

Введение

Сегодня информационно-телекоммуникационные сети подвержены серьезным угрозам со стороны деструктивного программного обеспечения (ПО). Данные атаки порождают различные негативные последствия, такие как: замедление со стороны скорости работы вычислительной системы (сети); элементное или совокупное блокирование работы сети; возникновение сбоев работы средств автоматизированных систем; перенаправление информационных сообщений и т.д. [19, 67]. Особую опасность в этом плане представляют информационные инфраструктуры, которые используются в структуре контроля и управления технологическими процессами в системах критического применения.

Интегрирование в сеть приводит к увеличению рисков, связанных с легкой возможностью распространения вредоносного ПО в сети, а также - компьютерных червей и вирусов [7], противодействие которым невозможно осуществить без разработки и внедрения математического обеспечения, с помощью которого описывается процесс заражения [6, 10, 12, 27, 38], можно оценить масштабы возникающей эпидемии, рассмотреть изменчивость числа зараженных компьютеров, произвести оценку эффективности тех или иных средств защиты, а затем уже применять меры для повышения эпистойкости сети.

В настоящее время распространение компьютерных вирусов и иных вредоносных программ наносит огромный ущерб различным организациям и отдельно взятым пользователям, работа и взаимодействие которых в той или иной степени зависит от глобальных сетей. В связи с этим, за последние десятилетия распространение вредоносного кода, носившее локальный характер, превратилось в глобальные сетевые эпидемии. На скорость распространения вредоносной программы по сети могут влиять различные факторы, как аппаратные (пропускная способность канала, выход из строя сетевого оборудования, топология сети), так и программные (ограничения, введенные в среде распространения, например, операционной системе, с целью противодействия сетевым атакам) [121].

Один из основных способов изучения сетей является моделирование, которое принято рассматривать в двух аспектах. Первый касается моделирования топологии (структуры информационных связей между узлами сети) сетей [73, 77, 91, 97], а второй затрагивает проблему изучения процессов, проходящих в ней. Однако проблемой является распространение информационной инфекции, описание которой возможно с помощью эпидемиологических моделей.

Обычно анализ сводится к использованию классических моделей эпидемий [83], которые были разработаны еще в XIX веке в качестве поля изучения эпидемий инфекционных заболеваний и основанных на системах дифференциальных уравнений. Однако эти модели нельзя считать совершенными, тем более в контексте дискретного риск-анализа. Поэтому задача создания новых, более адекватных математических моделей [71, 83], актуальна и необходима для предсказания характера эпидемий, организации эффективного противодействия им посредством повышения их эпистойкости.

Степень разработанности темы исследования.

Касательно вопросов обеспечения информационной безопасности [1, 3, 4, 8, 11, 14, 15, 70] и, в частности, методов противодействия эпидемиям, а также особенностей их реализации, опубликовано значительное количество работ, в которых проанализированы как сами вирусные эпидемии, так и возможные меры, и средства для противодействия им [7, 11, 16, 19, 20, 26, 95, 96]. Однако в данной области отсутствуют глубокие исследования вопросов оценки эпистойкости неоднородных сетей и эффективности противодействия их инфицированию, включая определения вероятных ущербов, возникающих в неоднородных сетях при развитии эпидемий. Таким образом, совершенствование методологии риск - анализа в целях противодействия возникновению и распространению вирусных эпидемий в неоднородных сетях представляется достаточно актуальным. При этом, анализ возникающих эпидемических процессов, а главное - повышение эпистойкости системы (сети) в такой структуре взаимодействия, как неоднородные сети, становится важнейшим направлением исследования.

Объектом исследования являются неоднородные сети, подвергающиеся вирусным атакам с целью возникновения информационных эпидемий.

Предметом исследования является риск-анализ эпидемических процессов, возникающих в неоднородных сетях.

Цель исследования состоит в повышении эпистойкости неоднородных сетей на основе построения дискретных риск-моделей возникающих в них эпидемических процессов. Для достижения цели представляется необходимым решить следующие задачи:

1. Формализация описания эпидемических процессов, возникающих в неоднородных сетях, наиболее широко распространенных в современном информационном пространстве, на основе построения дискретных риск - моделей, включая матрицу послойной внутрисетевой связности.

2. Построение моделей инфицирования (вирусования) элементов сетей посредством «компьютерных червей», являющихся источником эпидемических процессов в неоднородных сетях.

3. Компьютерное моделирование эпидемических процессов, вызванных в неоднородных сетях инфицированием ее элементов различными «червями», включая риск-анализ, оценку эпистойкости и выработку рекомендаций по ее повышению.

Заключение

Работа посвящена разработке итерационных риск-моделей информационных эпидемий с дискретизацией по переходам элементов сети из незараженного в зараженное состояние и обратно с оценкой на каждом этапе (шаге итерации) параметров развития процесса с учетом мощностей множеств (элементов незараженных; элементов зараженных; элементов восстановленных после излечения; элементов иммунизированных и т.п.) при разнообразных условиях инфицирования (количество первичных источников, латентности и вероятности реализации переходов, топологических особенностей анализируемых сетей).

В результате проделанной работы:

1. Построены эпидемические модели сетей в контексте их топологического многообразия и эпистойкости, что необходимо учитывать при проектировании и эксплуатации защищенных неоднородных сетей. Исследованы особенности аналоговых моделей вирусно-инфицированных гетерогенных сетей, в том числе с учетом статистической корреляции. Предложена многослойная формализация описания сетей с распределенной степенью вершин, включая матрицу послойной внутрисетевой связности, а также - макро и микро - модели распространения инфекции и вирусования элементов в гетерогенных сетевых структурах.

2. Разработаны дискретные модели процесса инфицирования элементов сети за счет внедрения почтовых червей, включая эффекты реинфицирования и мутации. Для процесса инфицирования элементов сети путем внедрения сетевого червя разработаны соответствующие модели, учитывающие латентность и мутацию червя. Предложены модели деструктивного воздействия на элементы сети за счет внедрения компьютерных IM -, IRC - и P2P - червей, включая эффект мутации червя.

3. В реализации практической части предложено описание разработанного программного обеспечения моделирования эпидемических процессов в неоднородных сетях, включая процедуру автоматизированной генерации сети, а также - послойного инфицирования. Для безмасштабных сетей, сетей типа «малые