https://lms.hse.ru/?apview&h_id=FE746748-1965-4346-81E6-52925EA9B121

ФИО:	Чудников Александр Александрович
Руководитель:	Нестеренко Алексей, профессор, доцент
Факультет:	Московский институт электроники и математики им. А.Н. Тихонова
Кафедра/Группа:	СКБ201
Уровень обучения:	Специалитет
Образовательная программа:	Компьютерная безопасность
Адрес электронной почты:	sasha.chudnikov@mail.ru
Контактный телефон:	+7(909)953-57-67
Название (тема) по-русски:	Исследование реализации виртуальных криптографических сетевых интерфейсов в ядре OS Linux
Название (тема) по-английски:	Research on the Implementation of Virtual Cryptographic Network Interfaces in the Linux Kernel
Язык работы:	Русский
Процент заимствования:	0
Дата загрузки работы:	08-01-2026 20:42:57

Аннотация:
Тема: Исследование реализации виртуальных криптографических сетевых интерфейсов в ядре ОС Linux.
Цель работы: Целью работы является исследование механизмов ядра семей ства операционной системы Linux с целью последующей реализации вир туальных сетевых интерфейсов на базе криптографических протоколов, опи санных в государственных стандартах (ГОСТ).
Поставленные задачи:
• исследование методов реализации виртуальных сетевых интерфейсов в ядре Linux;
• анализ криптографической подсистемы ядра «Crypto API» на возмож ность 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 криптогра фических 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 разра ботан 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 ре шениями в пространстве пользователя, тем не менее уступает оригинальному

WireGuard. Наиболее медленной частью системы стал блочный шифр «Куз нечик», который, по сравнению с «ChaCha20», используемым в оригинальном протоколе, является гораздо более дорогим с точки зрения вычислительной сложности.
Предложенные рекомендации: Для повышения производительности разра ботанного решения и приближения его показателей к скорости физическо го канала рекомендуется пересмотреть методы реализации блочного шиф ра «Кузнечик» в виде загружаемых модулей ядра, а также обеспечить более эффективную поддержку базовых математических операций используемых в ГОСТ.

Аннотация (англ.):
Topic: Research on the implementation of virtual cryptographic network interfaces in the Linux OS kernel.
Purpose: The purpose of the work is to study the mechanisms of the Linux operat ing system family kernel with the aim of the subsequent implementation of virtual network interfaces based on cryptographic protocols described in state standards (GOST).
Tasks:
• research of methods for implementing virtual network interfaces in the Linux kernel;
• analysis of the kernel cryptographic subsystem “Crypto API” regarding the possibility of embedding cryptographic protocols described in GOST;
• study of existing virtual network interfaces;
• selection of an optimal set of cryptographic protocols;
• development and testing of a virtual cryptointerface prototype.
Results: While carrying out the research the author decided to use WireGuard as a basis for embedding cryptographic protocols described in GOST. A set of basic cryptographic primitives was successfully developed in the form of Loadable Kernel Modules (LKM) using the Crypto API. Based on the WireGuard architecture, the WireGost module was developed using domestic cryptographic algorithms.
Testing showed that WireGost is capable of operating at speeds up to 900 Mbps. This confirms the advantage of inkernel implementation over userspace solutions; nevertheless, it yields to the original WireGuard. The slowest part of the system proved to be the “Kuznyechik” block cipher, which, compared to “ChaCha20” used in the original protocol, is much more expensive in terms of computational com plexity.
Recommendations: To improve the performance of the developed solution and bring its metrics closer to the physical link speed, it is recommended to revise the implementation methods of the “Kuznyechik” block cipher in the form of loadable kernel modules, as well as to ensure more efficient support for basic mathematical operations used in GOST.

Я подтверждаю, что выпускная квалификационная работа выполнена мною лично и:

1. не воспроизводит мою собственную работу, выполненную ранее, без ссылки на нее в качестве источника;
2. не воспроизводит работу, выполненную другими авторами, без указания ссылки на источник учебной или научной литературы, статьи, вебсайты, выполненные задания или конспекты других студентов;
3. не предоставлялась ранее на соискание ступени более высокого уровня;
4. содержит правильно использованные цитаты и ссылки;
5. включает полный библиографический список ссылок и источников, которые были использованы при написании работы.

Мне известно, что нарушение правил цитирования и указания ссылок рассматривается как обман или попытка ввести в заблуждение, а также квалифицируется как нарушение Правил внутреннего распорядка НИУ ВШЭ.

Я ~~разрешаю~~ / отказываюсь по причине (нужное оставить)

(указать причину отказа в публикации)

НИУ ВШЭ безвозмездно воспроизводить и размещать (доводить до всеобщего сведения) в полном объеме написанную мною в рамках выполнения образовательной программы выпускную квалификационную работу (бакалавра/дипломную работу/магистерскую диссертацию) с указанием моего авторства и даты выполнения работы, а также данных о научном руководителе моей работы, в сети Интернет на корпоративном портале (сайте) НИУ ВШЭ, расположенном по адресу www.hse.ru, таким образом, чтобы любой пользователь данного портала мог получить доступ к полному тексту выпускной квалификационной работы из любого места и в любое время по собственному выбору.

Дата: 12-01-2026

Подпись: