# ОТЗЫВ

на автореферат диссертационной работы КОВЦУРА Максима Михайловича на тему: «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»

В настоящее время связь с использованием IP-телефонии стала вытеснять традиционные сети телефонной связи прежде всего благодаря своей низкой стоимости ведения переговоров и простотой конфигурирования. Обеспечение безопасности IP-телефонии, как сравнительно нового вида связи, является весьма актуальной задачей, имеющей важное теоретическое и практическое значение.

В работе достаточно конкретно сформулирована общая цель исследований, заключающаяся в повышении защищенности информации в сеансах IP-телефонии и сокращении времени установления защищенного соединения. В частности, выбрана и впервые исследована модель атаки нарушителя типа «Man in the Middle» в условиях отсутствия у корреспондентов заранее выработанного ключевого материала.

Математическая модель активного нарушителя основана на четырех выбранных автором алгоритмах нарушителей, реализующих промежуточные цели. Учтен ряд возможных атак нарушителя.

Данная модель позволила автору получить общие выражения для вероятности НСД, выраженные через вероятности переходов через вершины соответствующих вероятностных графов, отражающих алгоритм нарушителя.

Обоснованность и достоверность научных результатов обеспечивается применением апробированного математического аппарата теории вероятности, математической статистики и теории массового обслуживания. Теоретические зависимости подтверждены экспериментальной оценкой, а также результатами имитационного моделирования. Результаты работы апробированы и опубликованы в изданиях, рекомендованных ВАК Минобрнауки России.

Результаты диссертационной работы имеют практическую значимость, о чем свидетельствуют акты внедрения в организациях связи, а также в университетском учебном процессе.

Материал диссертационной работы изложен логично. Выводы и предложения сформулированы в целом обоснованно.

Однако, автореферат не лишен недостатков:

– недостаточно полно описан характер распределения случайного события завершения протокола обмена. Автор ограничился выражениями (21) и (22). В явном

виде не приведена функция распределения, что не позволяет подтвердить корректность аналитических выражений для вероятностно-временных характеристик протоколов распределения ключей;

– качество канала связи характеризуется автором только вероятностью битовой ошибки величиной от $10^{-3}$ до $10^{-5}$ без учета группирования ошибок, которая зачастую встречается при низком качестве канала. Коме этого, имеет смысл провести анализ для более качественных каналов современных цифровых систем передачи с вероятностью ошибок в канале связи $10^{-6}…10^{-8}$ и ниже;

– отсутствует обоснование частных моделей нарушителя для организации атаки типа «Man in the Middle», а зависимость вероятности успешной атаки выражена весьма тривиальной формулой (8);

– из автореферата не ясно, применимы ли результаты исследований для сценария клиент-сервер.

Указанные недостатки связаны с ограниченностью объема автореферата и в целом не носят принципиального характера.

ВЫВОДЫ:

1. По материалам автореферата можно сделать вывод, что диссертационная работа М.М.КОВЦУРА представляет собой законченное актуальное и самостоятельное исследование, обладающее научной новизной и практической ценностью.

2. Выполненная диссертационная работа удовлетворяет требованиям п.9 «Положения о порядке присуждения ученых степеней» и соответствует требованиям ВАК Министерства науки и образования Российской Федерации к кандидатским диссертациям, а ее автор КОВЦУР Максим Михайлович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Начальник управления
научно-технического обеспечения
К.Т.Н., доцент