

## ОТЗЫВ

на автореферат диссертации Трушиной Оксаны Вячеславовны  
«Разработка теоретико-информационных методов обеспечения анонимности в  
телекоммуникационных сетях»,

представленной на соискание ученой степени кандидата физико-математических наук по  
специальности 05.13.17 – «Теоретические основы информатики»

Диссертационная работа О. В. Трушиной посвящена актуальной теме исследования анонимной передачи данных в телекоммуникационных сетях. Анонимность представляет собой развивающееся направление защиты информации, и ей посвящено много исследований. Можно выделить разные виды анонимности в зависимости от того, в чем состоит цель злоумышленника. В диссертации О. В. Трушиной злоумышленник, прослушивая сообщения, передающиеся по сети, не должен одновременно определять отправителя и получателя сообщения. Обеспечение анонимности рассматривается в диссертации О. В. Трушиной как составная задача. Первая часть задачи есть задача маршрутизации. Здесь объектом, которому необходимо обеспечить секретность, является маршрутная информация. Вторая часть задачи – передача сообщения по маршруту. Ключевая особенность этой задачи состоит в том, что необходимо передать сообщение так, чтобы, прослушивая это сообщение в разных точках маршрута, злоумышленник не мог установить, является ли это сообщение одним и тем же. В диссертации эта задача называется задачей обеспечения несвязываемости. Рассмотрев пример передачи сообщения и возможные действия злоумышленника, автор показывает, что обеспечение несвязываемости является необходимым условием анонимности. Проведенный автором анализ демонстрирует, что основным инструментом обеспечения несвязываемости является шифрование, и не существует методов обеспечения несвязываемости в теоретико-информационном смысле.

В диссертации предложен простой теоретико-информационный метод обеспечения несвязываемости. Стоит отметить, что метод может быть применен для разных типов передачи данных. В диссертации предложенный метод реализован для

традиционной передачи данных по протоколу Ethernet, для сетевого кодирования и для сетевого кодирования на физическом уровне.

В качестве замечаний можно отметить следующее: приведенное описание стойкости методов слишком краткое и не позволяет понять, в чем состоят влияющие на стойкость особенности методов; кроме того, использование термина «алгебраическая решетка» в рассматриваемом контексте некорректно, надо использовать «целочисленная решетка».

Несмотря на отмеченные недостатки, диссертационная работа О. В. Трушиной является законченной научно-исследовательской работой, результаты которой можно квалифицировать как решение новой научной задачи. Работа соответствует требованиям, предъявляемым ВАК к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.17 – Теоретические основы информатики.

Анисов Сергей Семенович  
к. ф.-м. н., аналитик  
sanisov@iponweb.net



02.05.2017

ООО «АйПиВеб»

Адрес: 115162, г. Москва, ул. Шаболовская, д. 31 стр. 5

Тел.: +7 (499) 653-64-69

E-mail: info@iponweb.net

Подпись Анисова Сергея Семеновича заверяю

Богданова Ольга Михайловна, специалист по кадровому администрированию

