Акционерное общество
«Научно-исследовательский институт «Вектор»
(АО «НИИ «Вектор»)

197376, г. Санкт-Петербург, ул. Академика Павлова, дом 14-а.
тел. (812) 295-10-97, тел/факс 596-33-61, факс 591-72-74;
e-mail: nii@nii-vektor.ru www.nii-vektor.ru

ОГРН 1117847020400
ИНН 7813491943
КПП 781301001

УТВЕРЖДАЮ
Генеральный директор
АО «НИИ «Вектор»

О Т З Ы В

Акционерного общества
«Научно-исследовательский институт «Вектор»
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»

Насколько следует из автореферата, диссертационная работа Ковцура Максима Михайловича посвящена оценке вероятностно-временных характеристик протоколов распределения ключей защищенной IP- телефонии, а также повышению безопасности данных протоколов. Актуальность работы обусловлена тем, что протоколы распределения ключей нашли широкое применение в таких продуктах IP-телефонии, как Asterisk, FreeSWITCH, 3CX, Phoner, Jitsi и других, однако вероятностно-временные характеристики данных протоколов, а также их влияние на обеспечение существующих норм, мало изучены.

Научной новизной обладают следующие результаты:

- Метод выявления нарушителя, который в отличие от существующих методов позволяет выявить активного нарушителя протоколов в используемых каналах связи при отсутствии ключевого материала между пользователями.

• Методика оценки вероятностно-временных характеристик протоколов распределения ключей, которая в отличие от существующих методик учитывает наличие ограниченного числа повторных передач сообщений в протоколе с переменной задержкой при повторе.

• Предложенная модификация протокола ZRTP, имеющая сокращенное время успешного завершения по сравнению с исходным протоколом.

Достоверность результатов и полученных выводов подтверждаются:

- применением апробированного математического аппарата;
- выполненной экспериментальной оценкой среднего времени успешного выполнения протокола распределения ключей;
- непротиворечивостью новых результатов с известными положениями в данной предметной области.

Теоретические результаты диссертационной работы внедрены и апробированы в трех организациях (Управлении Роскомнадзора по СЗФО, СПб ГУТ им М.А. Бонч-Бруевича, а также в ООО "Телкон"), что показывает практическую значимость работы.

Основные результаты диссертационного исследование прошли апробацию на научно-технических конференциях и представлены в 16 публикациях, 5 из которых в изданиях, рекомендованных ВАК.

По автореферату можно сделать следующие замечания:

1) Согласно странице 11 автореферата, собранные данные загружались в базу MySQL, однако не приведено аргументаций в пользу выбора именно этой базы данных при проведении дальнейших исследований.
2) При реализации метода повышения информационной безопасности применяется протокол Диффи-Хелмана, однако в автореферате не приведены длины и назначение ключей, вырабатываемых в процессе работы этого протокола и их влияние на результаты исследований.
3) При описании экспериментальной оценки времени успешного завершения протокола ZRTP не сказано, какая скорость была в канале связи, использовавшемся для соединения корреспондентов.

Отмеченные недостатки имеют частный характер и не снижают новизны, практической и теоретической ценности диссертационного исследования.

Диссертационная работа Ковцура Максима Михайловича, исходя из текста автореферата, имеет практическое и научное значение и отвечает предъявляемым к кандидатским диссертациям требованиям, п. 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. N 842, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Главный научный сотрудник