ВВЕДЕНИЕ

Сетевой принцип организации систем лежит сегодня в основе глобального информационного пространства. При этом сети принесли не только новые возможности, но и новые угрозы. Альтернативой сетевого взаимодействия и сотрудничества стало сетевое противоборство, наивысшей формой которого следует считать сетевые войны. Ущерб, наносимый столкновениями в информационно-телекоммуникационных сетях, становится все более значительным, а арсенал средств деструктивного сетевого воздействия — все более изощренным. Одним из наиболее коварных видов такого воздействия следует считать рукотворные эпидемии, реализуемые с помощью специально разработанных вирусов.

Моделированию эпидемических процессов, организуемых в гомогенных сетевых кластерах (т. е. кластерах с высокой степенью однородности их элементов) и в гетерогенных сетях (т. е. в сетях с высокой неоднородностью их элементов), посвящена настоящая монография. В гомогенном сетевом кластере практически все элементы имеют жесткую организацию связей (одинаковую степень вершин). В гетерогенных сетях жесткой организации связи в сети нет, и каждый элемент сети может иметь произвольную степень вершины.

Использование сетевых структур практически во всех сферах жизнедеятельности современного общества значительно расширяет возможности злоумышленников в использовании методов и средств деструктивного воздействия на информационно-телекоммуникационные сети (ИТКС) различного назначения [87, 162, 164].

Все чаще ИТКС подвергаются атакам вредоносного программного обеспечения (ПО), приводящего к различным негативным последствиям: уменьшение скорости работы вычислительной системы (сети); частичное или полное блокирование работы сети; имитация сбоев работы средств вычислительной техники; переадресация сообщений и др. [10, 161, 184, 185, 208]. Особую опасность в этом плане представляют информационные инфраструктуры, используемые для контроля и управления технологическими процессами в системах критического применения [181, 183, 217], где вирусы и черви фактически стали оружием сетевой войны.

Сетевая интеграция приводит к росту рисков, связанных с возможностью распространения по сети вредоносного ПО и одной из его разновидностей —компьютерных червей и вирусов [146], борьба с которыми невозможна без разработки и внедрения научно-методического обеспечения, описывающего процесс заражения [144, 145, 149, 150, 152, 168, 172, 176, 178, 186]. С помощью математических моделей можно оценить масштабы возможной эпидемии, изучить динамику изменения числа зараженных компьютеров, оценить эффективность тех или иных мер лечения уже зараженных компьютеров или предварительного устранения уязвимостей в ПО, которые используются вредоносным кодом для инфицирования.

В этом контексте, наиболее популярными являются различные антивирусные программы [187, 211, 215], хотя доказана принципиальная невозможность реализации «абсолютного антивируса» [15, 175]. Исследования показали, что механизм распространения компьютерных вирусов во многом схож с механизмами распространения инфекций в биологических популяциях [60—62, 81, 126, 139, 146, 176, 177].

Сетевое распространение компьютерных вирусов и других вредоносных программ наносит огромный ущерб различным организациям и отдельным пользователям компьютеров, работа и функционирование которых так или иначе связана или полностью зависит от глобальных сетей. Именно поэтому за последние десятилетия распространение вредоносного кода, носившее ранее локальный характер, превратилось в сетевые эпидемии [172, 177], исследованию которых и посвящена настоящая монография.

Один из основных способов изучения ИТКС является моделирование, которое можно рассматривать в двух аспектах. Первый касается моделирования топологии (структуры информационных связей между узлами сети) сетей [2, 9, 26, 33, 67, 73, 80], а второй посвящен изучению процессов, проходящих в ней. В нашем случае данной проблемой является процесс распространения информационной инфекции [190—204], описание которого возможно с помощью эпидемиологических моделей. Среди них есть модели, базирующиеся на исследованиях в области эпидемиологии — SI, SIR, SIS, а также модели, специально разработанные для исследования эпидемий в компьютерных сетях — AAWP, LAAWP, PSIDR. Рассматривая первую группу моделей [40], можно отметить, что среди них есть те, которые предусматривают лечение инфицированных элементов системы, и модели с отсутствием лечения. Такие модели могут предусматривать иммунизацию и даже смерть элементов сети. Из особенностей второй группы моделей [12, 57, 130, 138]

выделяется их ограниченная способность учитывать специфику распространения инфекции.

В настоящее время активно ведутся исследования различных аспектов противодействия вирусным атакам на основе риск-оценки [191—204, 212], включая разработку аппарата риск-анализа систем при множественности источников заражения [204, 205]. Разработаны модели сетевых атак с внедрением вредоносного программного обеспечения на основе сетей Петри—Маркова [144, 147, 152]. Изучаются воздействия различных типов вирусов на компьютерные системы [132, 190], включая влияние топологии сети на процесс развития эпидемий, ее защищенность от вирусов [2, 33, 100—102, 143, 148, 206] и динамику распространения вредоносного программного обеспечения в сетях с учетом действия антивирусов [163].

Имеет место широкое использование классических эпидемиологических моделей [40, 60, 61], разработанных еще в XIX веке для изучения эпидемий инфекционных заболеваний и основанных на системах дифференциальных уравнений. Однако эти модели нельзя считать совершенными, особенно в контексте дискретности эпидемических состояний и процедуры риск-анализа. Поэтому задача создания новых, более адекватных математических моделей [13, 16, 40, 61 62, 163, 172, 188, 206], актуальна и необходима для предсказания эпидемий и организации эффективного противодействия им.

В контексте развития вышеуказанных исследований представляется целесообразным формализованное описание механизмов инфицирования вредоносными программами элементов ИТКС и работы антивирусного программного обеспечения, включая разработку математических моделей процессов развития вирусных эпидемий. Данные модели должны учитывать топологию сети и возможность регулирования эпистойкости на основе анализа рисков заражения ее элементов на различных стадиях эпидемического процесса, чему и посвящена настоящая монография.

Такой подход представляет реальный практический интерес в контексте современного сетевого противоборства. Наиболее ярким тому примером следует считать процессы распространения деструктивного контента в социальных сетях. Они давно уже стали инструментом информационно-психологического воздействия на широкие массы людей, и прогнозирование возникающих в них эпидемических процессов является весьма актуальной задачей. Поэтому одну из последующих в настоящей серии монографий планируется посвятить именно вопросам распространения деструктивного контента в соцсетях. В этой связи на основе

разработанного в упомянутой серии методического обеспечения был создан программный комплекс «Netepidemic». Резюме этого проекта представлено в приложении к данной монографии. С его помощью для социальных сетей может быть осуществлено имитационное моделирование с представлением соответствующих результатов для различных значений параметров, характеризующих особенности распространяемого контента, источников его распространения и пользователей, потребляющих этот контент в сети.

Авторы выражают признательность Корнеевой Н.Н., Исламгуловой В.В., Пономаренко Е.Н., Суркову И.А., Манюхину В.А. и Попову А.И. за помощь в подготовке материалов рукописи настоящей монографии.