также в программе реализована функция параллельного шифрования, но её использование возможно только для текста, написанного во внутреннем редакторе.

KGpg имеет графический интерфейс, а также интегрируется в контекстные меню файлового менеджера Dolphin, используемого по умолчанию в KDE Plasma (рис. 2).

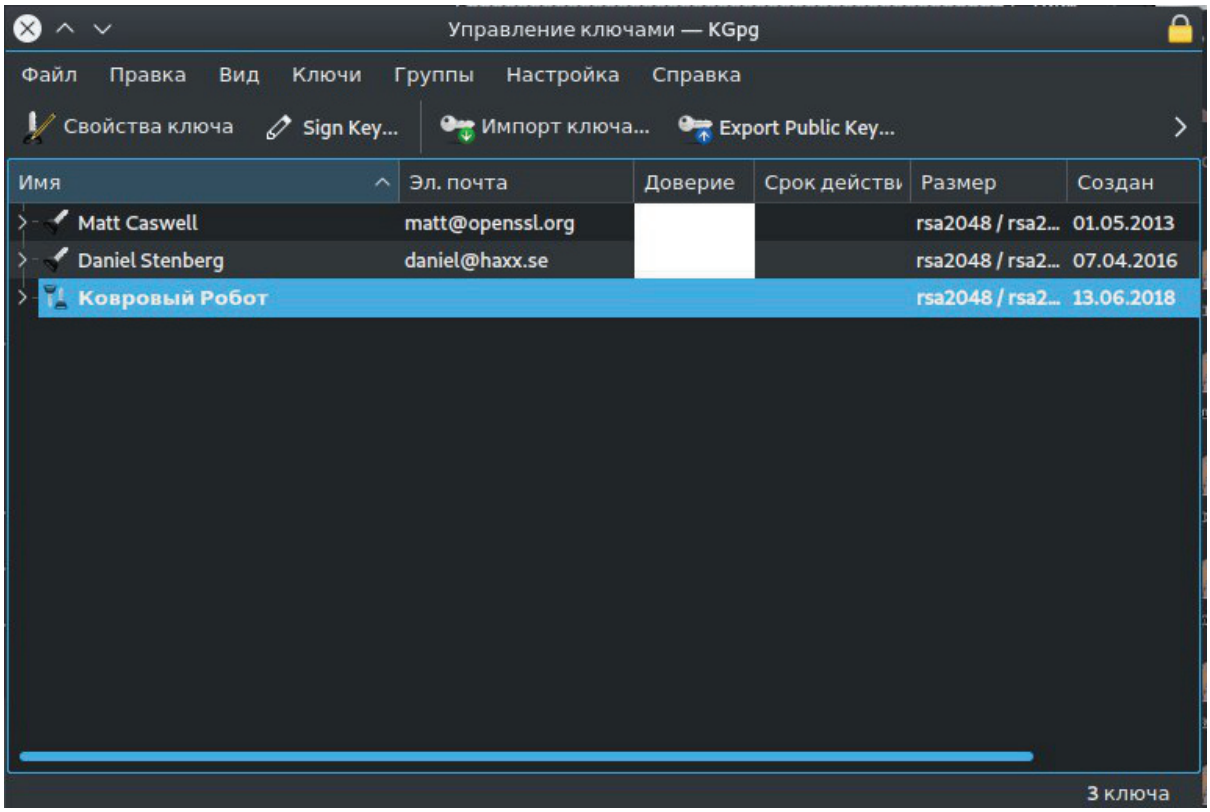


*Рис. 2.* Графический интерфейс KGpg

**EncFS**

EncFS — основанная на FUSE файловая система, использующая произвольную директорию для хранения зашифрованных файлов. Разрабатывается с 2003 года Валентом Гофом. Может быть установлена из репозиториев почти любых дистрибутивов.

Эта программа использует любые алгоритмы шифрования, имеющиеся в системе, чаще всего — Blowfish и AES. Позволяет выбирать размер блока шифрования, кодировать имена файлов, присваивать каждому файлу уникальный инициирующий вектор, улучшая криптостойкость, хранить контрольную сумму для отслеживания изменений и повреждений файлов. Разделы EncFS не занимают фиксированное место на диске и могут сжиматься и расширяться в зависимости от объёма находящихся на них данных. Некоторые директории в директории-точке монтирования могут физически находиться на различных устройствах. Средства резервного копирования обновляют не разделы целиком, а отдельные файлы, которые были изменены.

Тем не менее, у EncFS есть ряд недостатков. Например, тома EncFS не могут быть отформатированы под какую-либо файловую систему кроме системы директории-источника. Фрагментация зашифрованного тома вызывает фрагментацию файловой системы, содержащей директорию-источник. Каждый пользователь, имеющий доступ к директории-источнику может видеть количество файлов и их примерный размер. Также EncFS является консольной утилитой и не имеет графического интерфейса. В графическом окружении GNOME есть Gnome EncFS Manager, но функционал этого интерфейса ограничен. Информацию и руководства можно найти на man страницах пакета, а также на различных форумах в интернете (рис. 3).

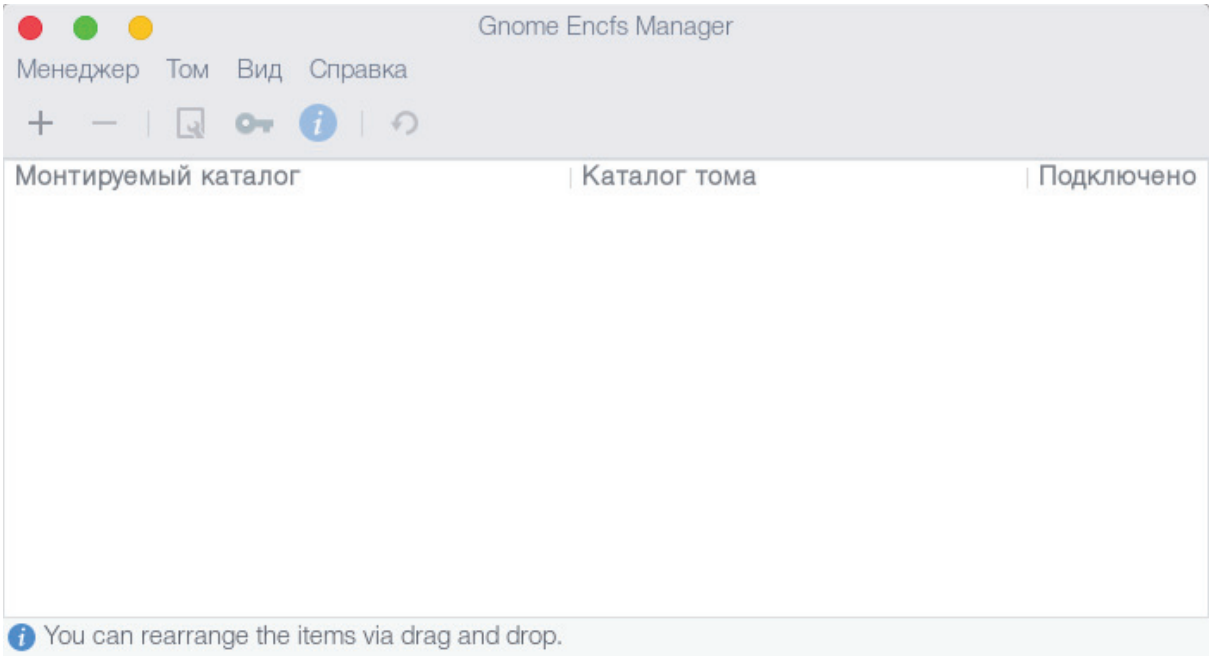


*Рис. 3.* Графический интерфейс Gnome EncFS Manager

**ZuluCrypt**

Интерфейс утилиты cryptsetup, разрабатываемый Френсисом Баниквой. По умолчанию ZuluCrypt создаёт тома LUKS (Linux Unified Key Setup), специально созданная для Linux спецификация шифрования диска. Помимо этого может создавать разделы TrueCrypt, VeraCrypt и Plain. Программа может использовать любой встроенный в ядро алгоритм шифрования. Также, как и VeraCrypt, ZuluCrypt может создавать вложенные шифрованные разделы и шифровать USB-носители. Есть удобный пользовательский интерфейс и возможность интеграции со связкой ключей GNOME или KDE. Поддержку при работе данного продукта можно получить при помощи справки внутри программы, а также на GitHub разработчика, который регулярно отвечает на вопросы пользователей (рис.4).

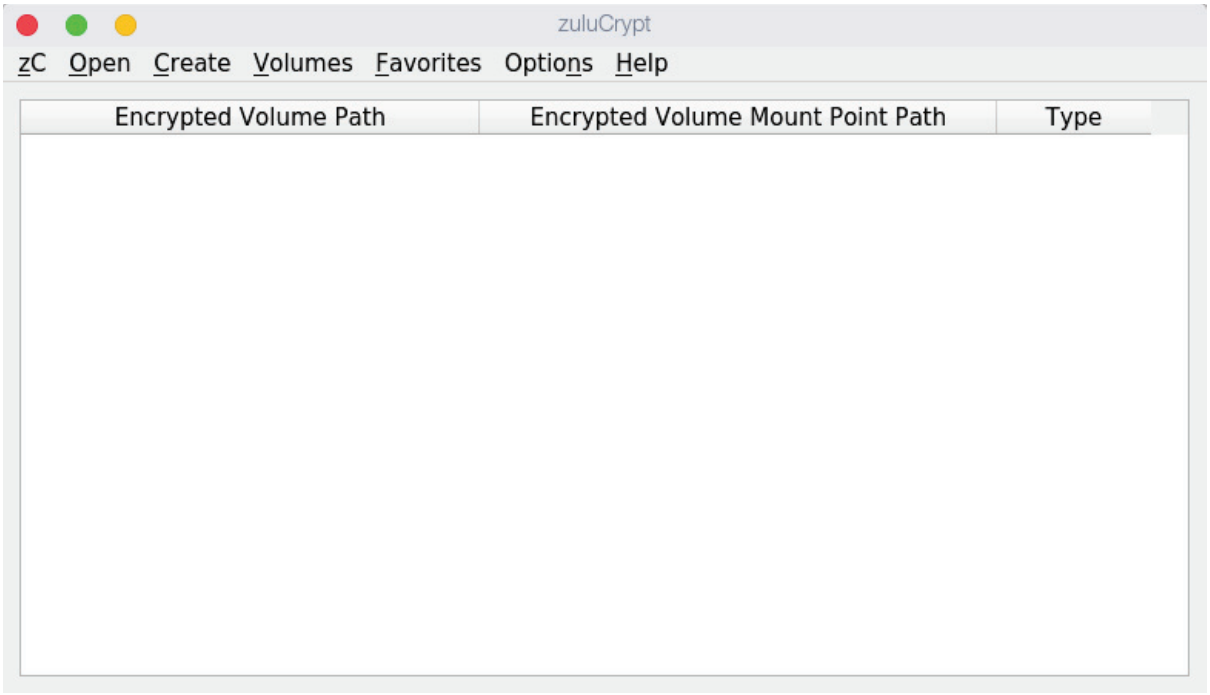


*Рис. 4.* Графический интерфейс ZuluCrypt

Таким образом, по совокупности критериев удобства использования, функциональности и наличия документации, лучшим продуктом из рассмотренных можно назвать VeraCrypt. Данная программа предоставляет возможность шифрования файлов и устройств при помощи различных алгоритмов, шифрования внешних носителей, создания шифрованных разделов, работы с разделами различных форматов и т.д. При этом у VeraCrypt есть удобная документация с гайдами для различных операций. Тем не менее, другие продукты также небесполезны, например, ZuluCrypt лучше справляется с очисткой файлов, а EncFS более удобен в условиях отсутствия графического интерфейса.

## СПИСОК ЛИТЕРАТУРЫ

1. VeraCrypt. [Электронный ресурс] Режим доступа: https://en.wikipedia.org/wiki/VeraCrypt, свободный.

2. GNU Privacy Guard. [Электронный ресурс] Режим доступа: https://en.wikipedia.org/wiki/GNU_Privacy_Guard, свободный.
3. zuluCrypt. [Электронный ресурс] Режим доступа: http://mhogomchungu.github.io/zuluCrypt/, свободный.