ОТЗЫВ

официального оппонента на диссертационную работу Абрамова Константина Германовича «**Модели угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях**», представленную на соискание ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций

Актуальность работы. Важным направлением в решении проблемы обеспечения безопасности информационно-телекоммуникационных сетей является задача разработки моделей и методов защиты абонентов от запрещенной информации. К числу дестабилизирующих факторов, оказывающих существенное негативное влияние на состояние информационной безопасности объектов информационно-телекоммуникационных сетей, относится лавинообразное распространение запрещенной информации. Условиями, благоприятствующими деструктивному проявлению отмеченного выше фактора, являются: низкий уровень грамотности пользователей в аспекте компьютерной безопасности; недостаточное знание законов, регламентирующих порядок взаимодействия абонентов в информационно-телекоммуникационных сетях; рост активности лиц, использующих методы распространения запрещенной информации для воздействия на элементы информационно-телекоммуникационных сетей; техническая сложность идентификации и противодействия распространению запрещенной информации.

Заблаговременное выявление наиболее значимых узлов сети, своевременное целенаправленная работа по принятию мер, препятствующих распространению запрещенной информации, оперативное прогнозирование угрозы распространения запрещенной информации, - все это позволяет в определенной степени минимизировать последствия от ее проявления.

С учетом изложенного, диссертационная работа Абрамова Константина Германовича, имеющая целью повышение точности прогнозирования угрозы

распространения запрещенной информации в информационно-телекоммуникационных сетях путем разработки, исследования и практической реализации новых моделей и алгоритмов, является достаточно актуальной и априорно имеет существенное практическое значение для обеспечения безопасности элементов информационно-телекоммуникационных сетей.

Содержание работы. Во *введении* обоснована актуальность темы диссертации, определена цель, объект и предмет исследования, а также сформулированы его задачи.

В *первой главе* рассмотрена проблема обеспечения информационной безопасности информационно-телекоммуникационных сетей, проанализированы методы и средства противодействия угрозам, выявлены факторы, влияющие на условия защиты от запрещенной информации, уточнены задачи исследования.

Вторая глава посвящена разработке имитационной и аналитической модели угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях, при этом автором уделено особое внимание учету их топологических особенностей.

В *третьей главе* разработана методика формирования топологии крупномасштабной информационно-телекоммуникационной сети, которая необходима для получения информации о структуре сети в условиях неполноты исходных данных.

Основным содержанием четвертой главы является экспериментальное исследование и рассмотрение особенностей внедрения.

В *заключении* приведены основные выводы и результаты диссертационной работы.

Основные научные результаты. К основным научным результатам могут быть отнесены:

1. Имитационная модель реализации угрозы запрещенной информации в информационно-телекоммуникационных сетях, учитывающая среднюю степень связности узлов, среднюю длину пути сети, коэффициент кластеризации сети, а также особенности информационного взаимодействия абонентов как человеко-машинных систем.

2. Аналитическая модель реализации угрозы запрещенной информации, отличающаяся от классической эпидемиологической модели Кермака-Маккендрика, тем, что в ней учены характеристики уязвимости информационно-телекоммуникационных сетей.

3. Методика формирования топологии крупномасштабных информационно-телекоммуникационных сетей, включающая:

- алгоритм формирования графа доступной части сети, позволяющий произвести сбор данных о топологии с любого узла-абонента;

- алгоритм формирования полного графа сети, позволяющий в условиях неполноты исходных данных осуществить прогноз топологии недостающей части сети.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, определяется корректным использованием автором методов исследования. В основу полученных научных результатов, выводов и рекомендаций, сформулированных в диссертации, положены теоретические положения математического аппарата теории графов, математической статистики, имитационного и аналитического моделирования.

Научная новизна результатов диссертационного исследования обусловлена тем, что при разработке имитационной модели реализации угрозы запрещенной информации в информационно-телекоммуникационных сетях учтены особенности их топологии (средняя степень связности узлов, средняя длина пути сети, коэффициент кластеризации сети), что позволило повысить точность представления процессов обеспечения информационной безопасности в анало-

1. Имитационная модель реализации угрозы запрещенной информации в информационно-телекоммуникационных сетях, учитывающая среднюю степень связности узлов, среднюю длину пути сети, коэффициент кластеризации сети, а также особенности информационного взаимодействия абонентов как человеко-машинных систем.

2. Аналитическая модель реализации угрозы запрещенной информации, отличающаяся от классической эпидемиологической модели Кермака-Маккендрика, тем, что в ней учены характеристики уязвимости информационно-телекоммуникационных сетей.

3. Методика формирования топологии крупномасштабных информационно-телекоммуникационных сетей, включающая:

- алгоритм формирования графа доступной части сети, позволяющий произвести сбор данных о топологии с любого узла-абонента;

- алгоритм формирования полного графа сети, позволяющий в условиях неполноты исходных данных осуществить прогноз топологии недостающей части сети.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, определяется корректным использованием автором методов исследования. В основу полученных научных результатов, выводов и рекомендаций, сформулированных в диссертации, положены теоретические положения математического аппарата теории графов, математической статистики, имитационного и аналитического моделирования.

Научная новизна результатов диссертационного исследования обусловлена тем, что при разработке имитационной модели реализации угрозы запрещенной информации в информационно-телекоммуникационных сетях учтены особенности их топологии (средняя степень связности узлов, средняя длина пути сети, коэффициент кластеризации сети), что позволило повысить точность представления процессов обеспечения информационной безопасности в анало-

защиты информационно-телекоммуникационных сетей, в аспекте противодействия методам лавинообразного распространения запрещенной информации.

Практическое значение результатов работы определяется тем, что полученные в диссертации практические наработки получили применение в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (РОСКОМНАДЗОР) по Владимирской области и в ОАО «Владимирское производственное объединение «Точмаш», что подтверждено соответствующими актами.

Автореферат в достаточной степени и верно раскрывает содержание основных положений диссертации.

К числу недостатков диссертационной работы следует отнести:

1. Постулированное свойство биективности при рассмотрении в 1-й главе человеко-машинной системы, когда одному пользователю соответствует одно устройство и одному устройству – один пользователь, в действительности не всегда выполнимо. На практике довольно часты ситуации, когда один пользователя использует несколько устройств, а также – когда несколько пользователей используют одно устройство.
2. Не ясно, из каких соображений был выбран объем реализации имитационного моделирования.
3. Автору следовало более детально подойти к обоснованию выбора эпидемиологической модели для использования в диссертационной работе в качестве базовой.
4. Автором уделено недостаточное внимание вопросу соответствия параметрам известной SIR-модели [формула (2.1), стр. 43] «физической сущности» исследуемого процесса распространения запрещенной информации в информационно-телекоммуникационной сети.

5. Практическую значимость исследования в определенной степени снижает то, что в диссертационной работе не уделено внимание оценке экономической эффективности предлагаемых решений.

Вывод

На основании материалов диссертации и автореферата следует сделать вывод, что диссертация является завершенной научно-квалификационной работой на актуальную тему, полученные в ней результаты имеют важное значение для повышения безопасности информационно-телекоммуникационных сетей от угрозы распространения запрещенной информации.

Диссертация удовлетворяет требованиям п.п. 9, 10, 11, 13, 14 Положения о присуждении учёных степеней, предъявляемым к кандидатским диссертациям, а её автор, Абрамов Константин Германович, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.12.13 – «Системы, сети и устройства телекоммуникаций».

Официальный оппонент

доктор технических наук, профессор, ведущий научный сотрудник отдела общесистемных исследований НИЦ МОУ «Институт инженерной физики»

Данилюк С.Г.

Подпись Данилюка С.Г. Заверяю

Начальник отдела кадров

04.09.14

Евченко В.В.