Таблица 1

Имя блока	**Расположение блока в Simulink library browser**	**Функции блока**
Constant	Simulink/Sources	Вводиться число константа
Gain	Simulink/Math operations	Усилитель сигнала
Display	Simulink/Sinks	Отражает результат в дисплее
Divide	Simulink/Math operations	Деление
Product	Simulink/Math operations	Умножение
Add	Simulink/Math operations	Вводиться “+” и “-”

Таблица 2

Параметр	Результаты по Акрамову А.А. [1]	Результаты Simulink моделирования
1.Дебит скважины линейного водозабора 2.Необходимое количество скважин	562 $м^3/сут$ 18,1 шт	562,9 $м^3/сут$ 17,76 шт

Выводы. Для обоснования проектов ВПВ перспективными является рациональное сочетание нечетко-детерминированных методов моделирования геофильтрации и имитационного моделирования на Simulink при определении параметров ВПВ.

В условиях нарушенного режима подземной гидросферы перспективным для формализация параметров области фильтрации ВПВ является применение принципов теории нечетких множеств.

В процессе НДМ ВПВ важным является установление информационной взаимосвязи между ВПВ (объектов) и её НДМ посредством построения информационной и информационно-технологических моделей. При этом информационная модель является основой для представления и решения обратных задач геофильтрации, а информационно-технологическая модель позволяет эффективно учитывать факторы, влияющие на ВПВ.

Литературы:

1. Акрамов А.А. Регулирование запасов пресных вод в подземных водохранилищах Средней Азии. – Ташкент: ФАН АН РУз. 1991.-216с.

2. Акрамов А.А. Технология искусственного восполнения подземных вод на водозаборах Приаралья. – Ташкент: ГГП «Узбекгидрогеология», 1977.-165с.

3. Гавич И.К. Методы охраны подземных вод от загрязнения и истощения– М.:Недра, 1985. -320 с.

4. Усманов Р.Н. К вопросу интеллектуализации нечеткого управления сложных процессов (на примере водозаборов подземных вод) // Вестник ТУИТ. -2007. - №1. – С.46-49.

5. Усманов Р.Н. К вопросу численного моделирования процессов формирования и эксплуатации водозаборов подземных вод в условиях нечеткой информации // Вестник Таш ГТУ. – Ташкент, 2006.

6. Усманов Р.Н., Сейтназаров К.К. Программный комплекс нечетко-детерминированного моделирования гидрогеологических объектов // Автоматика и программные изменения. 2014, №1(7).-С.29-34

7. Самарский А.А, Михайлов А.П. Математическое моделирование: Идеи. Методы. примеры.2-е изд., испр. - М: Физматлит,2005.-320 с.- ISBN 5-9221-0120-X.

8. Леоненков А.В. Нечеткое моделирование в среде MATLAB и Fuzzy TECH.- СПб.: БХВ - Петербург, 2003.- 736 с., ил.

Усманов Р.Н. д.т.н., профессор, Ташкентского университета информационных технологий имени Мухаммеда Ал-Хорезмий,
e-mail: rishat.tuit@mail.ru
Калимбетов Ж.К. ассистент, Нукусского филиала Ташкентского университета информационных технологий имени Мухаммеда Ал-Хорезмий,
E-mail: j.kalimbetov@umail.uz

Ф.М. Мухтаров

МЕТОДЫ ОТРАЖЕНИЯ ВНЕШНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

В статье анализируются проблемы ведения информационного противоборства, включая определение возможностей для планирования мероприятий по осуществлению или отражению информационного воздействия, а также требуемых направлений для более чётких выявлений основных информационных противоборств.

Ключевые слова: *информационный ресурс, информационное противоборство, угроза, мониторинг, ресурс, киберпреступления.*

I. Введение

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс является сегодня одним из главных источников экономической и военной мощи государства.

К началу 90-х гг. произошли качественные изменения в военно-политической и научно-технической сферах, заставившие во многом пересмотреть государственную политику в области защиты информации в целом.

Во-первых, информационные технологии принципиально изменили объем и важность информации, обращающейся в технических средствах ее передачи и обработки. Во-вторых, в РУз отошла в прошлое фактическая государственная монополия на информационные ресурсы, в частности получило конституционное закрепление право гражданина искать, получать и распространять информацию. В-третьих, прежний административный механизм управления защитой информации стал неэффективен, в то же время необходимость межведомственной координации в этой сфере объективно возросла. В-четвертых, в связи с усиливающимся включением РУз в международное разделение труда, укреплением экономических, культурных, гуманитарных контактов с другими государствами многие режимно-ограничительные меры, облегчающие защиту информации, например, система регионов, закрытых для посещения иностранными гражданами, стали неприемлемы.

II. Основная часть.

Методы и способы ведения шпионажа остаются неизменными на протяжении многих столетий развития общества и государства. При этом меняются только средства и формы его ведения.

Ведущие страны продолжают модернизировать и развивать свои разведывательные службы, совершенствовать техническую разведку, наращивать ее возможности.

С учётом рассмотренного содержания понятия угрозы государству, обществу и личности в широком смысле рассмотрим угрозы, непосредственно воздействующие на обрабатываемую конфиденциальную информацию. Система угроз безопасности представляет собой реальные или потенциально возможные действия или условия, приводящие к хищению, искажению, несанкционированному доступу, копированию, модификации, изменению, уничтожению конфиденциальной информации и сведений о самой системе и, соответственно, к прямым материальным убыткам.

Проявление угроз характеризуется рядом закономерностей. Во-первых, незаконным овладением конфиденциальной информацией, ее копированием, модификацией, уничтожением в интересах злоумышленников, с целью нанесения ущерба. Кроме этого, непреднамеренные действия обслуживающего персонала и пользователей также приводят к нанесению определённого ущерба. Во-вторых, основными путями реализации угроз информации и безопасности информации выступают:

– агентурные источники в органах управления и защиты информации;

– вербовка должностных лиц органов управления, организаций, предприятий и т. д.;

– перехват и несанкционированный доступ к информации с использованием технических средств разведки;

– использование преднамеренного программно-математического воздействия;

– подслушивание конфиденциальных переговоров в служебных помещениях, транспорте и других местах их ведения.

Концепция национальной безопасности не даёт определения угрозы, но называет некоторые из них в информационной сфере. Так, опасность представляют:

– стремление ряда стран к доминированию в мировом информационном пространстве;

– вытеснение государства с внутреннего и внешнего информационного рынков;

– разработка рядом государств концепции информационных войн;

– нарушение нормального функционирования информационных систем;

– нарушение сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Информационно-технический прогресс в военном деле обеспечил условия для ускоренного совершенствования вооружения и военной техники на основе широкого внедрения новых информационных технологий и создания информационного оружия. Интеллектуализация способствовала кардинальному увеличению точности, дальности и мощности действия классических видов вооружений, резкому увеличению возможностей разведки, систем сбора и обработки информации и, как следствие, уменьшению времени принятия оперативных решений. Внедрение сетевых технологий в военном деле принципиально изменяет военную стратегию и тактику, военное искусство. В этих условиях информационное оружие может стать тем самым искомым эффективным силовым средством, не предусматривающим разрушения объектов и уничтожения живой силы и населения противника, позволяющим решать многие конфликты без применения традиционных средств вооружённой борьбы, подчинять себе противника, его экономические и трудовые ресурсы без применения силовых методов.
Страны, обладающие таким оружием и военной техникой, получают громадное военное преимущество перед противником, оснащённым традиционными типами вооружений.

Многие аналитические центры в мире ведут проработку возможных сценариев информационных войн, исходя в своих стратегиях из задачи обеспечения информационного доминирования. Обобщение их результатов создаёт следующую схему.

*Первый сценарий. Государство - потенциаль-

ный инициатор информационной войны - располагает подавляющим превосходством в наступательном информационном оружии и способно преодолеть соответствующие оборонительные системы любой другой страны. В этом случае оно может выделить часть имеющихся у него средств ведения информационной войны своим союзникам, взяв на себя задачи координации совместных действий, а также идентификацию информационных угроз, откуда бы они ни исходили. При этом, однако, должна существовать гарантия того, что само это государство не будет разоблачено в качестве “информационного агрессора”.

*Второй сценарий. Допускается наличие некоторого ограниченного числа государств, обладающих информационным оружием, достаточным для проведения самостоятельных информопераций. При этом одно данное государство сохраняет своё превосходство в указанной области. Это обстоятельство должно сыграть роль фактора устрашения и удержать остальные страны от использования информационного оружия против доминирующего государства и обеспечить его “исключительность” и в дальнейшем.

Это вынудит большинство стран мира отказаться от создания его наступательных видов. В то же время они не смогут противостоять информационным атакам на себя, так как не обладают адекватными защитными технологиями. В такой ситуации инфолидер может навязать им свою систему принудительного контроля над информационным оружием.

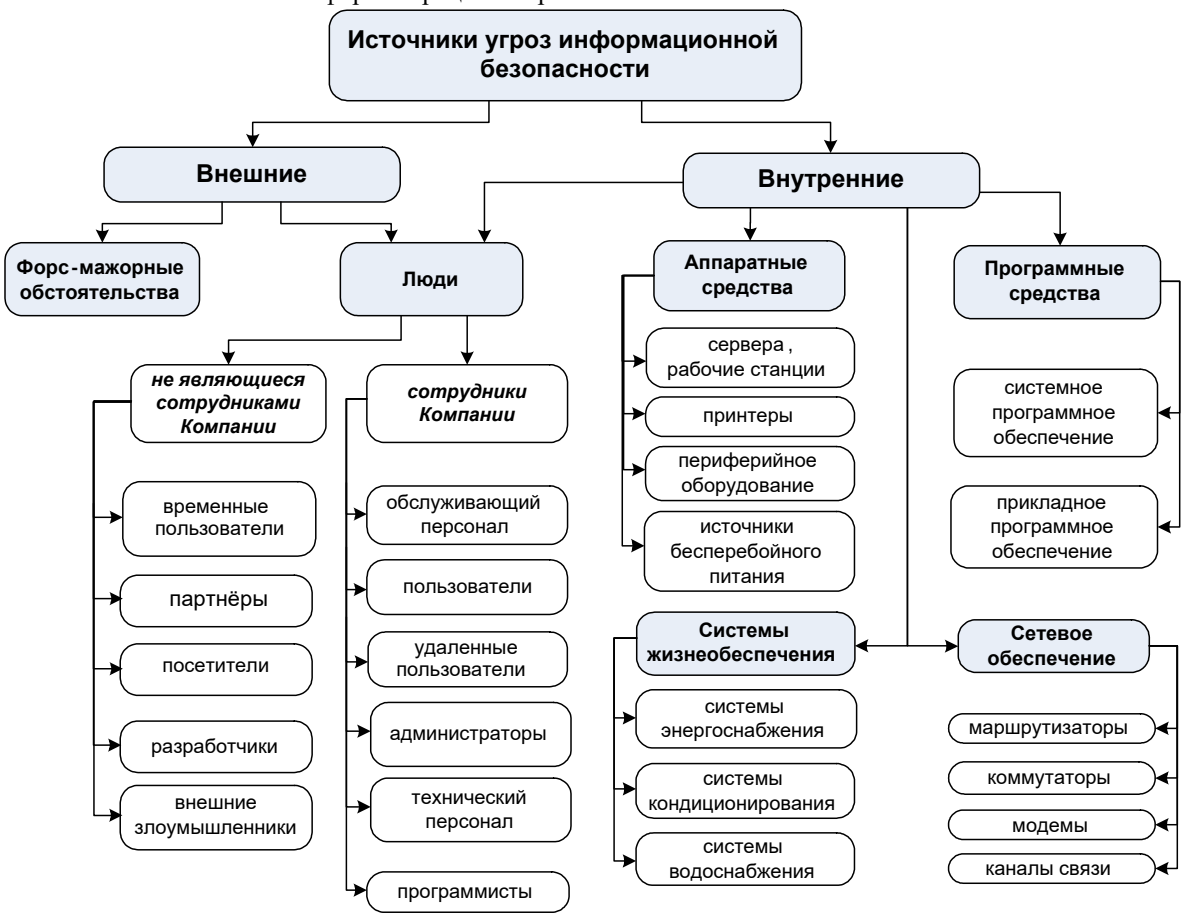

Рис.1. Источники угроз информационной безопасности ИС

Доминирование в информационной сфере реально означает не абстрактную возможность влиять на мировую инфосферу, а обладание вполне конкретным потенциалом, позволяющим диктовать свою волю, то есть обеспечить глобальное доминирование.

Анализ проблемы ведения информационного противоборства, включая определение возможностей для планирования мероприятий по осуществлению или отражению информационного воздействия, требует более чёткого выявления основных направлений информационного противоборства. Можно выделить восемь таких направлений:

1, Борьба с системами управления. Борьба с системами управления в контексте информационного противоборства может быть определена как военная стратегия (в рамках информационных операций при проведении военных действий), предусматривающая физическое уничтожение таких систем и отсечение командных структур вооружённых сил противника от управляемых частей с целью воспрепятствовать стабильному процессу боевого управления и руководства.

Такого рода борьба с системами управления мо-

жет достигаться как непосредственным уничтожением управляющих структур (так называемое «обезглавливание»), так и разрушением коммуникаций, связывающих системы управления с подчинёнными подразделениями («удушение»). Выбор метода борьбы во многом определяется поставленными тактическими и стратегическими целями.

Особая значимость информационных операций против систем управления состоит в том, что они могут оказаться особенно эффективными на ранних стадиях развития конфликта и, кроме того, создают предпосылки для достижения бескровной победы над противником. Однако эти «преимущества» могут быть в значительной степени нивелированы противником путём децентрализации командных систем, а также посредством ведения им так называемой «сетевой войны».

2. Информационно-разведывательные операции. Концепция ведения информационно-разведывательных операций в определённом смысле является развитием концепции оперативной разведки, хотя между ними наблюдаются и существенные различия, связанные с тем, что получаемые в ходе информационно-разведывательных операций сведения (например, данные целеуказания или сведения о нанесённом ущербе) поступают непосредственно участникам операции, вплоть до исполнительного уровня (реализация концепции «цифрового поля боя»), в то время как обычно данные военной разведки направляются в командные центры, где они суммируются, обрабатываются и затем в качестве приказов и вводных доводится до подчинённых. По сути дела, речь идёт об адаптации оперативной разведки к децентрализованной системе боевого управления и ведения боевых действий, требующей внесения значительных корректив в архитектуру и идеологию сбора, обработки и распределения разведывательной информации.

Новые децентрализованные автоматические и автоматизированные системы, призванные решать конкретные задачи в ходе информационно-разведывательных операций, сами по себе являются потенциальными объектами рассмотренной выше борьбы с системами управления. В этой связи представляется целесообразным рассматривать два аспекта таких операций: первый, условно называемый «наступательным», обеспечивает сбор разведывательной информации о противнике, а второй, «оборонительный» или «защитный» – связан с защитой собственной информации и противодействием информационно-разведывательным операциям противника.

3. Электронная борьба. Прежде всего, следует отметить, что первые два рассмотренные выше направления информационного противоборства по сути дела представляют собой либо борьбу с информационными системами, либо борьбу при помощи информационных систем. В отличии от них, целью электронной борьбы, как прикладного метода ведения информационного противоборства, является снижение информационных возможностей противника, в соответствии с чем она подразделяется на радиоэлектронную борьбу (РЭБ), криптографическую борьбу (искажение и ликвидация собственно информации) и борьбу с коммуникационными системами противника.

4. Психологическая борьба. В тех случаях, когда использование методов информационного противоборства направлено не против информационных систем противника, а непосредственно против человеческого разума и психики, речь идёт о психологической борьбе. В самом общем виде психологическую борьбу можно определить, как манипулирование общественным сознанием, общественным мнением на различных социальных уровнях. На Западе принято выделять следующие основные категории информационно-психологических операций, проводимых в рамках психологической борьбы:

- операции, направленные против структур государственного управления;
- операции, направленные против структур военного командования;
- операции по деморализации личного состава вооруженных сил.

5. *«Хакерская» борьба.* Понятие хакерской борьбы сводится главным образом к осуществлению «атак» на различные компоненты компьютерных сетей и хранящиеся в них информационные ресурсы. Основной особенностью хакерских «атак» является то, что они носят не аппаратный, а программный характер. Некоторые западные аналитики склонны даже считать, что информационное противодействие в целом должно быть сведено исключительно к хакерской борьбе.

Наиболее популярными из используемых в настоящее время средств являются так называемые компьютерные вирусы, «черви», «троянские кони», логические бомбы, «дыры» в системе, прошивка постоянного запоминающего устройства. Перечисленные средства могут рассматриваться как образцы информационного оружия, реализованного в форме вредоносных программ (так называемое, информационное оружие на основе программного кода).

6. *«Кибернетическая» и «сетевая» борьба.* Концепции «кибернетической» и «сетевой борьбы», несмотря на вполне «техническое» русское звучание, в наименьшей степени связаны с собственно с информационными технологиями и охватывают полный комплекс проблем и аспектов информационного противоборства (организационные, доктринальные, стратегические, тактические и технические стороны ведения наступательных и оборонительных информационных операций).

Так, концепция кибернетической борьбы, относящаяся к информационно-ориентированным военным операциям, в настоящее время становится все более актуальной именно в военной сфере, особенно когда речь идёт о конфликтах высокой интенсивности. Кибернетическая борьба нашла своё отражение также в более широкой концепции «революции в

военном деле» – использования новых технологий и, что особенно важно, осуществления организационных и управленческих изменений в военной области.

С другой стороны, роль сетевой борьбы возрастает в конфликтах низкой интенсивности и при проведении так называемых «операций, отличных от войны», а также в конфликтах, террористических действиях и иных преступлениях, носящих невоенный характер. При этом понятие сетевой борьбы относится скорее к организационной форме противоборства, использующей информационные возможности, чем собственно к борьбе с информационными инфраструктурами противника. Более того, концепция сетевой борьбы подразумевает использование информационных инфраструктур противника в своих целях.

7. *Экономическая информационная борьба.*

В последние годы возрастает озабоченность возможностью использования методов и средств информационной войны в экономической сфере, в связи с чем западные специалисты выделяют две основные формы экономического информационного противоборства: информационную блокаду и информационный империализм.

Информационная блокада. В условиях глобализации и развития неденежной экономики информационная экономическая блокада становится крайне гибким и эффективным методом воздействия на потенциального противника. В отличие от введения эмбарго на тот или иной вид товаров или других экономических санкций, информационная блокада может носить скрытый характер, а соответствующие информационные операции могут быть завуалированы под случайные сбои информационных систем или случайные хакерские проникновения компьютерных хулиганов. При этом, естественно, не снимается возможность и открытого государственного давления в этой области.

Информационный империализм. Глобализация мировых экономических процессов обеспечивается постоянно ускоряющимся развитием современных информационных технологий, поэтому не удивительно, что наиболее приспособленными к эффективной экономической деятельности в новых условиях оказались технологически развитые государства, среди которых бесспорным лидером выступают США. Не является секретом, что разработка основных компонентов компьютерной техники и общего программного обеспечения сосредоточена, прежде всего, в этой стране. Это предоставляет принципиальную возможность подчинить своим интересам деятельность структур, определяющих функционирование мировых информационно-коммуникационных систем.

8. *Международный информационный терроризм.* Сам по себе терроризм не может быть отнесён к противоборству (исключением является государственный терроризм). Однако в своей международной форме и в связи с трансформацией терроризма в сторону использования современных высокотехнологичных средств воздействия террористические организации могут выступать как самостоятельные субъекты международной политики, не являясь при этом, естественно, субъектами международного права. Кроме того, в связи с быстрым развитием информационных технологий проблема международного терроризма приобретает в условиях информационного противостояния новое звучание. Это связано, прежде всего, с двумя аспектами: с использованием террористами информационной инфраструктуры для развития так называемых сетевых способов собственной организации, а также с собственно террористическим воздействием на объекты информационных инфраструктур.

По мнению многих экспертов, террористические организации, независимо от мотивации их действий, постепенно трансформируются от первоначальной иерархической структуры к информационно-ориентированной сетевой организации. Внутри групп личностное влияние лидера все больше уступает место упрощённой децентрализованной системе. Разрозненные группы все чаще сливаются в транснациональные террористические сообщества.

III. Заключение

Наряду с сохранением принципов воздействия на объекты, разрушение которых может повлечь за собой значительные жертвы у населения и вызвать значительный политический и общественный резонанс, происходит трансформация взглядов на террористическую борьбу как на непосредственное средство достижения цели. Систематическое нарушение работоспособности информационных инфраструктур оказывается даже более эффективным, чем «точечные» террористические воздействия.

Не связанные инертностью развития государственных институтов террористические организации, как правило, значительно быстрее берут на вооружение перспективные информационные технологии, используемые ими как для проведения непосредственных террористических операций, так и для поддержки внутренней организации и координации действий. Многие аналитики даже склонны считать неверными спекулятивные рассуждения о том, что террористы будут предпринимать попытки нарушить работоспособность информационных сетей в целом. Они, по-видимому, будут больше заинтересованы в сохранении работоспособности таких сетей, что позволит им лучше и оперативное координировать свои действия, а также (о чем свидетельствует опыт работы в сети интернет) маскировать такие действия и пропагандировать свои взгляды.

И, наконец, следует учитывать возможность того, что государства, проводящие информационные операции, будут маскировать свои действия под террористическую деятельность некоторых известных или неизвестных групп. В этой связи наряду с проблемами поиска стратегии защиты от террористического воздействия все большую остроту приобретают задачи идентификации противника в информационном пространстве и адекватного реаги-

рования на возникающие вызовы.

Литературы:

1. Мухтаров Ф.М. «Концептуальные подходы совершенствования национального законадательства в сфере обеспечения информационной безопасности», World social science, Scientific – practical journal №1, p. 64-69, 2018 y..

2. Мухтаров Ф.М. «Методы защиты национальной безопасности от внешних и внутренних информационных угроз», Ташкент, ТУИТ «Мухаммад ал-Хоразмий авлодлари» илмий-амалий ва ахборот-тахлилий журнали 2017 й. №2-сон, 18-24 бетлар.

3. Мухтаров Ф.М. «Методы реализации информационных ресурсов в информационном обществе», «Инфокоммуникации: Сети – Технологии - Решения» научно - технической журнал , г.Ташкент 2018 г. 45-том №1, стр. 55-61.

4. Мухтаров Ф.М. «Обеспечение информационной безопасности государственных тайн в информационной среде» Вестник ТашГТУ №1, г.Ташкент 2018 г., стр. 40-45.

5. Мухтаров Ф.М. «Выбор приоритетных факторов концептуальной модели государственной информационной безопасности» International journal of innovative technologies in social science. 4(8)Volume 3, p. 89-94, Warsaw Poland, June 2018 y.

6. “Ахборот хавфсизлигини таъминлашнинг сиёсий масалалари” – Идоравий журнал 2016 йил.

УДК 004.421:519.178

О.Т.Алламов, А.Т.Бабажанова

КЎП ПАРАМЕТРЛИ ГРАФ ҚИРРАЛАРИНИ ТАЪСИР КОЭФФИЦИЕНТИНИ ТОПИШ АЛГОРИТМИ

Мақолада статик кўп параметрли графнинг қирралари учун умумий таъсир коэфффициентини топиш учун алгоритм келтирилган. Графнинг статик параметрларни баъзилари маршрут танланишида максимал бўлишини ва баъзилари минимал бўлиши қирранинг умумий таъсир коэффициентини топишда инобатга олинган. Таъсир коэффициенти орқали графда тугунлараро маршрутларни энг кам харажат билан топиш мумкин.

Калит сўзлар: кўп параметрли граф, графда умумий таъсир коэффициентини топиш, кўп параметрли графнинг берилиши.

Маршрутизация масаласи ёки энг қисқа йўлни топиш муаммоси манбаларда комбинатористиканинг оптималлаш масаласи сифатида жуда кўп ўрганилган[1]. Маршрутизация масаласи ва энг қисқа йўл топиш масалалари тушунчалари бир-бирига жуда яқин тушунчалар бўлиб, маршрутизация масаласида бир жойдан бошқа жойга боришда фақат йўл минимум бўлиши етарли эмас, бошқа параметрларни ҳам инобатга олиб ечиш назарда тутилса, энг қисқа йўлни топишда йўлнинг узунлигини инобатга олиб масалани ечиш талаб этилади[2]. Аммо, энг қисқа йўлни топиш масаласи маршрутизатция масаласининг хусусий ҳоли ҳисобланади ва маршрутизатция масалаларини ушбу масалани ечимлари ёрдамида мукаммал ечимларини топишда фойдаланиш мумкин. Энг қисқа йўлларни топиш масаласи жуда кўп масалларни қисм масаласи сифатида кенг қўлланилади.

Мақолада кўп параметрли графда энг мақбул маршрутларни топишда фойдаланиладаиган қирраларнинг умумий таъсир коэффициентини топиш алгоритми ишлаб чиқиш тадқиқ этилган[5,7,8]. Кўп параметрли графда энг мақбул ечимни топиш учун қурилган мақсад функцияси айрим параметрлари бўйича максималлаштириш ва баъзилари бўйича минималлаштириш масалалари қаралади ҳамда улар биргаликда тадқиқ этилади[9,10].

Бошланғич тушунча ва таърифлар

Фараз қилайлик кўп параметрли G=(V,E) граф берилган бўлсин [3,4]. Бунда

$$V=(v_1,v_2,v_3,...,v_n),\quad \overline{1\le i\le n} \tag{1}$$

v_i графдаги і тугунни билдиради.

$$E=(e_1,e_2,e_3,...,e_m),\quad \overline{1\le \mathrm{i}\le \mathrm{m}} \tag{2}$$

Бу ерда e_i - і қиррани билдириб, иккита ўзаро боғланган х ва у тугунлардан ташкил топган.

$$e_i=(x,y),\quad 1\le i\le m,\quad x\in V,\quad y\in V \tag{3}$$

Келтирилган (3) ифодадаги қирра e_i иккита элементдан ташкил топган бўлиб, x қирранинг бошланғич тугуни y эса, қирранинг тугалланувчи тугуни ҳисобланади.

Тугунлараро статик параметрларни ифодалаш учун С-матрица берилган.

$$C=\{c_{ij}\}_{m\times u} \tag{4}$$

Берилган (4) матрицанинг i қатор элементлари e_i қирранинг статик параметрларини ифодалайди. Статик параметрлар сони u га тенг.

Бундан ташқари u ўлчовли

$$\sigma=(\sigma_1,\sigma_2,\sigma_3,...,\sigma_u) \tag{5}$$

Буль вектор берилган бўлсин. Буль вектор компоненталари 0 ва 1 қийматлардан ташкил топган бўлиб, статик параметрлар бўйича қайси устунлар максималлаштирилишини (агар $\sigma_i=1$ бўлса і устун $\rightarrow$ max) ва аксича бўлса, қайси устунлар