О Т З Ы В

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

Актуальность работы

Обеспечение информационной безопасности, исследование и разработка новых методов защиты информации являются одним из важнейших направлений исследований в области сетей, систем и устройств телекоммуникаций. Снижение уровня безопасности в телекоммуникационных системах связано, в первую очередь, с проблемой низкой защищенности абонентов от вредоносной и запрещенной информации. К сожалению, в настоящее время не существует эффективных механизмов защиты от таких угроз. Современные системы безопасности решают проблемы, связанные в первую очередь с защитой информации в телекоммуникационных сетях от вредоносной информации, а существующие типовые решения защиты пользователей от запрещенной информации не обладают необходимой гибкостью и точностью. В данных условиях одной из актуальных является задача повышения достоверности прогнозирования угрозы распространения запрещенной информации за счет разработки и внедрения новых моделей защиты сетей, систем и устройств телекоммуникаций.

Проведенное Абрамовым К.Г. исследование, связанное с разработкой и практической реализацией моделей угроз распространения запрещенной информации в информационно-телекоммуникационных сетях, несомненно, является актуальным и необходимым для обеспечения информационной безопасности в системах и сетях телекоммуникаций.

Содержание работы в целом соответствует названию и обозначенной проблематике. В диссертацию входит обзорная глава, в которой определен

объект исследования и уточнены задачи исследования; глава, в которой разрабатываются и исследуются модели угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях; глава, посвященная разработке методики формирования топологии крупномасштабной информационно-телекоммуникационной сети в условиях неполноты исходных данных, для этого предлагается комплекс алгоритмов; глава с результатами экспериментальных исследований угрозы распространения запрещенной информации, в которой также рассматриваются примеры эффективного апробирования механизмов прогнозирования угрозы.

Достоверность и новизна основных выводов и результатов диссертации.

Целью диссертационной работы является решение научно-технической задачи разработки новых моделей и алгоритмов, направленных на повышение достоверности и точности прогнозирования угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях.

Сформулированная цель достигается путем решения ряда задач. Выявлены существенные характеристики объекта и внешних факторов, влияющих на процесс реализации угрозы, разработана имитационная модель, учитывающая топологические особенности сети и информационного взаимодействия абонентов, синтезирована аналитическая модель реализации угрозы, учитывающая топологию сети, позволяющая провести оперативный прогноз, разработана методика формирования топологии крупномасштабной сети, позволяющая повысить точность представления модели топологии сети.

В целом предложенные модели позволяют повысить достоверность и точность прогнозирования угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях. Достоверность предложенных подходов определяется внедрением в практическое использование в организациях: ФГБОУ ВПО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столето-

вых» (ВлГУ), федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (РОСКОМНАДЗОР) по Владимирской области, ОАО «Владимирское производственное объединение «Точмаш», что подтверждено соответствующими актами.

Научная новизна разработанных алгоритмов, процедур и методик также подтверждается результатами обсуждения на международных научно-технических конференциях, публикациями 15 статей, в том числе 3-х в изданиях, включенных в перечень ВАК, а также получением трех свидетельств о государственной регистрации программ для ЭВМ.

Ценность для науки и практики

Ценность для науки определяется ранее научными результатами, выносимыми на защиту.

1. Разработана имитационная модель реализации УгЗИ в ИТКС, учитывающая среднюю степень связности узлов, среднюю длину пути сети, коэффициент кластеризации сети, а также особенности информационного взаимодействия абонентов как человеко-машинных систем и позволяющая повысить точность представления процессов обеспечения информационной безопасности в крупномасштабных ИТКС.

2. Предложена аналитическая модель реализации УгЗИ, отличающаяся от классической эпидемиологической модели Кермака-Маккендрика учетом характеристик уязвимости ИТКС и позволяющая повысить точность оперативного прогноза, особенно в условиях неполноты исходных данных о топологии сети.

3. Разработана методика формирования топологии крупномасштабной ИТКС, 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 спрогнозировать топологию недостающей части сети.

Применение методики позволяет повысить точность представления модели топологии ИТКС.

Они развивают методологию прогнозирования угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях.

Практическая ценность работы состоит в том, что разработанные программы имеют достаточно большой функционал, могут быть применены на широком кругу задач в информационно-телекоммуникационных сетях.

Замечания

1. Во второй главе работе при проведении экспериментов не приведено обоснование объема выборки для имитационного моделирования. Не раскрыто, чем обосновано выбранное количество проведенных экспериментов?

2. В пункте 3.2 рассматриваются три топологические характеристики: средняя степень связности, средняя длины пути, кластерный коэффициент. Непонятно, насколько обоснован выбор именно этих трех параметров.

3. Какова сложность представленных в третьей главе алгоритмов 3.1 и 3.2?

4. Не приведено описание процесса проверки точности (релевантности) модели реально существующей ситуации.

5. В работе не отмечено кто проводил оценку времени получения информации о топологии сети (20 суток) на с. 52.

Заключение

В целом работа представляет законченное научное исследование, включающее постановку проблемы, теоретические исследования и новые научные и практические результаты.

Представленная работа направлена на исследование и разработку новых методов защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций.

Автореферат соответствует содержанию диссертации, а опубликован-

ные научные работы отражают основные положения диссертации.

Диссертация Абрамова Константина Германовича соответствует требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Официальный оппонент
кандидат технических наук, доцент
начальник факультета подготовки научно-педагогических кадров
ФКОУ ВПО «Владимирский юридический институт федеральной службы исполнения наказаний»

К.Н. Курысев

05.09.2014