Отзыв официального оппонента
д.ф.-м.н Соколова Валерия Анатольевича на диссертационную работу
Антоненко Виталия Александровича
«Разработка и исследование модели функционирования глобальной сети для анализа динамики распространения вредоносного программного обеспечения», представленную к защите на соискание ученой степени кандидата физико-математических наук по специальности 05.13.11 – Математическое обеспечение вычислительных машин, комплексов и компьютерных сетей

В настоящие время наблюдается отчетливый рост новых экземпляров вредоносных программ. Так, например, 20% от всех когда-либо созданных вредоносных программ появилось в 2013 году, что составило порядка 30 млн. новых угроз, находящихся в обращении. Порядка 82 тыс. угроз появляется ежедневно. К сожалению, современное программное обеспечение не способствует снижению числа новых эпидемий вредоносных программ, которые находят все новые уязвимости в различных программных продуктах. Противодействие распространению вредоносных кодов достаточно сложная задача, которая имеет множество аспектов.

Построение системы обороны информационных и физических ресурсов современной компьютерной сети является актуальной и очень сложной задачей. Ее сложность проистекает из-за сложности информационных процессов в самой сети и ее масштабов. Естественным подходом при работе со сложными системами является имитационное моделирование. Моделирование работы сети позволяет произвести оценку стойкости системы обороны/защиты, оценить необходимые ресурсы.

Однако имитационные модели наряду с характерными для них достоинствами имеют ряд существенных недостатков. Разработка хорошей имитационной модели часто обходится дороже создания аналитической модели и требует больших временных затрат. Тем не менее, имитационное моделирование является одним из наиболее широко используемых методов при решении задач анализа сложных систем, к которым безусловно относится компьютерная сеть. Из достоинств имитационного моделирования можно выделить возможность описания поведения компонентов сети на высоком уровне детализации, возможность исследования взаимодействия компонент во времени и пространстве параметров системы, возможность подмены процесса смены событий в исследуемой системе в реальном масштабе времени на ускоренный процесс смены событий. Указанные достоинства обеспечивают имитационному методу широкое распространение.

Существенным моментом является масштаб моделируемой сети, что особенно становится важным при моделировании распространения некоторых типов вредоносного программ, например, сетевых червей. В современных глобальных компьютерных сетях (ГКС) актуально уметь оперативно прогнозировать динамику распространения вредоносного программного обеспечения. Для моделирования больших сетей, сопоставимых с ГКС, обычно используют наиболее абстрактные подходы к моделированию процесса функционирования сети. Для таких подходов характерна невысокая точность моделирования процессов сетевого обмена между узлами сети, что существенно, например, при прогнозировании динамики распространения вредоносного программного обеспечения (ВПО). Исходя из большой размерности и сложности структуры ГКС, эксперименты без использования моделирования затруднены по финансовым причинам, а также из-за невозможности физического воссоздания сети столь большого размера.

Таким образом, тема диссертации Антоненко В.А., связанная с моделированием динамики распространения вредоносного программного обеспечения, является безусловно актуальной как в теоретическом, так и в практическом плане.

Диссертация состоит из введения, четырех глав и заключения. Полный объем диссертации составляет 108 страниц с 36 рисунками и 5 таблицами. Список литературы содержит 115 наименований.

Во введении обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи работы, сформулированы научная новизна и практическая значимость представляемой работы. Первая глава посвящена обзору математических методов описания, построения моделей функционирования сети и средств реализации моделей сети. Во второй главе приведено описание формальной модели ГКС при помощи математических аппаратов: теории графов, элементов теории массового обслуживания, а также теории автоматов. Третья глава описывает архитектуру системы имитационного моделирования (СИМ) Network Prototype Simulator (NPS). В четвертой главе представлено экспериментальное исследование разработанной и реализованной СИМ NPS на примере моделирования динамики распространения активных сетевых червей (один из типов ВПО).

Основными результатами данной работы являются:

- Оригинальный подход к решению задачи имитационного моделирования глобальной компьютерной сети (ГКС);
- Формальная модель ГКС с возможностью оценки динамики распространения вредоносного программного обеспечения;
- Доказательство разрешимости задачи нахождения числа вредоносных хостов и доли вредоносного трафика в рамках предложенной модели ГКС;
- Реализация системы имитационного моделирования ГКС и проведение экспериментального исследования динамики распространения существующих экземпляров ВПО.

Основная идея предложенного подхода к моделированию ГКС заключается в представлении ГКС как сети автоматов. Оригинальность данного подхода заключается в применении комбинации математических методов: теории графов, теории массового обслуживания, теории автоматов, а также использования эпидемических моделей распространения вредоносных программ; что делает возможным строить масштабные, но в тоже время достаточно точные модели сетей.

Отдельно стоит отметить оригинальность подхода в реализации системы моделирования компьютерных сетей. Реализованная автором система имитационного моделирования базируется на методах легковесной виртуализации, что позволяет даже при существенно ограниченных вычислительных ресурсах строить точные имитационные модели компьютерной сети. Данный подход был справедливо назван «прототипированием» компьютерной сети, так как, по сути, совмещает в себе черты моделирования и эмулирования компьютерной сети. Автором показано, что такая система имитационного моделирования компьютерной сети уникальна в своем роде.

К достоинствам работы можно отнести возможность использования разработанной и реализованной системы моделирования в программно-конфигурируемых (ПКС) сетях, в исследованиях, посвященных разработке приложений для ПКС контроллеров, и при тестировании ПКС-сегментов сетей. Данное направление компьютерных сетей активно развивается в последние годы.

Также автором проведено экспериментальное исследование динамики распространения существующих экземпляров ВПО на примере сетевых червей CodeRedv2 и Sasser, демонстрирующее соответствие моделируемых процессов распространения ВПО в сети с реальными данными об эпидемиях конкретных сетевых червей. Выполнены эксперименты, показывающие возможности временной синхронизации между различными компонентами модели ГКС, по результатам которых показано, что системы моделирования может избегать некорректного поведения модели при несоответствии физических характеристик оборудования и требуемых модельных характеристик.

В качестве достоинств данной работы необходимо отметить понятный стиль изложения, строгость определений и четкость аргументации. Следует также обратить внимание на высокий уровень публикаций (в частности, статьи в трудах ведущих мировых конференций SIGCOMM и SCSC).

В качестве недочетов по содержанию и оформлению данной работы можно указать следующее:

- Описание возможностей разработанной и реализованной системы имитационного моделирования (особенно графического интерфейса) в автореферате является слишком лаконичным;
- Эксперименты с реальными данными о распространении сетевого червя Sasser носят чисто качественный и демонстрационный характер. Конечно, в первую очередь, это связанно с отсутствием информации необходимого уровня детальности об эпидемии Sasser в открытых источниках, что указанно в тексте диссертации. Однако, хотелось бы иметь четкий численный критерий точности моделирования динамики распространения сетевого червя Sasser;
- В эксперименте, посвящённом временной синхронизации между компонентами модели, нахождения физических каналов, которые не соответствуют моделируемым характеристикам, происходит только на этапе инициализации модели, что не позволяет детектировать подобные несоответствия в ходе моделирования. Наличие такой возможности позволило бы точнее определить изменения характеристик модели ГКС, связанных с несоответствием физических и моделируемых параметров.

Отмеченные недостатки не влияют на общую высокую оценку работы. Работа производит целостное впечатление, написана на хорошем математическом уровне,

содержит четкую постановку задачи, доказательство теоремы корректности предложенной формальной модели ГКС и подробное описание экспериментального исследования. Оригинальные результаты работы не имеют аналогов в известных оппоненту публикациях, т.е. являются новыми научными результатами. Содержание диссертации в достаточной степени опубликовано в научной печати, в том числе в трудах ведущих международных конференций и статьях в рецензируемых научных журналах из списка ВАК. Результаты работы прошли широкую апробацию на ведущих российский и международных конференциях. Научная достоверность и обоснованность полученных результатов определяются корректностью применения используемых в работе математических методов, а также результатами экспериментов на модельных и реальных данных.

Автореферат достаточно полно и правильно отражает содержание диссертации. Тематика и содержание диссертационного исследования соответствует специальности 05.13.11 – «Математическое обеспечение вычислительных машин, комплексов и компьютерных сетей».

В целом данная диссертационная работа представляет собой законченное научное исследование, выполненное на высоком научном уровне на актуальную тему, содержит новые научные результаты, имеющие существенное значение для рассматриваемой предметной области, и отвечает всем требованиям, предъявляемым ВАК к кандидатским диссертациям, а ее автор, Антоненко Виталий Александрович, заслуживает присуждения ему ученой степени кандидата физико-математических наук по специальности 05.13.11 «Математическое обеспечение вычислительных машин, комплексов и компьютерных сетей».

Официальный оппонент,
заведующий кафедрой теоретической информатики
Ярославского государственного университета
им. П.Г. Демидова,
доктор физико-математических наук, профессор Соколов В. А.

Подпись Соколова В.А. заверяю.
02.09.2014

Начальник управления по работе с персоналом
Р.И. Волкова