СОВРЕМЕННЫЕ ТЕНДЕНЦИИ СТРУКТУРНО-ЛОГИЧЕСКОГО АНАЛИЗА НАДЕЖНОСТИ И КИБЕРБЕЗОПАСНОСТИ АСУТП.

МОЖАЕВА И.А., НОЗИК А.А., СТРУКОВ А.В.
АО «СПИК СЗМА», С-Петербург, E-mail: info@szma.com
ЧЕЧУЛИН А.А.
ФГБУН СПИИРАН, С-Петербург, E-mail: chechulin@comsec.spb.ru

Аннотация.
На основе современной концепции надежности информационных систем представлены основные тенденции развития структурно-логического анализа надежности и безопасности автоматизированных систем управления технологическими процессами (АСУТП). Показано, что одно из направлений развития связано с разработкой так называемых динамических деревьев неисправностей, в которых реализованы дополнительные логические операторы. Другое направление связано с расширением формализма деревьев неисправностей и деревьев событий путем их конвертации в сети Петри и Байесовские вероятностные сети. Развивается также направление, связанное с разработкой деревьев атак. Показаны примеры решения задач с использованием ПК АРБИТР.

Ключевые слова: Надежность, кибербезопасность, оценка риска и безопасности, дерево неисправностей, дерево событий, ПК АРБИТР.

Введение

Автоматизированные системы (АС) как системы, состоящие из персонала и комплекса средств автоматизации его деятельности, реализующие информационную технологию выполнения установленных функций, являются объектом повышенного внимания в области кибербезопасности. На конференции, организованной Координационным Центром НАТО по реагированию на компьютерные инциденты (Таллин, 2014г.) говорилось о смещении центра внимания кибератак в сторону автоматизированных систем управления ответственных и опасных производственных процессов. Поэтому современный подход к анализу надежности АС, широкий класс которых представляют автоматизированные системы управления технологическими процессами (АСУТП), должен учитывать тот факт, что атрибутами надежности таких систем следует считать не только безотказность, ремонтопригодность и готовность, но и безопасность, конфиденциальность и целостность [1].

Расширенное понятие надежности (dependability – надежный, заслуживающий доверие) базируется на понимании того, что кроме феноменологических причин возникновения неисправностей в аппаратной части (естественные отказы элементов, человеческие ошибки) возможны неисправности программного обеспечения, вызванные преднамеренными вредоносными действиями. То есть неисправности возможны не только в домене физическом, но и в домене информационном. Поэтому понятие надежности современных АСУТП должно развиваться от понятий безотказности/готовности к понятиям безопасность/конфиденциальность, целостность вместе с технологическими и программными разработками автоматики, сетевой и компьютерной техники для того, чтобы адекватно реагировать на возникающие проблемы.

Эксперты компании Positive Technologies в отчете о безопасности промышленных систем управления в 2012г. [2] отмечают, что АСУТП все чаще становятся целью для кибератак, причем угрозы развиваются быстрее, чем защита.

Традиционная парадигма информационной безопасности АСУТП строится вокруг таких понятий, как конфиденциальность, целостность и доступность (готовность). Новый подход включает в себя анализ последствий кибератак с учетом их влияния на промышленную безопасность и количественные экономические показатели. Будем называть такой подход к анализу кибербезопасности АСУТП функциональным и риск-ориентированным. Такой подход предполагает решение задач оценивания не только успешности/неуспешности самой кибератаки, но и сохранения устойчивого функционирования АСУТП и объекта управления (ОУ) путем их адаптации к результатам кибервторжения (несанкционированного проникновения).

Обычно процесс адаптации включает в себя следующие этапы:

a) диагностика неисправности, ее обнаружение и идентификация;

b) изоляция неисправности, которая производит физическое или логическое удаление неисправных компонент из дальнейшего участия в работе;

c) системная реконфигурация, которая коммутирует резервные элементы или переназначает задачи среди не отказавших элементов;

d) системная реинициализация (повторная инициализация), которая проверяет, обновляет и записывает новую конфигурацию и обновляет системные таблицы и записи.

Следовательно, на двух последних этапах требуется оперативное решение задач оценивания показателей надежности измененной структуры АСУТП и риска снижения производительности ОУ, потому что зачастую невозможно предотвратить угрозу или устранить последствия атак без потери качества функционирования. Для полного анализа надежности и безопасности всей системы (АСУТП и ОУ) необходимо рассматривать ее поведение в физическом пространстве и поведение информационной инфраструктуры в киберпространстве, что соответствует задачам анализа многоагентных систем.

В этой связи обосновано использование терминов «отказобезопасность», «атакоустойчивость» и «функциональная устойчивость к кибератакам». Термин «отказобезопасность», относящийся к способности системы в случае отказа некоторых ее элементов переходить в безопасное для людей , окружающей среды или материальных ценностей состояние, может рассматриваться совместно с термином «отказоустойчивость». Свойство «отказобезопасность» может быть количественно оценено, например, вероятностью перехода/неперехода в опасное состояние в результате проведения кибератаки.

В Руководстве по безопасности «Методические основы по проведению анализа опасностей и оценки риска аварий опасных производственных объектов», утвержденном приказом Ростехнадзора от 13 мая 2015 №188, прямо записано, что «…При анализе опасностей, связанных с отказами технических устройств, систем обнаружения утечек, автоматизированных систем управления технологическим процессом (АСУТП), систем противоаварийной защиты выделяют технический риск, показатели которого определяются соответствующими методами теории надежности технологических систем и функциональной безопасности систем противоаварийной автоматической защиты, систем управления технологическим процессом в соответствии с серией ГОСТ Р МЭК 61508/61511…» [3]. Далее в этом документе приводится обоснование необходимости и целесообразности использовании математического и методического аппарата теории надежности при решении задач анализа безопасности опасных производственных объектов.

Важным и в настоящее время активно развивающимся элементом методического аппарата анализа надежности и моделирования угроз является структурно-логический метод. Суть метода состоит в том, что система как некоторая структура описывается как топология взаимосвязанных элементов (оборудование, материалы, программное обеспечение, персонал), которые однозначно определяют состояния системы. Взаимосвязи элементов описываются функциями алгебры логики (ФАЛ). Также с помощью ФАЛ при построении вероятностных и детерминированных структурно-логических моделей формируются критерии нахождения исследуемой системы в безопасных, предопасных (критичных) и опасных (аварийных) состояниях. Получение количественных показателей надежности и безопасности осуществляется по правилам перехода от логической функции в виде минимальной дизъюнктивной нормальной формы (ДНФ) к функциям полного замещения логических переменных на вероятностные или детерминированные характеристики, а логических действий - на алгебраические.

Универсальной графической интерпретацией структурно-логического метода являются схемы функциональной целостности (СФЦ), позволяющие использовать методики построения блок-схем, деревьев неисправностей, деревьев событий, а также методику «галстук-бабочка» [3,7], совмещающую на одном экранном интерфейсе перечисленные выше графические методики [1]. Методические документы, разработанные Международной морской организацией (ИМО) для проведения количественного анализа риска, используют термин RCT (Risk Contribution Trees) – объединенные деревья неисправностей и событий для анализа рисковых последствий [5].

Кроме графического расширения возможностей структурно-логического моделирования ведутся исследования в направлении снятия таких ограничений, как бинарность событий. В частности, разработана алгебра групп несовместных событий (ГНС) в рамках общего логико-вероятностного метода [6]. Разработка алгебры ГНС позволяет моделировать надежность системы, элементы которых могут находиться в нескольких состояниях. При этом события ГНС нельзя считать независимыми.

В отличие от консервативного характера использования метода структурных блок-схем, метод анализа деревьев неисправностей (ДН) развивается по двум направлениям. Первое связано с

увеличением номенклатуры логических операторов (гейтов). В настоящее время программы анализа ДН имеют в своем составе не только традиционные гейты OR (ИЛИ), AND (И), NOT (НЕ), XOR (Исключающее ИЛИ), VOTE (К из N), но и такие гейты, которые образуют новый класс ДН, получившие название динамических деревьев неисправностей (ДДН) [8]. ДДН имеют в своем составе такие специальные гейты, как PAND (приоритетное И), SEQ (учет последовательности наступления событий), SPARE (ненагруженное резервирование), FDEP (учет функциональной зависимости), PDEP (учет вероятностной зависимости). Введение новых гейтов расширяет, в частности, возможности моделирования надежности и безопасности систем с сильной зависимостью между элементами.

Второе направление связано с разработкой так называемых обобщенных деревьев неисправностей (ОДН), которые приспособлены для сопряжения или конвертации в Байесовские сети, сети Петри. Это связано с тем, что за последние 10-15 лет Байесовские сети получили широкое применение для представления неопределенностей знаний в системах искусственного интеллекта. Байесовские сети имеют такое преимущество, как наглядное графическое представление условных независимых высказываний и компактный способ представления совместного распределения случайных величин, например, в виде таблицы условных вероятностей [9,10].

Расширение методов структурно-вероятностного моделирования путем использования дополнительного формализма Байесовский сетей и сетей Петри в настоящее время имеет, в основном, научно-исследовательский характер. Получение практических результатов, которые могут быть непосредственно использованы в инженерной практике проектирования и эксплуатации таких сложных технических систем, какими являются АСУТП, встречается крайне редко. По-прежнему более простые методы логико-вероятностного анализа (структурные схемы, деревья неисправностей и деревья событий) востребованы в инженерной практике. Стимулирующим фактором такой востребованности является разработка соответствующего программного обеспечения автоматического структурно-логического моделирования надежности и безопасности структурно-сложных систем.

На рис.1 приведен фрагмент экранного интерфейса ПК АРБИТР [4], иллюстрирующий графическое представление опасного события [3] и связанных с ним событий с помощью схемы функциональной целостности (СФЦ), позволяющей реализовывать алгоритмы анализа дерева неисправностей и дерева событий в рамках единого интерфейса. В левой части схемы построено дерево неисправностей, модель которого описывает последовательность отказов и причин, приводящих к опасному событию. Для этих целей также может быть использован метод структурных схем надежности. Вершинное событие этой части схемы (обозначено треугольником) является характеризуется рассчитанным значением вероятности (частоты) опасного события (реализации) события.

В правой части схемы построено дерево событий, модель которого описывает последовательность событий и отказов, приводящих к эскалации опасного события. В правой части СФЦ получена модель 8 сценариев развития аварии (эскалации). Каждому сценарию (фиктивные вершины №№34-41) приписана мера последствий (Столбец «Ущерб» в правой части экрана). По формуле, например, взвешенного среднего может быть получена оценка ***Wr*** ущерба для исследуемой опасности.

На рис.2 приведен фрагмент экранного интерфейса ПК АРБИТР [4], иллюстрирующий взаимосвязь барьеров безопасности с методами анализа риска [3]. В левой части создана модель источника риска в виде совокупности трех причин, приводящих к опасному состоянию. В системе могут применяться предупреждающие меры (барьеры безопасности), уменьшающие влияния причин на вероятность реализации опасного состоянии (функциональные вершины №№ 4, 6-10 со светлой заливкой). Оператор «Контроль эскалации» (функциональная вершины №5 с серой заливкой) может быть использован для анализа чувствительности мер безопасности, уменьшая или увеличивая влияние соответствующей причины на вероятность реализации опасного состоянии (треугольник №20).

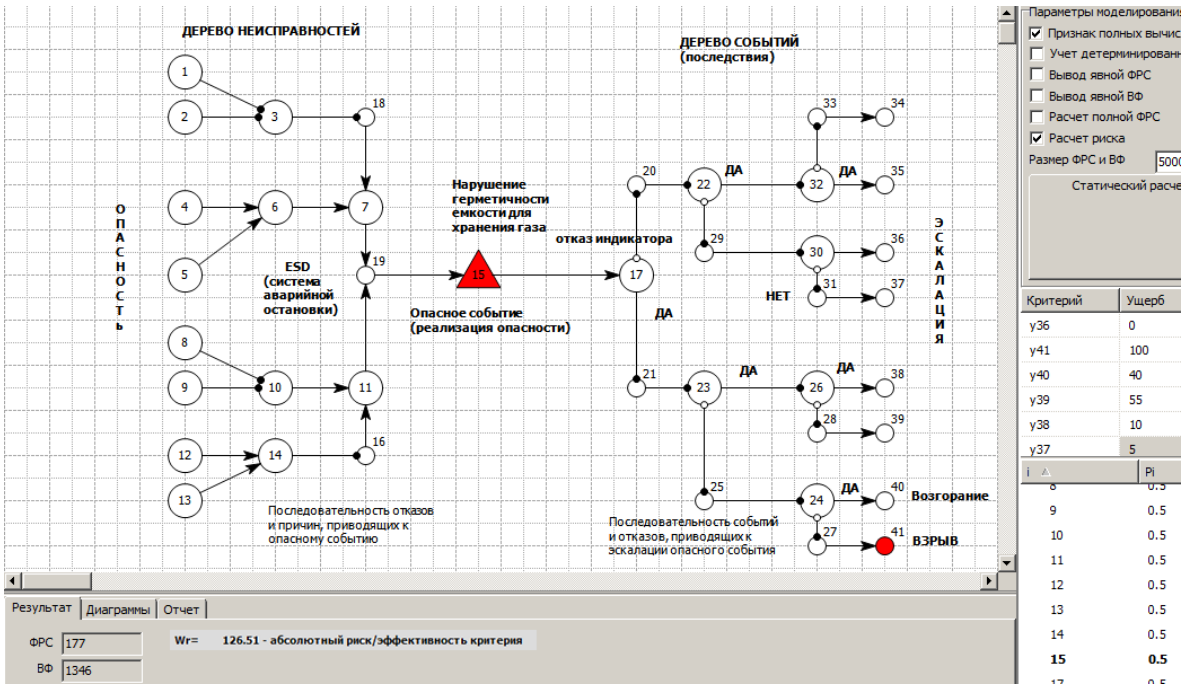

Рисунок 1 – Совместное применение методов анализа деревьев неисправностей и деревьев событий

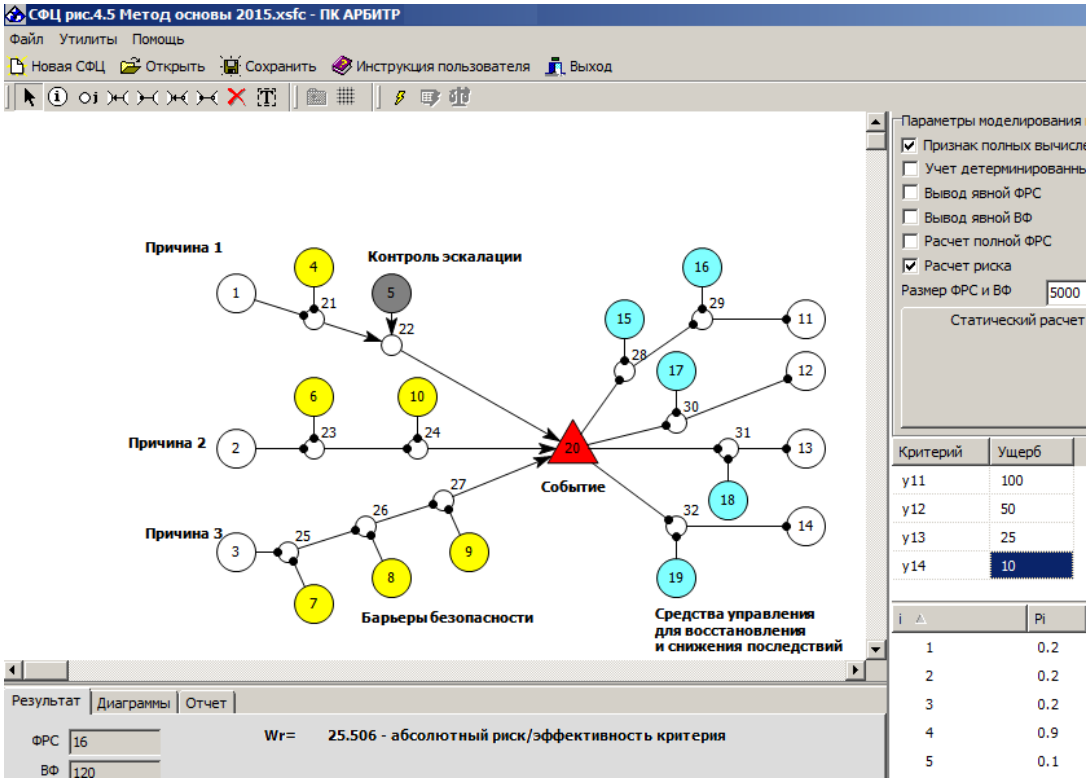

Рисунок 2 – Взаимосвязь барьеров безопасности с методами анализа риска

Несколько иной тенденцией развития компьютерных методов структурно-логического анализа кибербезопасности технических систем является использование технологии деревьев атак (ДА) для описания потенциальных угроз и способов атак, реализующие эти угрозы. ДА представляют собой мультиуровневые диаграммы, состоящие из одного корня, листьев и потомков. Для построения ДА используют булевы выражения для описания условий, при которых дочерние узлы обеспечивают реализацию родительских узлов. Наиболее часто при этом используют сокращенный набор логических операторов (гейтов), ограничиваясь операторами «ИЛИ», «И», « К из N». В то же время событию ДА могут быть приписаны не только вероятностные характеристики, но и детерминированные (стоимость, объем оборудования и т.д.).

В этом случае пользователь может задавать арифметические действия, которые должны выполняться над детерминированными характеристиками событий. Например, при представлении логической функции вершинного события в виде ДНФ могут определяться действия над детерминированными характеристиками событий в конъюнкциях (сложение, нахождение минимума/максимума) и над детерминированными характеристиками конъюнкций в дизъюнкции.

Компьютерная реализация метода ДА может быть реализована, в частности, сокращением функциональных возможностей программы, предназначенной для анализа надежности сложных систем. Примером такой реализации можно назвать программу AttackTree компании Isograph [11].

На рис.3 приведен фрагмент экранного интерфейса ПК АРБИТР [4], иллюстрирующий построение ДА для Web-доступной АСУТП [12] с использованием эквивалентированных вершин (обозначены треугольниками), внутри которых могут быть реализованы алгоритмы получения количественных мер оценки не только вероятности реализации угрозы, но и детерминированных характеристик уязвимости, стоимости атаки и т.д. [13].

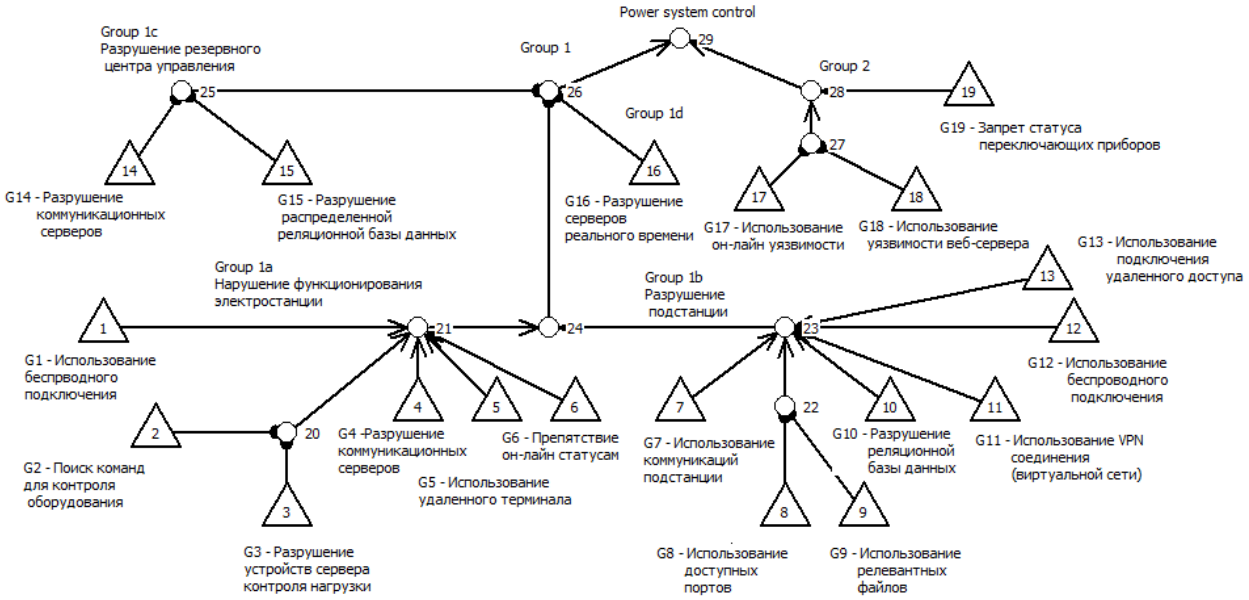

Рисунок 3 –Дерево атак для Web-доступной АСУТП

Заключение

Риск-ориентированный подход к анализу надежности и кибербезопасности современных АСУТП предполагает использование математического и методического аппарата структурно-логического моделирования для оценки как вероятностных, так и детерминированных характеристик не только самой АСУТП, но и объекта управления. Для полного анализа надежности и безопасности всей системы (АСУТП и ОУ) необходимо рассматривать ее поведение в физическом пространстве и поведение информационной инфраструктуры в киберпространстве. Как указано в Руководстве «Методические основы по проведению анализа опасностей и оценки риска аварий опасных производственных объектов» для решения задач анализа риска следует использовать математический и методический аппарат теории надежности как научной дисциплины, «… в которой разрабатываются и изучаются методы обеспечения эффективности работы объектов…» [3]. Методы структурно-логического анализа надежности сложных систем и процессов, получившие широкое применение в виде компьютерных программ анализа структурных схем надежности, деревьев неисправностей и деревьев событий, развиваются как в направлении создания обобщенных и смешанных деревьев, так и в направлении конвертации в сети Петри и Байесовские сети. Определенную нишу в области анализа кибербезопасности занимают деревья атак. Кроме оценок последствий атак актуальной является также задача метрической оценки уязвимостей АСУТП и их влияния на эффективность работы объекта управления при изменении конфигурации информационной инфраструктуры.

ССЫЛКИ

1. A.Avizienis, J.-C. Laprie , B. Randell," Fundamental Concepts of Dependability," *Research Report No 1145, LAAS-CNRS,* pp 1-6

2. URL: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (Дата обращения 8.10.2015)

3. Методические основы по проведению анализа опасностей и оценки риска аварий опасных производственных объектов. Приказ Ростехнадзора от 13 мая 2015 №188.

4. АРБИТР. Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности АСУТП на стадии проектирования (ПК АСМ СЗМА). Автор: Можаев А.С. Правообладатель: АО "СПИК СЗМА". Аттестационный паспорт ПС №222 от 21 февраля 2006 г., Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) РФ.:URL: http://www.szma.com/pkasm.shtml (Дата обращения 8.10.15).

5. Гладкова И.А., Струков А.В., Струков А.А. Сценарное логико-вероятностное моделирование опасной ситуации с использованием ПК АРБИТР // Сборник докладов второй международной научно-практической конференции «Имитационное и комплексное моделирование морской техники и морских транспортных систем» (ИКМ МТМТС 2013) // ISBN 978-5-902241-22-5 // ОАО «Центр технологии судостроения и судоремонта», Санкт-Петербург, 2013, с. 50-54.

6. Можаев А.С.Нозик А.А., Струков А.В. Оценка надежности системы из элементов с тремя состояниями с использованием ПК АРБИТР// Труды СПИИРАН, выпуск №8 (31), с.123-147. 2013.

7. Гладкова И.А., Нозик А.А., Струков А.В. Логико-вероятностное моделирование последствий аварий с использованием программного комплекса «АРБИТР» // Моделирование и Анализ Безопасности и Риска в Сложных Системах: Труды Международной Научной Школы МА БР-2014 (Санкт-Петербург, 18-20 ноября, 2014), ГОУ ВПО «СПбГУАП». СПб., 2014, С.223-228.

8. Викторова В.С., Степанянц А.С.Динамические деревья отказов// Надежность. — 2011. — №3(38).-С.20-32.

9. Codetta-Raiteri D. Generalized Fault Trees: from reliability to security// URL: http://people.unipmn.it/dcr/papers/qasa.pdf (Дата обращения 8.10.2015).

10. Bobbio A., Portinale L., Minichino M., Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks.- Reliability Engineering & System Safety. V.71 (2001). pp.249-260.

11. URL: http://www.isograph.com/software/attacktree/ (Дата обращения 8.10.2015).

12. Ten C., Liu C., Govindarasu M. Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees //

URL:http://powercyber.ece.iastate.edu/publications/GM-CS.pdf (Дата обращения 8.10.2015).

12. Можаева И.А. Методики структурно-логического моделирования сложных систем с сетевой структурой // Автореферат диссертации на соискание ученой степени кандидата технических наук. Санкт-Петербург. 2015. 19с.