ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы.Информация сегодня выступает как средство обеспечения успеха в бизнесе, так и объект самой серьезной защиты, это и один из наиболее значимых активов предприятия, но и один из наиболее существенных элементов риска. В этом контексте, прежде всего информационные сети становятся все более уязвимыми и требующими серьезной многоуровневой защиты. При этом, существенно вырастает цена, которую приходится платить владельцу ценной информации, не предпринимающему к защите своих ресурсов должных усилий.

Уже недостаточно рассматривать информационные сети как совокупность различных элементов. Сегодняшние реалии требуют более глубокого их изучения, а именно, учета веса элементов сети, которые формируют так называемые взвешенные сети. Именно они являются основной целью деструктивных действий злоумышленников.

В основе многих деструктивных процессов в информационных сетях сегодня зачастую являются информационные конфликты [**Ошибка! Источник ссылки не найден.–Ошибка! Источник ссылки не найден.**]. Современные деструктивные (в том числе террористические) воздействия во многом реализуются в информационных сетях, причем их последствия (ущербы) весьма ощутимы как для самих сетей, так и для их пользователей [**Ошибка! Источник ссылки не найден.–Ошибка! Источник ссылки не найден.**]. Поэтому очень важно понимать причину информационных конфликтов, механизмы их развития и сценарии протекания.

В связи с этим конфликт рассматривается как взаимообусловленные действия по нанесению заданного информационного ущерба и обеспечению минимума потерь, осуществляемые с целью достижения информационного превосходства.

В этой связи очевидно растут риски. Причем увеличиваются не только размеры возможных ущербов, но и вероятность их наступления. В этом контексте актуальность сетевого риск–анализа и управление рисками становится одной из важнейших проблем, разрешение которой может значительно повысить защищенность взвешенных сетей.

Поэтому представляется актуальнымразработка моделей взвешенных сетей, учитывающих конфликтность противоборствующих в них субъектов.

Степень проработанности темы исследования. Современная теория сетейсоздавалась зарубежными учеными, такими как Y. Ahn [**Ошибка! Источник ссылки не найден.**], L.C. Freeman [**Ошибка! Источник ссылки не найден.**–**Ошибка! Источник ссылки не найден.**],M. E. J. Newman [**Ошибка! Источник ссылки не найден.**–**Ошибка! Источник ссылки не найден.**], но онануждается в модернизации, так как в основном ориентирована на так называемые не взвешенные сети [**Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**–**Ошибка! Источник ссылки не найден.**], где весами вершин и дуг (физическими параметрами хранимого и перекачиваемого в сети наполнителя) стараются пренебречь. Однако такой подход не приемлем для измерения вероятных ущербов [**Ошибка! Источник ссылки не найден.**], объективно необходимого для риск–анализа [**Ошибка! Источник ссылки не найден.**–**Ошибка! Источник ссылки не найден.**], при обеспечении сетевой безопасности [**Ошибка! Источник ссылки не найден.**,**Ошибка! Источник ссылки не найден.**].

В этой связи для анализа процессов сетевого противоборства необходимо значительное развитие теоретических основ описания сетей в контексте учета взвешенности их элементов в соответствии со спецификойдеструктивных операций, приводящих к информационным конфликтам в сетях.

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 взвешенные информационные сети и возникающие в них конфликты противоборствующих сторон.

Предметом исследования являютсяриски, возникающие в процессе информационного противоборства во взвешенных информационных сетях.

Цель исследования состоит в повышении защищенности взвешенных сетей на основе разработки их моделей, учитывающих конфликтность противоборствующих в них субъектов.

Для достижения поставленной цели необходимо решить **следующиезадачи:**

1. Формализация описания взвешенных сетей с учетом ценности хранящегося и циркулирующего в них наполнителя, включая аналитические выражения метрик взвешенности этих сетей и их элементов.

2. Качественная и количественная оценка конфликтов сетевого характера, мотивирующих противоборство во взвешенных сетях.

3. Формализация стратегий и тактических приемов противоборства в сетях с учетом ресурсного обеспечения (ценности наполнителя) узлов и ребер взвешенных сетей и его чувствительности в динамике разрешения конфликта.

4. Формализация вероятностных и энтропийных моделей сетевого конфликта террористического характера с учетом возникающих рисков при атаках на элементы критической инфраструктуры.

Результаты, выносимые на защиту:

1. Формализация описания взвешенных сетей на основе матрицы весов (ресурсов) их дуг и вершин, оценивающих ценность циркулирующего и хранящегося наполнителя, а также – метрик взвешенности элементов сети.

2. Формализация сетевого конфликта, использующая функции чувствительности еѐ ресурса в его классификации и измерении глубины во взвешенных сетях.

3. Стратегии и тактические приемы сетевого противоборства, схемы реализации которых формализованы для взвешенных сетей с помощью графов и функций чувствительности ресурса сети.;

4. Вероятностные и энтропийные моделисетевого конфликта террористического характера, а так же аналитическая оценка рисков террористических атакна элементы критической инфраструктуры.

Методы исследования. Для решения поставленных задач в работе используются методы системного анализа, математического анализа, теория игр, теория графов, теория конфликтов и методы математического моделирования.

Новизна результатов:

1. Впервые введены матрица и метрики взвешенности дуг и вершин сети, оригинальность которых заключается в оценке ценности хранящегося и циркулирующего сетевого наполнителя.
2. Модели сетевого конфликта, отличающиеся от аналогов оценкой его глубины и существа с помощью функций чувствительности ресурса элементов сети.
3. Стратегии и тактические приемы сетевого противоборства, модели реализации которых в отличии от аналогов формализованы с помощью графов и функций чувствительности ресурса элементов сети.
4. Вероятностные и энтропийные модели, которые в отличие от аналогов предусматривают оценкуи регулирование рисков при террористических атакахна элементы критической инфраструктуры.

Теоретическая значимость результатов работы, состоит в том, что:

– доказаны положения, вносящие вклад в расширение представлений о теориивзвешенных информационных сетей, в которых в отличии от невзвешенных сетей все структурные элементы имеют вес (ресурс), обусловленный ценностью наполнителя;

– изложены обновленные положения и элементы теории конфликтов для аналитического описания классов конфликтов, совместносо своей спецификой, характеризующей взаимодействие конфликтующих информационных сетей;

– изучены факторы и причинно–следственные связи реализации стратегий и тактик сетевого противоборства, инициированного развитием динамики процессов информационных конфликтов;

– проведена модернизация существующих вероятностных и энтропийныхмоделей террористических атак на взвешенные сети, обеспечивающая возможность аналитической оценки и регулирования рисков, с учетом особенностей атак ихарактеристик сетей.

Практическая ценность результатов:

1. Матрица и метрики взвешенности элементов сети открывают перспективы описания наиболее часто встречающихся на практике сетей, где вершины и дуги имеют обусловленный ценностью наполнителя вес, без учета которого не представляется возможным оценить ущербы и риски сетевого противоборства.

2. Оценка существа и глубины конфликта, как источника возникновения сетевого противоборства, является практической основой как для стратегических, так и для тактических действий в ходе разрешения конфликтных ситуаций между соперничающими в сетях сторонами.

3. Инструментарий стратегий и тактик противоборства расширяет пространство практического применения на наиболее распространенные сегодня взвешенные сети, где стратегические и тактические управленческие решения необходимы принимать с учетом ценности защищаемого ресурса в сетях.

4. Вероятностные и энтропийные модели сетевого конфликта террористического характера открывают возможности для применения разработанного математического аппарата при управлении рисками в сетях критически важных объектов.

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 работе, подтверждаются тем, что:

– теория построена на известных, проверяемых фактах исследования в области построения и функционирования сетей, а также теории конфликтов, что

согласуется с опубликованными данными в областисетевого противоборства[**Ошибка! Источник ссылки не найден.**,**Ошибка! Источник ссылки не найден.**,**Ошибка! Источник ссылки не найден.**];

– идея базируется на анализе практики и обобщении передовогоотечественного и зарубежного опыта в области построения и исследования характеристик сетей, функционирующих в условиях информационногоконфликта[**Ошибка! Источник ссылки не найден.**,**Ошибка! Источник ссылки не найден.**];

– использовано сравнение авторских данных с результатами, полученнымиранее, по рассматриваемой области в работах NewmanM. E. J.[**Ошибка! Источник ссылки не найден.–Ошибка! Источник ссылки не найден.**], FreemanL. C. [**Ошибка! Источник ссылки не найден.–Ошибка! Источник ссылки не найден.**],Pastor–SatorrasR. [**Ошибка! Источник ссылки не найден.–Ошибка! Источник ссылки не найден.**] в области развитиямоделей эпидемических процессов в сетях и сетевых метрик, используемых при анализе сетей;

– установлено качественное совпадение авторских результатов срезультатами, представленными в работах по рассматриваемой области Новикова Д.А. [**Ошибка! Источник ссылки не найден.**], Борисов В.И. [**Ошибка! Источник ссылки не найден.**], Остапенко А.Г. [**Ошибка! Источник ссылки не найден.**],Калашников А.О. [**Ошибка! Источник ссылки не найден.–Ошибка! Источник ссылки не найден.**];

– использованы современные методики риск–анализа террористических атак на сети[**Ошибка! Источник ссылки не найден.**,**Ошибка! Источник ссылки не найден.**].

Внедрение результатов работы.Полученные основные научные результаты дипломного 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 10.05.01«Компьютерная

безопасность», 10.05.02«Информационная безопасность телекоммуникационных систем», 10.05.03 «Информационная безопасность автоматизированных систем», что подтверждено актом о внедрении в учебный процесс.

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

Личный вклад автора. Все основные результаты работы получены автором самостоятельно. В работах, опубликованных в соавторстве, лично автору принадлежат: элементы моделей атак террористов на элементы критической инфраструктуры [**Ошибка! Источник ссылки не найден.**]; элементы вероятностных и энтропийных моделей террористических атак[**Ошибка! Источник ссылки не найден.**]; анализ сетевой террористической деятельности[**Ошибка! Источник ссылки не найден.**].

Структура и объем работы. Работа состоит из введения, четырех глав, заключения, списка литературы, включающего 72 наименований. Основная часть работы изложена на 125 страницах, содержит 29 рисунков и 7 таблиц.

ЗАКЛЮЧЕНИЕ

Работа посвящена развитию теории взвешенных сетей и повышению защищенности на основе разработки их моделей, учитывающих конфликтность противоборствующих в них субъектов.В результате выполнения работы были получены следующие основные результаты:

1. В целях развития теории сетей в части учета весов их элементов предложено обратить внимание на сетевой наполнитель и такие его параметры как удельная ценность и объѐм. В этой связи предложено оценивать веса через ресурсы и потенциалы. При этом ресурс вершины определен как произведение удельной ценности наполнителя на его объем, хранящийся в вершине. В свою очередь, вес дуги определен как произведение удельной ценности наполнителя на его объем,

прокачиваемый по дуге в единицу времени. Соответственно потенциалы этих элементов определены как предельно допустимые их ресурсы. Для формализации описания взвешенных сетей предложена матрица взвешенности, диагональные элементы которой представляют собой ресурсы вершин, а прочие – ресурсы дуг. Такая формализация дает картину не только смежности элементов, но и их значимости в сети на основе оценки ценности еѐ аккумулируемого и циркулирующего наполнителя. В развитие традиционных сетевых измерений были предложены метрики для взвешенных сетей, включая: степень взвешенной центральности вершины; нормированную оценку степени взвешенной центральности вершины; степень центральности всей сети; плотность центральности; плотности взвешенной центральности; центральность как посредничество; взвешенную эквивалентность вершин. Эти метрики важны для выявления наиболее опасных элементов взвешенных сетей с точки зрения возможных деструктивных воздействий.

2. С использованием понятия потенциала и ресурса сети предложена обобщенная формализация сетевого конфликта, включая измерение его глубины с помощью полуотносительной чувствительности для множеств вершин и дуг. Известная классификация разновидностей конфликтов через функции относительной чувствительности ресурсов сети интерпретирована для сетевой конфликтологии. Полученные в этой связи аналитические выражения могут быть полезны для анализа и описания конфликтных ситуаций в сетевых структурах в динамике функцийотносительной чувствительности к изменению параметров ресурса и потенциала сети.

3. С учетом взвешенности элементов сети предложена новая классификация стратегий сетевого противоборства: устранение пользователей сети, нарушение внутрисетевых связей, обесценивание наполнителя сети, обескровливание сети по наполнителю, а так же – гибридная стратегия. С помощью графов формализованы схемы их реализации. С использованием функций полуотносительной чувствительности предложены и формализованы тактики сетевого противоборства: противодействие развитию сети противника, сокращение

динамического ресурса противника, наращивание объема наполнителя, наращивание потенциальных возможностей, ограничение наполнителя в сети противника, изоляция сети противника, снижение ценности наполнителя в сети противника, шунтирование, введение альтернативного хаба, подмена недружественного кластера управляемым аналогом.

4. С использованием ресурса сети формализована структура сетевого конфликта террористического характера, включая метрики его глубины. Предложены вероятностные и энтропийные модели сетевого конфликта террористического характера с учетом аналитической оценки и регулирования рисков возникновения конфликтных ситуаций. С учетом таких характеристик как ценность единицы объема наполнителя и пропускной способности сети в контексте риск–анализа предложены аналитические выражения риска, ущерба, шанса, и жизнестойкости элементов критической инфраструктуры.

Применение полученных результатов в работе позволит создать научно–методическую основу для эффективного существования и функционирования взвешенных сетей, а также существенно снизить риски реализации и ущербы, возникающие в результате межсетевого противоборства, а также при проведении террористических атак на взвешенные сети.