ИНТЕГРИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ ДЛЯ UNIX

В.П. КАРАЛКИН, В.П. БУРЦЕВА

Целью данной работы является проектирование и реализация концепции комплексной интегрированной системы безопасности для операционных систем семейства *nix.

В работе реализован и разработан мощный интерфейс для управления подключаемыми модулями, а также демонстрационные примеры плагинов. Сформирован паттерн, с помощью которого любой сторонний программист, не вникая в суть работы системы безопасности, а обладая лишь знаниями языка C, может разработать плагин, выполняющий любые требуемые функции.

Для этого в работе были исследованы open-source программные продукты: TrueCrypt 7.0a, Image Encryption, Rtcrypt-0.6, на основании сравнительного анализа которых выявлены их преимущества и недостатки. Вышеперечисленные программные средства выполняют свойственные им задачи, но ни одно из них не претендует на полностью комбинированную программу в сфере информационной безопасности. Так как разрабатываемый программный продукт работает под управлением ОС Linux, используются различные стандартные и некоторые внешние утилиты для предварительного сжатия данных. Последние могут быть сжаты, затем зашифрованы одним из алгоритмов и только потом записаны в контейнеры одного из типов.

Разрабатываемая система является интегрированной, так как при некотором расширении функционала её можно тесно интегрировать с *nix-

системами, например, частично на уровне ядра. Существенное преимущество такой системы безопасности — возможность ощутимого расширения её функциональности за счёт плагинов. Например, создание модернизированной версии ядра Linux, в которую включены некоторые возможности и модули системы безопасности. Ядро Linux обладает мощным защитным функционалом и библиотеками, которые можно использовать совместно с подсистемой защиты.