ОТЗЫВ

на автореферат диссертации Трушиной Оксаны Вячеславовны
«Разработка теоретико-информационных методов обеспечения анонимности в телекоммуникационных сетях»,
представленную на соискание ученой степени кандидата физико-математических наук
по специальности 05.13.17 – «Теоретические основы информатики»

Развитие информационных технологий приводит к тому, что задачи защиты информации становятся все более актуальными. По сравнению с задачей обеспечения секретности сообщения, которую можно считать хорошо изученной, задача обеспечения анонимности относительно новая и недостаточно изученная.

Диссертация О. В. Трушиной посвящена новому подходу к обеспечению анонимности – теоретико-информационному подходу. Проведенный анализ существующих работ по этой теме демонстрирует, что основной подход к решению задачи криптографический. На примере автором показано, что для обеспечения анонимности необходимо решить так называемую задачу обеспечения несвязываемости. Под обеспечением несвязываемости сообщений понимается преобразование входящего сообщения таким образом, чтобы нельзя было сопоставить входящее и выходящее сообщения некоторого узла сети.

В диссертации О. В. Трушиной предлагается обеспечивать несвязываемость сообщений с помощью статистической независимости. Такой тип несвязываемости в диссертации получил название совершенной несвязываемости. Если входное и выходное сообщения некоторого узла сети статистически независимы, то они совершенно несвязываемы, и злоумышленник не может установить между ними связи даже при наличии неограниченных вычислительных мощностей. Идея обеспечения несвязывамости посредством статистической независимости оказалась применима к разным типам каналов. В диссертации эта идея реализована для трех видов каналов.

В качестве замечаний можно отметить, что довольно краткое описание принципа сетевого кодирования не дает возможности понять почему разработанный в диссертации метод применим к нему лучше, чем криптографические методы. В диссертации

утверждается, что секретность передаваемых сообщений является необходимым условием для обеспечения несвязываемости. Криптографический подход обеспечивает семантическую секретность, в то время как для предлагаемого теоретико-информационного подхода семантическая секретность рассмотрена только для гауссовского канала и не рассмотрена для других каналов, что приводит к неясности возможна ли семантическая секретность для этих каналов.

Несмотря на отмеченные недостатки, полученные результаты дают основание для положительной оценки диссертации. Диссертация О. В. Трушиной является законченной научно-исследовательской работой, представляющей научный интерес. О. В. Трушина заслуживает присуждения степени кандидата физико-математических наук по специальности 05.13.17 – Теоретические основы информатики.

Витязев Владимир Викторович,
заведующий кафедрой телекоммуникаций
и основ радиотехники Рязанского государственного
радиотехнического университета, д.т.н., профессор

Лихобабин Евгений Александрович,
старший научный сотрудник кафедры телекоммуникаций
и основ радиотехники Рязанского государственного
радиотехнического университета, к.т.н.

390005, г. Рязань, ул. Гагарина, д. 59/1, Федеральное государственное бюджетное образовательное учреждение высшего образования «Рязанский государственный радиотехнический университет» (ФГБОУ ВО «РГРТУ»),
http://rsreu.ru
***Тел.:** (4912) 46-03-03*
***Факс:** (4912) 92-22-15*
***E-mail:** rgrtu@rsreu.ru*

Подпись профессора Витязева В.В. и старшего научного сотрудника Лихобабина Е.А заверяю, Ученый секретарь Совета ФГБОУ ВО «РГРТУ»,
к.т.н., доцент В.Н. Пржегорлинский

11.05.2017