ЗАКЛЮЧЕНИЕ

экспертной комиссии диссертационного совета Д.002.199.01 по кандидатской диссертации Ковцура Максима Михайловича на тему: «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей», научный руководитель – д.т.н., профессор Молдовян Александр Андреевич

Экспертная комиссия диссертационного совета Д.002.199.01 в составе: д.т.н., проф. Воробьёва В. И.(председатель), д.т.н. Кулешова С.В., д.т.н., проф. Котенко И.В. в соответствии с п. 25 Положения о совете по защите диссертации на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (утв. Приказом Минобрнауки России от 13 января 2014 г. №7) на основании ознакомления с диссертацией **Ковцура Максима Михайловича** и состоявшегося обсуждения приняла следующее заключение:

1. Соискатель ученой степени кандидата технических наук соответствует требованиям пп. 2-4 Положения о порядке присуждения ученых степеней (утв. Постановлением Правительства России от 24.09.2013 г. №842), необходимым для допуска его диссертации к защите.

2. Диссертация на тему “Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей” в полной мере соответствует специальности: 05.13.19 – «Методы и системы защиты информации, информационная безопасность», к защите по которой предоставлена работа и по которой диссертационному совету Д.002.199.01 предоставлено право проведения защит диссертаций.

3. Диссертационная работа Ковцура М.М. посвящена решению актуальной научно-технической задачи повышения уровня защищенности информации в сеансах безопасной IP-телефонии и сокращения времени установления защищенного соединения за счет улучшения вероятностно-временных характеристик протоколов.

Целью исследования является повышение уровня защищенности информации и сокращение времени установления защищенного соединения в сеансах безопасной IP-телефонии. Практическая значимость и недостаточная проработка проблемы в современной литературе определили выбор темы, ее актуальность, цель, задачи, основные направления и содержание диссертационного исследования.

Основные положения, выносимые на защиту:

- Математическая модель активного нарушителя для защищенной IP-телефонии позволяет получить аналитическую зависимость вероятности успешной атаки НСД с учетом вероятности атаки "человек посередине" на протоколы распределения ключей.
- Метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, позволяет повысить безопасность IP-телефонии при отсутствии предраспределенного ключевого материала.
- Методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии позволяет рассчитать вероятность и среднее время успешного выполнения протоколов распределения ключей при работе по каналам связи с различными параметрами.

Теоретическая значимость полученных научных результатов дополняет и развивает теорию информационной безопасности, в части свойств протоколов совместной выработки общего ключа, а также вероятностно-временных характеристик этих протоколов.

Практическая важность результатов заключается в возможности, путем их реализации, повысить уровень ИБ для систем IP-телефонии, автоматически обнаружить вмешательство нарушителя протоколов в канал связи между корреспондентами, снизив вероятность успешной атаки НСД, и сократить время успешного выполнения протокола распределения ключей. Результаты могут быть использованы при разработке методик контроля защищенных сетей электросвязи, а также для оценки эффективности протоколов распределения ключей, в части времени выполнения и вероятности успешного завершения. Кроме того, предложенные модель, методы и методика могут применяться в расчетах при проектировании и разработке решений защищенной IP-телефонии

Обоснованность и достоверность научных положений обеспечены анализом современных исследований и разработок в данной области, корректным использованием апробированного математического аппарата. Теоретически расчеты подтверждаются результатами экспериментов и имитационного моделирования, сверкой результатов с реальным положением дел и апробацией в печатных трудах и докладах на российских и международных научных и научно-практических конференциях.

4. Основные положения и выводы диссертационного исследования в полной мере изложены в 16 научных работах, в том числе в 5 публикациях в периодических журналах, рекомендованных ВАК (журналы «Информационно-управляющие системы», «Фундаментальные исследования», «Электросвязь»).

5. Представленные соискателем сведения об опубликованных им работах, в которых изложены основные научные результаты диссертации, достоверны.

6. В диссертационной работе Ковцура М.М. отсутствуют некорректные заимствования материала из других источников.

7. Результаты диссертационного исследования имеют научную и практическую значимость и вносят вклад в развитие технических наук.

Комиссия предлагает:

1. Принять кандидатскую диссертацию Ковцура М.М. к защите на диссертационном совете Д.002.199.01 как соответствующую профилю диссертационного совета по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.
2. В качестве официальных оппонентов назначить специалистов по данной проблеме: **доктора технических наук, профессора, Липатникова Валерия Алексеевича**, старшего научного сотрудника федерального государственного казенного военного образовательного учреждения высшего профессионального образования "Военной академии связи имени Маршала Советского Союза С.М. Буденного" Министерства обороны Российской Федерации;
   кандидата технических наук, Кирюшкина Сергея Анатольевича, советника генерального директора ООО «Газинформсервис»
3. В качестве ведущей организации утвердить **ПАО «Информационные телекоммуникационные технологии»** (ПАО «Интелтех»), г. Санкт-Петербург.
4. Разрешить Ковцуру М.М. опубликовать автореферат и утвердить список рассылки авторефератов.
5. Защиту диссертации назначить на «__26__» __мая__ 2016 г.

Члены комиссии:

д.т.н., проф

д.т.н., проф

д.т.н. Кул