Закрытое акционерное общество
«Лаборатория противодействия промышленному шпионажу»
(ЗАО «Лаборатория ППШ»)
194295, Россия, Санкт-Петербург, пр. Просвещения, д.35 тел. +7 (812) 309-45-09; факс: +7 (812) 702-73-83
e-mail: lab@pps. http://www.pps.ru

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»

Широкое использование IP-телефонии в современных корпоративных сетях в Российской Федерации не вызывает сомнения. При разработке и эксплуатации защищенных систем IP-телефонии значительное внимание уделяется режимам работы с предварительно распределенным ключевым материалом. Однако недостаточно рассмотрены режимы работы без предварительно распределенного секрета, которые могут использоваться в случае компрометации существующего ключевого материала или в аварийном режиме работы системы. Именно этой области исследований и посвящена диссертационная работа.

Материал, представленный в автореферате Ковцура М.М, показывает, что диссертационная работа направлена на решение **актуальной научно-технической задачи** сокращения времени установления защищенного соединения и повышения уровня защищенности информации в сеансах безопасной IP-телефонии.

Наиболее значимыми **научными результатами**, полученными Ковцуром М.М., являются метод выявления нарушителя, который в отличие от существующих методов позволяет выявить активного нарушителя протоколов в используемых каналах связи при отсутствии ключевого материала между пользователями, а также методика оценки вероятностно-временных харатеристик протоколов распределения ключей.

Практическая значимость работы состоит в разработке модифицированного протокола ZRTP, имеющего, по сравнению с исходным, меньшее время успешного выполнения, а также метода выявления нарушителя, позволяющего сократить вероятность успешной атаки НСД для защищенной IP-телефонии.

Выносимые результаты прошли апробацию на конференциях различного уровня и опубликованы в печатных изданиях из перечня ВАК.

По автореферату стоит отметить следующие **замечания**:

1) Оценка вероятности совпадения маршрутов приведена для пар и троек маршрутов, но не рассмотрена для четверок и пятерок;

2) В автореферате не приведено пояснение, почему экспериментальная оценка среднего времени успешного выполнения производится только для протокола ZRTP и не выполняется для протокола DTLS.

Несмотря на отмеченные замечания, диссертационная работа Ковцура Максима Михайловича представляет собой законченное исследование.

Указанные замечания не снижают ценности и практической значимости диссертационной работы «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей» Ковцура Максима Михайловича, представленной на соискание ученой степени по специальности 05.13.19. Исследование является научно-квалификационной работой, удовлетворяет требованиям, предъявляемым к кандидатским диссертациям, изложенным в п. 9 Положения о присуждении ученых степеней, утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. N 842, а ее автор Ковцур Максим Михайлович заслуживает присуждения ученой степени по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».