# ОТЗЫВ

на автореферат диссертации Метлинова Александра Дмитриевича на тему «Модели и алгоритмы повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*», представленной на соискание ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

**Целью диссертации** является решение научно-технической задачи разработки новых моделей и алгоритмов повышения криптостойкости и производительности защищенного канала связи в телекоммуникационных сетях *TCP/IP*. Данные разработки направлены на повышение эффективности обеспечения информационной безопасности в каналах связи систем и сетей телекоммуникаций предприятий.

Это, безусловно, задача актуальная, которая, кроме теоретического, имеет явную практическую направленность в вопросах обеспечения информационной безопасности современных предприятий и организаций. Следует отметить, что по мере развития и усложнения моделей, алгоритмов и средств обработки и передачи информации в защищенных каналах связи телекоммуникационных сетей *TCP/IP* повышается уязвимость существующих протоколов безопасности канала связи, напрямую влияющая на возможность несанкционированного копирования, уничтожения, блокирования или искажения информации. Каналы связи сетей *TCP/IP* не имеют встроенных средств защиты, существующие механизмы обеспечения информационной безопасности реализованы на сеансовом уровне сетевой модели *OSI* и имеют множество уязвимостей. Исследования, направленные на разработку новых моделей и алгоритмов повышения криптостойкости и производительности защищенного канала связи на базе симметричной рюкзачной криптографической системы в сетях *TCP/IP*, актуальны и имеют практическое значение в решении проблемы обеспечения информационной безопасности сетей телекоммуникаций предприятий.

**Достоинством диссертационной работы** является ее практическая значимость. На основе предложенных моделей и алгоритмов было разработано информационное и программное обеспечение комплекса алгоритмов симметричной рюкзачной

криптосистемы с общей памятью, включающее: программный комплекс *CBC*-блочной симметричной рюкзачной криптологической системы, программный тестовый комплекс для симметричной рюкзачной криптосистемы и программный модуль генератора общей памяти для симметричной рюкзачной криптосистемы. Результаты опытной эксплуатации программного комплекса на ряде предприятий Владимира и Владимирской области показали, что разработки автора позволяют безопасно хранить данные предприятия, составляющие коммерческую тайну, а также безопасно их передавать между подразделениями, снизить материальные затраты на активные средства по защите.

**Среди основных результатов исследования**, имеющих научную новизну, хотелось бы отметить предложенную автором математическую модель рюкзачной системы защиты канала связи, позволяющую повысить криптостойкость и производительность этого канала; алгоритмы передачи и приема сообщений в защищенном канале связи в телекоммуникационных сетях *TCP/IP* и модификации протокола *TLS*.

**Замечание:** из содержания автореферата не очевидно, почему для сравнения по криптостойкости и производительности из всего шифронабора протокола *TLS* был выбран алгоритм *AES*.

Несмотря на замечание, диссертация, судя по автореферату, представляет собой самостоятельно выполненное, законченное исследование по решению актуальной научной задачи, соответствует требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.12.13 - Системы, сети и устройства телекоммуникаций, а ее автор Метлинов А.Д. заслуживает присуждения ученой степени кандидата технических наук.

Отзыв составил: **Панов Евгений Юрьевич,** доктор физико-математических наук, профессор, главный научный сотрудник ФГБОУ ВО «Новгородский государственный университет имени Ярослава Мудрого»

173003 г. Великий Новгород, ул. Б.Санкт-Петербургская, 41

телефон +79116410377, e-mail: Eugeny.Panov@novsu.ru

07.05.2018 г. Е.Ю. Панов

Подпись д.ф.-м.н., проф. Панова Е.Ю. заверяю:

Ведущий специалист