ВВЕДЕНИЕ

Актуальность. В настоящее время интернет проник во все сферы жизнедеятельности человека благодаря предоставлению огромного числа услуг и сервисов. Ещё несколько лет назад, доступ к интернету осуществлялся, преимущественно, путем проводного соединения из-за низкой скорости беспроводных сетей.

Однако относительно недавно беспроводные сети вышли на качественно новый уровень развития – по всему миру стали активно использоваться технологии четвертого поколения мобильной связи LTE и WiMAX 2, которые позволяют осуществлять передачу данных со скоростью более 100Мбит\с. Помимо этого увеличилось качество и других типов беспроводной связи. Так как в одну беспроводную сеть объединены разнообразные технологии предоставления доступа к сети интернет и устройства с различными ОС, то можно назвать такую сеть гетерогенной беспроводной сетью.

В условиях современности сетевые структуры стремительно развиваются – как с точки зрения их топологии, так и с точки зрения расширения их функциональных возможностей. При этом увеличивается не только число пользователей сети, но и количество ее оборудования, а также объемы передаваемого наполнителя. В этом контексте становится необходимым системный анализ данного процесса, являющийся важным не только для успешного функционирования этих сетей, но и для полноценной их защиты.

По мере эволюции подобных сетей расширяется область их применения в качестве плацдарма для сетевых конфликтов.

В настоящее время диапазон возможностей информационного оружия настолько велик, что имеются прецеденты достижения победы в операциях и конфликтах только за счет его применения, без использования традиционных средств вооруженной борьбы [41].

В связи с этим исследование беспроводных гетерогенных сетей, стратегий сетевого противоборства, используемых в конфликтах, которые происходя в этих

сетях, и обеспечение их безопасности является одним из самых актуальных направлений не только в России, но и по всему миру.

Степень проработанности темы исследования. В настоящее время существует множество статей, посвященных беспроводным гетерогенным сетям, сетевому противоборству, риск-анализу и моделированию. В имеющейся литературе рассмотрены такие вопросы, как:

– общая информация о беспроводных гетерогенных сетях, преимущества и недостатки данных сетей;

– построение модели беспроводной сети на основе графа, определение взвешенности графа и ценности информации, циркулирующей в данной сети;

– стратегии и тактики сетевого противоборства;

– меры, средства и модели противодействия воздействию противника;

– оценка, анализ и управление рисками.

Несмотря на большой объем литературы, в данной области мало исследовался вопрос воздействия на беспроводные гетерогенные сети (как на информацию, передаваемую в этих сетях, так и на информационные системы в целом) в процессе сетевого противоборства. Таким образом, совершенствование методологии риск-анализа в целях повышения защищенности пользователей беспроводных сетей и самих сетей от воздействия участников сетевого конфликта представляется актуальным.

Цель исследования заключается в повышении защищенности беспроводных сетей с помощью разработки моделей, учитывающих конфликтность использующих их субъектов.

Объектом исследования являются беспроводные гетерогенные сети и возникающие в них конфликты противоборствующих сторон.

Предметом исследования является риск-анализ состояния элементов беспроводных гетерогенных сетей при реализации стратегий сетевого противоборства и управление их защищенностью.

Для достижения поставленной цели представляется необходимым решить следующие **задачи**:

1. Анализ структурно-функциональных особенностей беспроводных гетерогенных сетей, угроз и атак, направленных на эти сети со стороны конфликтующих сторон в сетевом противоборстве.

2. Формализация стратегий и тактических приемов сетевого противоборства с учетом ценности элементов гетерогенных беспроводных сетей в динамике разрешения конфликта.

3. Формализация понятия и математическое представление гетерогенной беспроводной сети, разработка методологии оценки и регулирования рисков воздействия в ходе сетевого противоборства на гетерогенную беспроводную сеть.

Результаты, выносимые на защиту:

1. Разработанная на основе структурно-функциональной специфики математическая модель гетерогенной беспроводной сети в виде взвешенного графа.

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

3. Модель анализа рисков гетерогенной беспроводной сети и результаты применения данной модели для оценки рисков реализации стратегии устранения элементов гетерогенной беспроводной сети оператора сотовой связи.

Новизна результатов.

1. Разработана модель анализа рисков воздействия на элементы беспроводной гетерогенной сети в результате сетевого противоборства, учитывающая, в отличие от имеющихся аналогов, веса этих элементов и структурно-функциональную специфику сети.

2. Предложены модели сетевого конфликта, выделяющиеся оценкой его глубины, и классифицированные через функции относительной чувствительности ресурса элементов сети.

3. Построена математическая модель стратегии устранения элементов беспроводной гетерогенной сети, и выработаны рекомендации по регулированию риска беспроводных гетерогенных сетей, подвергающихся воздействию в результате сетевого противоборства.

ЗАКЛЮЧЕНИЕ

В результате выполнения работы были получены следующие основные результаты:

1. Произведен анализ структурно-функциональной специфики гетерогенных сетей, в результате которого было выявлено, что она имеет сложную, крупномасштабную, иерархическую структуру, состоящую из следующих уровней: опорная сеть, подсистема базовых станций, уровень пользователей. Элементы нижних уровней имеют высокую степень неоднородности, что и обуславливает гетерогенный характер рассматриваемых сетей. Из-за характерных свойств, ГБС являются уязвимыми к атакам, направленными на устранение её элементов.

2. На основании статистических данных о ГБС ОСС и структурно-функциональной схемы была построена математическая модель ГБС в виде взвешенного графа для пакетной передачи данных и голосовых вызовов. Для дальнейшего риск-анализа была произведена репрезентативная выборка, построены усеченные графы сети.

3. На основе понятий потенциала и ресурса сети, была предложена обобщенная формализация сетевого конфликта, включая измерение его глубины (степени конфликтности) с помощью полуотносительной чувствительности для множеств вершин и дуг. Предложена классификация сетевых конфликтов через функции относительной чувствительности ресурсов сети. Получены аналитические выражения, предназначенные для исследования конфликтных ситуаций в динамике функций относительной чувствительности к изменению параметров сети. На основе двумерных распределений вероятной ресурсной динамики сети построены риск-модели эскалации и деэскалации сетевого конфликта.

4. Предложена классификация стратегий межсетевого противоборства с учетом взвешенности элементов сети, а именно выделены и с помощью графов формализованы схемы реализации следующих стратегий: устранения пользователей сети; нарушения внутрисетевых связей; обесценивания наполнителя сети; обескровливания сети по наполнителю; гибридная стратегия. Предложены и