

Телефон: (812) 718-6191, факс: (812) 718-6130**E-mail: info@eureca.ru www.eureca.ru****ОКПО 44332499, ОГРН 1027809212595,****ИНН/КПП 7827008143/ 784001001**от 11.05.2016 № 2228/270
на № _____ от _____**ОТЗЫВ****на автореферат диссертационной работы
Ковцура Максима Михайловича
по теме «Методы повышения информационной безопасности IP-
телефонии с учетом вероятностно-временных характеристик
протоколов распределения ключей», представленной на соискание
ученой степени кандидата технических наук по специальности 05.13.19 -
«Методы и системы защиты информации,
информационная безопасность»**

Защищенная IP-телефония позволяет пользователям, общающимся через открытые каналы связи общего доступа, сохранить конфиденциальность и целостность передаваемой информации, обеспечивая защиту от нарушителей. В связи с ростом числа кибератак на сети провайдеров и операторов услуг, а также на абонентское оборудование, тема исследования является весьма актуальной. Вклад автора позволяет повысить степень защиты информации, передаваемой между корреспондентами, не имеющими предварительно распределенного ключевого материала.

Выносимые на защиту положения обоснованы. Разработанные модель нарушителя для оценки защищенности системы IP-телефонии, методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии, метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, внедрены

в Управлении Роскомнадзора по Северо-Западному федеральному округу, в ООО «Телкон», а также в СПб ГУТ им. М.А. Бонч-Бруевича.

Проведенные соискателем исследования являются новыми с точки зрения применения вероятностных графов для анализа протоколов защищенной IP-телефонии с учетом переменного таймера повторного переспроса сообщений, а также обоснования и применения методов повышения информационной безопасности протоколов распределении ключей IP-телефонии с использованием нескольких каналов связи одновременно.

Из автореферата Ковцура М.М. следует, что соискателю в полной мере удалось раскрыть предлагаемые методы повышения информационной безопасности для проколов защищенной IP-телефонии, методику оценки вероятностно-временных характеристик, а также предлагаемую модель нарушителя.

Однако к автореферату есть несколько замечаний:

- из автореферата не очевидно, почему именно протокол ZRTP был выбран для модернизации вероятностно-временных характеристик;
- не сказано, возможно ли использовать предлагаемую модификацию ZRTP, реализующую метод повышения безопасности, совместно с Multipath RTP (MPRTP).

Выше указанные замечания не влияют на общую положительную оценку диссертационной работы Ковцура М. М. Согласно автореферату, диссертация представляет собой законченное исследование, результаты которого обладают научной новизной.

На основании анализа автореферата можно сделать вывод о том, что диссертационная работа Ковцура Максима Михайловича соответствует всем требованиям, установленным п. 9 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, а ее автор заслуживает присуждения

ученой степени кандидата технических наук по специальности 05.13.19 –
«Методы и системы защиты информации, информационная безопасность».

Заместитель начальника отдела
тематических исследований
ЗАО «ЭВРИКА»,
кандидат технических наук

А.А. Вяхирев

6 мая 2016

ЗАО «ЭВРИКА»,
196084, Санкт-Петербург, Московский пр., 118
тел.: (812) 718-6191, 718-6130
e-mail: info@euresa.ru