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. 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. 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.

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.

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