Аннотация

Тема: Исследование реализации виртуальных криптографических сетевых интерфейсов в ядре ОС Linux.

Цель работы: Целью работы является исследование механизмов ядра семейства операционной системы `Linux` с целью последующей реализации виртуальных сетевых интерфейсов на базе криптографических протоколов, описанных в государственных стандартах (ГОСТ).

Поставленные задачи:

- исследование методов реализации виртуальных сетевых интерфейсов в ядре Linux;
- анализ криптографической подсистемы ядра «`Crypto API`» на возможность встраивания криптографических протоколов, описанных в ГОСТ;
- изучение существующих виртуальных сетевых интерфейсов;
- выбор оптимального набора криптографических протоколов;
- разработка и тестирование прототипа виртуального криптоинтерфейса.

Полученные результаты: В ходе выполнения работы было принято решение об использовании `WireGuard` в качестве основы для встраивания криптографических протоколов, описанных в ГОСТ. Был успешно разработан набор базовых криптографических примитивов в виде загружаемых модулей ядра (`LKM`) с использованием `Crypto API`. На базе архитектуры `WireGuard` разработан модуль `WireGost`, использующий отечественные криптографические алгоритмы.

Тестирование показало, что `WireGost` способен работать на скоростях вплоть до **900 Мбит/с**. Это подтверждает преимущество реализации в ядре перед решениями в пространстве пользователя, тем не менее уступает оригинальному `WireGuard`. Наиболее медленной частью системы стал блочный шифр «Кузнечик», который, по сравнению с «`ChaCha20`», используемым в оригинальном протоколе, является гораздо более дорогим с точки зрения вычислительной сложности.

Предложенные рекомендации: Для повышения производительности разработанного решения и приближения его показателей к скорости физического канала рекомендуется пересмотреть методы реализации блочного шифра «Кузнечик» в виде загружаемых модулей ядра, а также обеспечить более эффективную поддержку базовых математических операций используемых в ГОСТ.