АО НИИ Рубин

АКЦИОНЕРНОЕ ОБЩЕСТВО
"НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИ
"РУБИН"

а/я 359, Кантемировская, 5, Санкт-Петербург, 197342, тел. (812)670-89-89, факс (812)596-35-81, e-mail: inforubin@rubin-spb.ru
ИНН/КПП 7802776390/780201001, ОГРН 1127847043720, ОКПО 07542394

Экз № 1

Утверждаю
Генеральный конструктор -
заместитель генерального директора
АО «НИИ «Рубин» по научной работе
доктор технических наук, доцент

ОТЗЫВ

на автореферат диссертации 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»

АКТУАЛЬНОСТЬ ТЕМЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

В связи с бурным развитием средств и методов передачи информации по IP-сетям, вопросы обеспечения безопасности речевой информации, передаваемой с их использованием IP-сетей, в последнее время приобретают особую остроту. Это обусловлено несовершенством существующих и широко используемых на практике как протоколов передачи информации по IP-сетям, так и протоколов распределения ключей, используемых для ее безопасной передачи.

В связи с этим, диссертационная работа Ковцура М.М., целью которой является повышение уровня защищенности информации в сеансах безопасной IP-телефонии и сокращение времени установления безопасного соединения, является актуальной, своевременной и имеющей практическую значимость.

НАУЧНАЯ НОВИЗНА

Судя по материалам автореферата, представленная работа содержит новые результаты, направленные на разрешение существующего

противоречия между возможностями существующих протоколов обеспечения безопасности IP-телефонии и возможностями нарушителя по реализации различных классов атак, в частности, атак типа MITM.

В работе диссертантом получены следующие новые научные результаты:

Математическая модель активного нарушителя для защищенной IP-телефонии, которая отличается от известных учетом атаки типа MITM, что позволяет получить аналитические выражения для вычисления вероятности успешной атаки с целью НСД.

Метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хеллмана, в отличие от существующих позволяет выявить активного нарушителя при отсутствии общего доверенного центра или ключа между корреспондентами, в том числе и нарушителя, использующего технологию синтеза речи.

Методика оценки вероятностно-временных характеристик протоколов распределения ключей в отличие от существующих позволяет учесть ограничения числа повторных передач сообщений при работе по каналам с ошибками и задержками и рассчитать вероятность и среднее время успешного выполнение протоколов распределения ключей.

Таким образом, научные результаты, полученные автором, расширяют существующий научно-методический аппарат в области защиты информации, передаваемой с использованием сетей IP-телефонии и обладают новизной и теоретической ценностью.

ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ

Практическая значимость работы заключается в том, что полученные автором научные результаты могут быть использованы научно-исследовательскими и проектными организациями при совершенствовании существующих и проектировании новых защищенных сетей IP-телефонии, а также при создании средств обнаружение активного нарушителя.

ДОСТОВЕРНОСТЬ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Обоснованность и достоверность научных результатов заключается в применении апробированного научно-методического аппарата вероятностных графов, теории вероятностей, комбинаторики и методов объектно-ориентированного программирования, а также отсутствием противоречий с ранее полученными результатами в данной предметной области.

Судя по материалам автореферата, диссертационная работа хорошо структурирована, полученные результаты методически увязаны друг с другом и обладают научной новизной и практической значимостью. Выводы логически связаны с содержанием работы и позволяют уяснить ее основные положения и научные результаты.

Судя по списку публикаций, представленном в автореферате, полученные в работе научные результаты достаточно полно опубликованы и апробированы на научно-технических конференциях различного уровня.

Тема диссертации соответствует специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Вместе с тем, судя по материалам, представленным в автореферате, диссертационная работа не лишена недостатков, из которых целесообразно представить следующие:

1. Тема диссертации предполагает разработку нескольких методов повышения информационной безопасности IP-телефонии, тогда как в работе реально представлен только один метод выявления нарушителя протоколов распределения ключей.

2. В материалах автореферата не представлены ни вероятностный граф, описывающий работу оцениваемого протокола распределения ключей, ни аналитические выражения для определения его вероятностно-временных характеристик, полученные с использованием производящих функций, что не позволяет судить ни о корректности построения указанного графа, ни о корректности получения аналитических выражений для расчета среднего времени и вероятности успешного завершения протокола.

3. Оценки полученного выигрыша по значениям только среднего времени успешного завершения протокола нельзя считать в достаточной степени корректными, так как не учтенное автором возможное наличие большой дисперсии значений этого времени, что является характерным для вероятностных графов, содержащих петли, может даже в случае малого среднего его значения привести к существенно худшим результатам, чем случай с большим средним временем, но малой дисперсией,.

Однако указанные недостатки в целом не снижают значимости полученных автором результатов диссертационного исследования и не ставят под сомнение их достоверность.

ВЫВОДЫ:

Судя по автореферату, диссертационная работа Ковцура Максима Михайловича является законченной научно-квалификационной работой.

По новизне, научному уровню и практической ценности работа соответствует требованиям Положения присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Отзыв обсужден и одобрен на заседании секции № 1 НТС АО «НИИ «Рубин», протокол № 8 от « 21 » апреля 2016 года.

Главный конструктор комплексной безопасности систем связи-
заместитель главного конструктора
кандидат технических наук, доцент

Ведущий научный сотрудник,
кандидат технических наук, доцент