ОГЛАВЛЕНИЕ

Введение 6
1 Дискретные риск-модели развития эпидемий в неоднородных сетях 13
1.1 Модели эпидемий в сетях 13
1.1.1 Разновидности эпидемических моделей и сетей 13
1.1.2 Топологическое многообразие сетей в контексте их эпистойкости 16
1.1.3 Особенности аналоговых моделей вирусно-инфицированных сетей 22
1.1.4 Аналоговые модели, учитывающие корреляцию 32
1.2 Многослойная формализация описания сетей с распределенной степенью вершин 41
1.2.1 Сущность дискретных моделей послойной формализации 41
1.2.2 Дискретные модели многослойного риск-анализа 49
1.2.3 Микро-фрактал дискретной модели заражения 59
1.3 Выводы по первой главе 64
2 Модели инфицирования элементов сетей посредством компьютерных червей 65
2.1 Модели инфицирования элементов сетей почтовыми червями 65
2.1.1 Модель без реинфекции с мутацией почтового червя 68
2.1.2 Модель без реинфекции и без мутации 70
2.1.3 Модель с реинфекцией и мутацией 73
2.1.4 Модель без мутации и реинфицирования 76
2.1.5 Модель с мутацией и без реинфицирования 80
2.2 Модели инфицирования сетевыми червями 83
2.2.1 Простейшая модель инфицирования 83
2.2.2 Модель инфицирования с учетом мутации 85
2.2.3 Модель инфицирования с учетом латентности 87
2.2.4 Модель инфицирования по образу файлового вируса 89
2.3 IM - , IRC - и P2P - черви: модели инфицирования элементов сетей 92
2.3.1 IM - черви как инструмент деструктивного воздействия на неоднородные сети 92
2.3.1.1 Модели инфицирования IM - червями без мутации 93
2.3.1.2 Модель инфицирования IM - червями с мутацией 97
2.3.2 IRC - черви как инструмент деструктивного воздействия на неоднородные сети 101
2.3.2.1 Специфика заражения IRC - червем 101
2.3.2.2 Модель инфицирования IRC - червем с учетом мутации 103
2.3.3 P2P - черви как инструмент деструктивного воздействия на неоднородные сети 106
2.3.3.1 Модель инфицирования P2P - червей с учетом его мутации 107
2.3.3.2 Модель инфицирования P2P - червем с мутацией 110
2.4 Выводы по второй главе 113
3 Имитационное моделирование эпидемического процесса в неоднородных сетях 114

3.1 Программное обеспечение и тесты для дискретного моделирования эпидемического процесса, порожденного компьютерными червями 114
3.1.1 Генерация неоднородных сетей 114
3.1.2 Моделирование эпидемических процессов в сетях 121
3.2 Анализ результатов моделирования эпидемического процесса и выработка рекомендаций по управлению эпистойкостью сети 131
3.2.1 Результаты моделирования эпидемического процесса, порожденного компьютерными червями 131
3.2.2 Выработка рекомендаций по управлению эпистойкостью атакуемой сети 147
3.3 Выводы потретей главе 151
Заключение 152

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 быстроты 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.

Работа выполнена в соответствии с одним из основных направлений ФГБОУ ВПО «Воронежский государственный технический университет» «Управление информационными рисками и обеспечение безопасности инфокоммуникационных технологий» на базе Воронежского научно-образовательного центра управления информационными рисками.

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.

На защиту выносятся:

1. Многослойная формализация эпидемических неоднородных сетей на основе послойной матрицы внутрисетевой связности.

2. Модели процессов инфицирования всевозможными «компьютерными червями» элементов неоднородных сетей.

3. Программное обеспечение и результаты компьютерного моделирования эпидемических процессов, протекающих в неоднородных сетях.

Новизнарезультатов:

1. Созданы дискретные риск-моделивирусования, отличающиеся от аналогов наличием многослойной формализацией инфицированных неоднородных сетей с использованием матрицы послойной внутрисетевой связности.

2. Разработаны эпидемиологические модели инфицирования элементов неоднородных сетей «компьютерными червями», в отличие от аналогов, на основе микро-фракталов учитывающие такие процессы, как латентность, мутацию, и эффекты реинфицирования червя.

3. Осуществлено компьютерное моделирование эпидемических процессов в неоднородных сетях, посредством программного обеспечения, отличается от аналогичных применением дискретных послойных моделей, а также оценкой эпистойкости.

Теоретическая значимость работы, состоит в том, что:

- доказаны положения, вносящие вклад в расширение представлений о явлении вирусования компьютерными червями элементов сетей;

- применительно к проблематике работы, с получением обладающих новизной результатов, использован аппарат теории риск-анализа в отношении инфицирования неоднородных сетей почтовыми, сетевыми, IM - , IRC - и P2P - червями;

- изложены положения и элементы теории для аналитической оценки ущерба, риска и эффективности защиты элементов неоднородных сетей, подвергающихся инфицированию компьютерными червями;

- раскрыты противоречия между значимостью проблемы защиты элементов сетей и адекватностью моделей и методик оценки и управления их эпистойкостью в рамках эпидемий, создаваемых в неоднородных сетях;

- изучены внутренние и внешние противоречия, факторы и причинно-следственные связи, порождающие информационные риски успешного

инфицирования неоднородных сетей компьютерными червями сетевого и почтового типа, а также различными модификациями IM - , IRC - и P2P - червей;

- проведена модернизация существующих математических моделей и алгоритмов, которая предоставляет возможность аналитической оценки и управления рисками неоднородных сетей, подвергающихся вирусованию.

Практическая ценность работы заключается в том, что:

- в рамках существующей концепции моделирования эпидемий, предложена оригинальная послойная формализация, которая может быть применена для описания неоднородных сетей различных типов;

- разработанные дискретные риск-модели, дают необходимый инструментарий для оптимизации, управления эпистойкостью и регулирования рисков, что позволяет улучшить устойчивость неоднородных сетей при возникновении эпидемических процессов;

- программное обеспечение моделирования, предлагает эффективный инструментарий для автоматизированного анализа эпидемических процессов и оценки эпистойкости в неоднородных сетях.

Методы исследования. В исследовании используются методы системного и математического анализа, теории вероятностей и математической статистики, методы теории рисков.

Соответствие специальности научных работников. Полученные научные результаты соответствуют следующим пунктам специальности научных работников 05.13.19 «Методы и системы защиты информации, информационная безопасность»: анализ риска нарушения безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения (п. 7); модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты (п. 10); модели и методы управления информационной безопасностью (п. 15).

Степень достоверности научных положений и выводов, сформулированных в исследовании, подтверждаются тем, что:

- теория построена на известных, проверяемых фактах статистического исследования заражения компьютерными червями элементов сетей, что согласуется с опубликованными результатами в данной области [15, 27, 46, 85, 101];

- идея базируется на анализе практики и обобщении передового отечественного и зарубежного опыта в области оценки и управления рисками, представленного в нормативных документах [23-25, 29, 30-38, 60];

- использовано сравнение авторских данных с результатами, полученными ранее, по проблематике рассматриваемой области в работах Новикова Д.А. [28, 29], Борисова В.И. [37], Остапенко А.Г. [30, 32, 33, 35, 102], Калашникова А.О. [24, 25, 86];

- установлено качественное совпадение авторских результатов с результатами, представленными в работах лаборатории Касперского [21], Pastor-Satorras R. [108, 112, 113] и Радько Н.М. [42, 44] в области вирусных эпидемий и моделирования процессов инфицирования элементов сети;

- использованы современные методики сбора и обработки информации, предоставленные ведущими отечественными и зарубежными организациями в области защиты и информации, выборочные совокупности численных значений частоты возникновения эпидемий в сетях [56, 58, 73, 88, 103].

Внедрение результатов работы.

Полученные основные научные результаты исследования используются в ФГБОУ ВО «Воронежский государственный технический университет» в учебном процессе на кафедре систем информационной безопасности при организации изучения специальных дисциплин в ходе подготовки специалистов по специальности 10.05.03 «Компьютерная безопасность», 10.05.04 «Информационная безопасность телекоммуникационных систем», 10.05.05 «Информационная безопасность автоматизированных систем», что подтверждено актом о внедрении в учебный процесс, а также АО «Нововоронежская атомная станция».

Апробация работы. Основные результаты исследований и научных разработок докладывались и обсуждались на Международной научно- практической конференции «Безопасность инфокоммуникационных технологий» (Воронеж, 2015

и 2016 гг.), 56-й научно-технической конференции профессорско-преподавательского состава, сотрудников, аспирантов и студентов Воронежского государственного технического университета (Воронеж, 2016 г.).

Публикации. По теме работы опубликовано 3 научные работы в изданиях, рекомендованных ВАК РФ.

Структура и объем работы. Работа состоит из введения, трех глав, заключения, списка литературы, включающего 141 наименование. Основная часть работы изложена на 170 страницах, содержит 95 рисунков и 2 таблицы.

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

миры», экспоненциальных и пуассоновских сетей с помощью разработанной программы осуществлено моделирование эпидемических процессов, порожденных компьютерными червями. На основе исследования результатов моделирования выработаны рекомендаций по управлению эпистойкостью атакуемых неоднородных сетей.

Аналитический характер полученных результатов открывает перспективу численных многовариантных расчетов и оптимизации в целях управления эпистойкостью системы и позволит создать научно-методическую основу для эффективного функционирования вирусно-атакуемых неоднородных сетей.

Результаты работы нашли свое применение в учебном процессе и в производстве.