ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета 26.05.2016 г. № 2

О присуждении Ковцуру Максиму Михайловичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 24 марта 2016, протокол № 2 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, 199178, Россия, Санкт-Петербург, 14 линия В.О., дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года.

Соискатель Ковцур Максим Михайлович, 1985 года рождения, в 2008 г. с отличием окончил Санкт-Петербургский государственный университет телекоммуникаций имени профессора М.А. Бонч-Бруевича по специальности «Многоканальные телекоммуникационные системы» (диплом ВСА 0718383 от 5 июня 2008 года). В 2011 году окончил очную аспирантуру Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича. В период подготовки диссертации Ковцур Максим Михайлович являлся соискателем по направлению 05.13.19 – «Методы и системы защиты информации, информационная безопасность» в Федеральном государственном бюджетном учреждение науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук. Справка о сдаче кандидатских экзаменов № 5/195, выдана

в 2016 г. Федеральным государственным бюджетным учреждением науки Санкт-Петербургским институтом информатики и автоматизации Российской академии наук. В настоящее время Ковцур Максим Михайлович работает техническим директором в Обществе с ограниченной ответственностью "Дилер".

Диссертация выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук.

Научный руководитель – доктор технических наук, профессор МОЛДОВЯН Александр Андреевич, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук, заместитель директора по информационной безопасности СПИИРАН.

Официальные оппоненты:

ЛИПАТНИКОВ Валерий Алексеевич, доктор технических наук, профессор, Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации, старший научный сотрудник;

КИРЮШКИН Сергей Анатольевич, кандидат технических наук, ООО «Газинформсервис», советник генерального директора;

дали положительные отзывы на диссертацию.

Ведущая организация – Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»), г. Санкт-Петербург, в своем положительном заключении, подписанном Будко Павлом Александровичем, доктором технических наук, профессором, главным научным сотрудником, Салюком Дмитрием Владиславовичем, кандидатом технических наук, доцентом, заместителем начальника отдела и утвержденном И.А. Кулешовым, кандидатом военных наук, первым заместителем генерального директора ПАО «Интелтех» по научной работе, указала, что в целом диссертационная работа М.М. Ковцура представляет собой завершенную научно-квалификационную работу, выполненную на актуальную тему и обладающую практической и теоретической значимостью полученных результатов,

научной новизной. Автором сформулирована и решена важная научная задача повышения защищенности информации в сеансах безопасной IP-телефонии и сокращения времени установления защищенного соединения.

Основные выводы и положения, представленные в диссертации, обоснованы и аргументированы. Результаты исследований прошли апробацию на 7 международных и всероссийских конференциях. По теме диссертации опубликовано 16 научных работ, в том числе 5 в журналах, входящих в перечень рецензируемых научных изданий.

Результаты диссертационной работы целесообразно использовать в организациях, занимающихся исследованием и разработкой технических систем защищенной IP-телефонии и решений на базе данных разработок. Результаты рекомендуется использовать для доработки существующих программных клиентов IP-телефонии, применяемых, в том числе, в сценарии корреспондент-корреспондент.

Основные этапы работы, результаты, выводы представлены в автореферате, который достаточно полно отражает содержание диссертации.

Диссертационная работа «Методы повышения информационной безопасности IP-телефонии с учетом вероятностно-временных характеристик протоколов распределения ключей» соответствует паспорту научной специальности и отвечает критериям, предъявляемым к кандидатским диссертациям и установленным Положением о присуждении ученых степеней, утвержденным постановлением Правительства РФ № 842 от 24.09.2013 г., а ее автор - Ковцур Максим Михайлович по уровню профессиональных, общенаучных, специальных знаний заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 22 опубликованных работы, в том числе по теме диссертации 16 работ, опубликованных в рецензируемых научных изданиях – 5 работ, из них опубликованных в изданиях, рекомендуемых ВАК РФ - 5.

Основные научные результаты опубликованы в 16 научных трудах общим объемом 8,55 п.л., из которых 11 статей объемом 5,76 п.л. выполнены в соавторстве, а 5 статей объемом 2,79 п.л. – лично. Наиболее значительные работы по теме диссертации:

1. **Ковцур, М. М.** Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи / М.М. Ковцур, В.Н. Никитин, Д.В. Юркин // Информационно – управляющие системы. – 2014. – №1(68). – С. 70-75. Авторский вклад 33%.

2. **Ковцур, М. М.** Обеспечение информационной безопасности ИТС / М.М. Ковцур, В.Н. Никитин, О.И. Лагутенко // Электросвязь. – 2014. – №1. – С. 29-31. Авторский вклад 33%.

3. **Ковцур, М. М.** Исследование путей совершенствования протоколов распределения ключей в защищенной IP-телефонии / Ковцур М.М. // Фундаментальные исследования. – 2014. – № 8(часть 6). – С. 1300-1308.

4. **Ковцур, М. М.** Исследование вероятностно-временных характеристик протокола распределения ключей защищенной IP-телефонии / М.М. Ковцур, В.Н. Никитин, А.В. Винель // Информационно – управляющие системы. – 2013. – №1(62). – С. 54-63. Авторский вклад 33%.

5. **Ковцур, М. М.** Математическая модель активного нарушителя для защищенной IP-телефонии / М.М. Ковцур, В.Н. Никитин // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно - методическая конференция, Санкт-Петербург, 3-5 марта 2015: сб. научных статей в 2 т. / под. ред. С.В. Бачевского, сост. А.Г. Владыко, Е.А. Аникевич, Л.М. Минаков. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 920 с. – С 330-335. Авторский вклад 50%.

6. **Ковцур, М. М.** Оценка скоростных характеристик реализации атаки типа перебор пароля на IP-АТС при использовании FAIL2BAN / М.М. Ковцур, А.А. Молдовян // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г.: Материалы конференции / СПОИСУ. – СПб, 2015. – 418 с. – С. 171. Авторский вклад 50%.

На автореферат диссертации поступило 7 отзывов, все отзывы положительные:

1) Федеральное государственное унитарное предприятие «ЦентрИнформ». Отзыв составили начальник управления научно-технического обеспечения, к.т.н., доцент П.С. Вихлянцев, Лауреат Государственной премии Российской федерации в области науки и техники, к.т.н., доцент М.В. Симонов. Замечания: 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 и величиной от 10^{-3} до 10^{-5} без учета группирования ошибок, которая зачастую встречается при низком качестве канала. Кроме 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 неясно, применимы ли результаты исследований для сценария клиент-сервер.

2) ЗАО «Лаборатория противодействия промышленному шпионажу» («Лаборатория ППШ»). Отзыв составили президент специализированного холдинга "Лаборатория ППШ", советник ЗАО "Лаборатория ППШ", заместитель генерального директора ООО "Лаборатория ППШ" Остапенко А. Н., заместитель начальника отдела специальных проверок и специальных исследований ЗАО "Лаборатория ППШ", к.т.н. Новаковский С.Н., заместитель начальника отдела компьютерной безопасности ЗАО "Лаборатория ППШ", к.т.н. Кравченко И.Д. Замечания: оценка вероятности совпадения маршрутов приведена для пар и троек маршрутов, но не рассмотрена для четверок и пятерок; в автореферате не приведено пояснение, почему экспериментальная оценка среднего времени успешного выполнения производится только для протокола ZRTP и не выполняется для протокола DTLS.

3) Научно-исследовательский институт «Рубин». Отзыв составили главный конструктор комплексной безопасности систем связи - заместитель главного конструктора, к.т.н., доцент Таран В.В., ведущий научный сотрудник, к.т.н., доцент

Никифоров О.Г. Замечания: 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; 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. 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.

4) ОАО «НИИ «Вектор». Отзыв составили главный научный сотрудник, д.т.н., с.н.с., Емелин В.И., начальник научно-технического отдела, Гончаров В. Б. Замечания: согласно странице 11 автореферата, собранные данные помещались в базу MySQL, однако не приведено аргументаций в пользу выбора именно этой базы данных при проведении дальнейших исследований; 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; при описании экспериментальной оценки времени успешного завершения протокола ZRTP не сказано, какая скорость была в канале связи, использовавшемся для соединения корреспондентов.

5) ЗАО «Ниеншанц-Защита». Отзыв составил начальник производственно-технического отдела, к.т.н., Мурашов С.В. Замечания: из текста автореферата неясно, учитываются ли при расчете среднего времени успешного выполнения размеры сообщений исследуемых протоколов, а также заголовки IP-пакетов; в автореферате не

приведены результаты имитационного моделирования, обозначенные в первом разделе автореферата.

6) ЗАО «ЭВРИКА». Отзыв составил заместитель начальника отдела тематических исследований, к.т.н. Вяхирев А.А. Замечания: из автореферата не очевидно, почему именно протокол ZRTP был выбран для модернизации вероятностно-временных характеристик; не сказано, возможно ли использовать предлагаемую модификацию ZRTP, реализующую метод повышения безопасности, совместно с Multipath RTP (MPRTP).

7) ООО «РТК Новые Технологии». Отзыв составил ведущий специалист, к.т.н. Клюкин А.И. Замечания: использование вероятностных графов предполагает наличие процедур постоянной актуализации значений этих вероятностей, которые, очевидно, изменяются во времени. К сожалению, в автореферате отсутствуют описания подобных процедур; для эксперимента при проверке наличия независимых маршрутов канал связи устанавливается между двумя точками (городами), но в таблице 1 указывается только одна точка. Возможно, второй точкой является Санкт-Петербург, однако в тексте автореферата это не указано; в автореферате следовало бы привести ссылки на нормативные документы, описывающие требования, предъявляемые к каналам связи для предоставления услуг IP-телефонии.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Липатников В.А. является ведущим ученым в области защиты информации и безопасности современных систем и технологий, сетей и программного обеспечения; к.т.н. Кирюшкин С. А. - крупный специалист в области оценки и аудита систем информационной безопасности, а также цифровой подписи; ведущая организация ПАО «Информационные телекоммуникационные технологии» (ПАО «Интелтех») известна как в России, так и за рубежом в области моделирования, разработки, построения защищенных сетей связи специального назначения и оценки характеристик систем связи.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработан новый метод выявления нарушителя для защищенной IP-телефонии, позволяющий, в отличие от существующих, выявить активного нарушителя в используемых каналах связи при отсутствии общего доверенного центра или секрета;

предложены новые научно-обоснованные рекомендации по модернизации протокола ZRTP для сокращения времени работы, что снижает временные затраты протокола при работе по каналам связи с ошибками и задержками; методика оценки вероятностно-временных характеристик протоколов распределения ключей, учитывающая в отличие от существующих наличие ограниченного числа повторных передач сообщений с переменным таймером повторной передачи при работе по каналам с ошибками и задержками;

доказана возможность применения предлагаемого метода повышения безопасности с учетом текущего уровня развития телекоммуникационных сетей в Российской Федерации и в мире;

введены новые оценки защищенности протоколов распределения ключей, использующие вероятностно-временные характеристики алгоритмов легитимного выполнения протоколов IP-телефонии и алгоритмов воздействия нарушителя на анализируемый протокол.

Теоретическая значимость исследования обоснована тем, что:

доказана возможность повышения уровня информационной безопасности в части обеспечения конфиденциальности и целостности протоколов IP-телефонии за счет использования двухканального и трехканального метода выявления нарушителя в условиях современного состояния сетевой инфраструктуры;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов)

использован математический аппарат вероятностных графов и производящих функций вероятностей переходов при построении модели нарушителя и при разработке методики оценки вероятностно-временных характеристик протоколов, а также элементы теории вероятности и комбинаторики при разработке метода выявления нарушителя протоколов;

изложены математическая модель нарушителя и методика повышения информационной безопасности протоколов распределения ключей, развивающая и

дополняющая теорию информационной безопасности в части свойств протоколов распределения ключей;

раскрыты проблемы протоколов обеспечения безопасности IP-телефонии, вызванные неустойчивостью протоколов распределения ключей к атакам активного нарушителя при отсутствии предраспределенного ключевого материала и доверенной третьей стороны;

изучено влияние протоколов обеспечения информационной безопасности на соблюдение норм, предъявляемых к сетям телефонной связи общего пользования, а также на показатели качества защищенной IP-телефонии;

проведена модернизация существующего протокола распределения ключей ZRTP, обеспечивающая повышение уровня информационной безопасности протокола распределения ключей, а также сокращение времени работы при работе по каналам связи с ошибками и задержками.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены (указать степень внедрения) следующие результаты диссертационной работы:

1) Математическая модель активного нарушителя для защищенной IP-телефонии, методы повышения информационной безопасности для протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана, использовались при разработке методики контроля защищенных сетей электросвязи в Управлении Роскомнадзора по Северо-Западному федеральному округу;

2) Математическая модель активного нарушителя для защищенной IP-телефонии; метод выявления нарушителя протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана; методика оценки вероятностно-временных характеристик протоколов распределения ключей IP-телефонии использованы в учебном процессе при чтении лекций и проведении лабораторных работ бакалавров по специальностям 210700.62 “Инфокоммуникационные технологии и системы связи” и 090900.62 “Инфокоммуникационная безопасность”, при чтении лекций и проведении лабораторных работ магистров по специальностям 210700.68 “Инфокоммуникационные технологии и системы связи” 090900.68

“Инфокоммуникационная безопасность” по дисциплине “Безопасность IP-телефонии” в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича;

3) Методика оценки вероятностно-временных характеристик протоколов распределения ключей защищенной IP-телефонии; метод улучшения временных характеристик криптографического протокола ZRTP; метод повышения безопасности протоколов распределения ключей, основанных на алгоритме Диффи-Хелмана; метод автоматического обнаружения вторжений нарушителя в середину канала связи для протокола ZRTP использованы в ООО "Телкон" в отчете о научно-исследовательской работе “Исследование путей совершенствования характеристик протоколов IP-телефонии для внедрения в абонентских голосовых терминалах, предназначенных для работы по беспроводным каналам связи”;

определены перспективы практического использования полученных результатов диссертационной работы при повышении защищенности и стандартизации программных и программно-аппаратных решений по безопасности IP-телефонии;

создана модель нарушителя на основе анализа возможных действий, которые могут быть выполнены нарушителем, исходя из текущего уровня развития технологий защиты и нападения, а также существующих угроз в защищенной IP-телефонии;

представлены предложения по дальнейшему совершенствованию протоколов распределения ключей IP-телефонии с использованием стеганографии.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ показана воспроизводимость результатов экспериментов, выполненных на современном сертифицированном оборудовании;

теория построена на известных принципах, проверенных фактах и данных с применением апробированных методов исследования, согласуется с опубликованными экспериментальными данными по теме диссертационного исследования;

идея базируется на анализе текущего состояния дел в области защищенной IP-телефонии, существующих инструментов атак и защиты от атак, а также анализе текущего развития современных сетей связи;

использованы сравнение достоинств и недостатков предшествующих научных разработок по исследуемой проблематике и преемственность основных научных положений;

установлено, что полученные теоретические и экспериментальные зависимости не противоречат результатам других исследований, представленных в независимых источниках по данной тематике;

корректно **использованы** фундаментальные принципы, концепции и подходы, применяемые в теории вероятности, комбинаторике, теории вероятностных графов;

теоретические зависимости **подтверждены** результатами экспериментальной оценки и результатами имитационного моделирования;

результаты базируются на исследовании большого числа отечественных и зарубежных публикаций и источников литературы по теме диссертации, отраженных в списке литературы.

Личный вклад соискателя состоит в:

анализе актуального состояния дел предмета и объекта исследования;

разработке методики по оценке вероятностно-временных характеристик протоколов и обоснование с ее помощью необходимости модернизации протокола ZRTP;

разработке модели нарушителя и обоснование на основе модели необходимости модернизации протокола распределения ключей с целью повышения устойчивости этого протокола к атаке активного нарушителя;

непосредственном **участии** соискателя **в получении исходных данных** и в научных экспериментах;

разработке экспериментального стенда для оценки среднего времени выполнения ZRTP, обработка полученных экспериментальных данных выполнена лично автором;

автору принадлежит **решающая роль** в подготовке основных публикаций по выполненной работе и **апробации результатов** на всероссийских и международных конференциях.

Диссертационный совет считает, что Ковцур М.М. в своей диссертационной работе решил актуальную научно-техническую задачу повышения уровня защищенности передаваемой информации в сеансах безопасной IP-телефонии и сокращения времени установления защищенного соединения за счет улучшения вероятностно-временных характеристик протоколов, имеющую важное техническое, социально-экономическое и хозяйственное значение.

На заседании 26.05.2016 г. диссертационный совет принял решение присудить Ковцуру М.М. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 21 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 21, против нет, недействительных бюллетеней нет.

Председатель диссертационного совета,
д.т.н., член-корреспондент РАН Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета
к.т.н., доцент Фаткиева Роза Равильевна
26.05.2016 г.