ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 519.6

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ СИНТЕЗА СИСТЕМЫ УПРАВЛЕНИЯ ЗАЩИЩЕННОСТЬЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В УСЛОВИЯХ ДЕЙСТВИЯ ОПТИМИЗИРОВАННЫХ АТАК ПРИ ИНФОРМАЦИОННОМ КОНФЛИКТЕ

ГРАКОВ В.И.,
МЕДЕНЕЦ В.В.
ХАБАРОВА Д.С.

АННОТАЦИЯ

В статье обосновываются и рассматриваются компоненты концептуальной модели организации управления защищённостью автоматизированной системы при оптимизированных информационных атаках противодействующей системы в условиях информационного конфликта или войны.

Ключевые слова: национальная безопасность; информационная безопасность; система управления; система защиты информации; управление автоматизированной системой; оптимизация управленческих воздействий.

CONCEPTUAL SYNTHESIS MODEL OF SYSTEM SECURITY MANAGEMENT OF THE AUTOMATED SYSTEM UNDER THE ACTION OF OPTIMIZED ATTACKS IN INFORMATIONAL CONFLICT

GRAKOV V.I.,
MEDENETS V.V.,
KHABAROVA D.S.

ABSTRACT

The article considers and substantiates the components of the conceptual model of organizing the security control management of automated system under the optimized information attacks of counteracting system in conditions of information conflict or war.

Keywords: national security; international security; control system; information security system; automated system control; management actions optimization.

Основными направлениями обеспечения национальной безопасности РФ являются стратегические национальные приоритеты: национальная оборона, государственная и общественная безопасность [1]. Компонентами системы обеспечения национальной безопасности являются информационные и телекоммуникационные системы, для развития которых в среднесрочной перспективе потребуется преодолеть технологическое отставание, разработать и внедрить технологии информационной безопасности в системах государственного и военного управления.

Под информационной безопасностью РФ понимается состояние защищенности

её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [2]. В Доктрине информационной безопасности РФ одной из составляющих национальных интересов РФ выделена защита информационных ресурсов и обеспечение безопасности информационных и телекоммуникационных систем, развернутых и создаваемых на территории России в условиях обозначенных видов и источников угроз.

Среди внешних источников угроз информационной безопасности РФ определены следующие [2]:

– деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

– стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

– обострение международной конкуренции за обладание информационными технологиями и ресурсами;

– деятельность международных террористических организаций;

– увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

– деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

– разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Можно заключить, что все перечисленные источники угроз являются потенциальными источниками информационных конфликтов и информационных войн. Очевидно, что поражение в информационной войне- войне систем управлений - предопределяет и поражение в целом [3,4].

Под информационной войной будем понимать целенаправленные оптимизированные действия конфликтующих систем с помощью информационного оружия (информационных атак), проводимые с целью снижения государственного, военного и боевого потенциалов конфликтующей противодействующей стороны и сохранения (повышения) своих соответствующих потенциалов.

Из выше проведенного анализа следует, что разрешение проблем синтеза моделей и алгоритмов функционирования систем управления информационными и телекоммуникационными системами, защитой информации автоматизированных систем различного назначения в условиях целенаправленного противодействия являются актуальными и определены пунктами 3, 5 в Перечне приоритетных направлений развития науки, технологий и техники Российской Федерации, утвержденного Президентом Российской Федерации 7 июля 2011 г., а также в пунктах 1 и 13 Перечня критических технологий Российской Федерации, утвержденного Президентом Российской Федерации 7 июля 2011 г [5, 6].

Обоснование проблемы управления защищенностью автоматизированной системы. Концептуальная модель управления защищенностью автоматизированной системы (АС) базируется на факте развития и внедрения IT-технологий во все сферы деятельности общества [7–11]. Основной целью совершенствования систем управления различного назначения является автоматизация функций и задач управления. интеллектуализация подсистем контроля и принятия решений, как о состоянии управляемых объектов, так и о стратегии (плане) управления его состоянием [12].

С другой стороны, обостряется проблема национальной информационной безопасности [2–4, 10, 11] и свидетельствующая текущая статистика из средств массовой информации о вооруженных и информационных конфликтах в различных иностранных регионах. Свойством любых конфликтов является втягивание сторонних объектов, чьи интересы затрагиваются [13].

В [3, 4] и ряде других работах рассматриваются основные аспекты разрешения проблемы защиты информации и компонентов АС в информационных войнах. В [14, 15] осуществлена постановка задачи синтеза систем, и предлагается обобщённая модель противодействующих систем в конфликтной ситуации.

Из анализа цикла управления защищенностью АС результатом синтеза защиты АС является решение в виде плана защиты информации в АС в виде совокупности управляющих воздействий на интегрированные в элементы и подсистемы АС компоненты системы защиты. При этом оптимизируется не только структура совокупности управляющих защитой воздействий, но и их последовательность реализации для определенных условиях противодействия.

Целенаправленность управления защитой информации (ЗИ) заключается в синтезе таких управленческих воздействий на систему защиты информации (СЗИ), которые переводят её в наиболее предпочтительное (оптимальное) состояние или подмножество предпочтительных допустимых состояний с нечёткими границами, определёнными руководящими документами, текущей стратегией противодействующей системы (ПДС) и имеющихся ресурсов защитных механизмов и сервисов.

В терминах теорий управления и принятий решений выбор управляющих воздействий, как элементов упорядоченного плана (стратегии) управления системой защиты АС, называется принятием решения и является центральным моментом всякого управления [12, 16, 17].

Концепция задачи принятия решения на управление защищенностью АС в условиях оптимизированного противодействия. Задачу выбора плана синтезируемой системы ЗИ в условиях, определённых текущим вектором *Y*, характеризующий текущее поведение ПДС, $Y \in \bar{Y}$, представим двумя компонентами: реализационной и оценочной структурой. Пусть $\bar{X}$ – множество допустимых вариантов построения СЗИ АС представленных векторами *X*, множество $\bar{Y}$ – условий функционирования АС (определяются структурой реализуемых угроз противодействующей системы). Задачей управления является принятие оптимального решения на управление структурой, алгоритмами функционирования и параметрами элементов структуры СЗИ. Неопределенность условий функционирования свяжем со следующими факторами: субъективизм и запаздывание в оценке стратегии реализации угроз ПДС; флюктуация границ значений параметров и показателей СЗИ в динамике функционирования; субъективизм руководящих документов, относительно требований и оценивания защищённости АС; не возможность учёта всех параметров системы и факторов противодействия, оказывающая влияние на точность и достоверность оценивания; относительная своевременность контроля параметров и состояния системы в целом.

Из этого следует, что решение задачи оценивания состояния защищенности АС и синтеза требуемой СЗИ АС в определенных условиях необходимо реализовывать в границах математического аппарата для ε–оптимальных систем [17]. Функциональная структура задачи принятия решения при синтезе оптимального плана защиты АС в условиях оцененной ситуации показана на рисунке.

Состояние СЗИ и соответственно защищённой автоматизированной системы (ЗАС) $S \epsilon \bar{S}$ полностью определяется выбором плана управляющих воздействий $X \epsilon \bar{X}$ и состоянием ПДС $Y \epsilon \bar{Y}$, тогда существует такая функция реализации $F: X \times Y \to S$, которая каждой паре $(X; Y)$ ставит в соответствие некоторое состояние ЗАС $S \epsilon \bar{S}$ [16, 17]. Таким образом, кортеж $< \bar{X}, \bar{Y}, \bar{S}, F >$ составляет реализационную структуру задачи принятия решения на управление защитой АС. Состояние полностью зависит от выбранного варианта защиты АС и от оцен-

ки текущего состояния ПДС. Неопределённость ПДС порождают условия, в которых принимаются решения: неопределенности, риска и конфликта. Поэтому концептуальная модель должна предусматривать постановки частных задач синтеза СЗИ АС:

– синтез СЗИ АС в условиях определённости, характеризующаяся тем, что состояние ПДС определяемое применяемой стратегией известна;

– синтез СЗИ АС в условиях риска, характеризующаяся тем, что имеет информация статистического характера о результатах стохастического поведении ПДС или распределения вероятностей характеристик стратегии ПДС;

– синтез СЗИ АС в условиях неопределённости предполагает, что никакой дополнительной информации, кроме возможно самого множества потенциальных стратегий ПДС;

– синтез СЗИ АС собственно в конфликтных условиях, когда цели функционирования систем противоположны, а частные решения осуществляются в определенном порядке и в разных и комбинированных многоуровневых условиях.

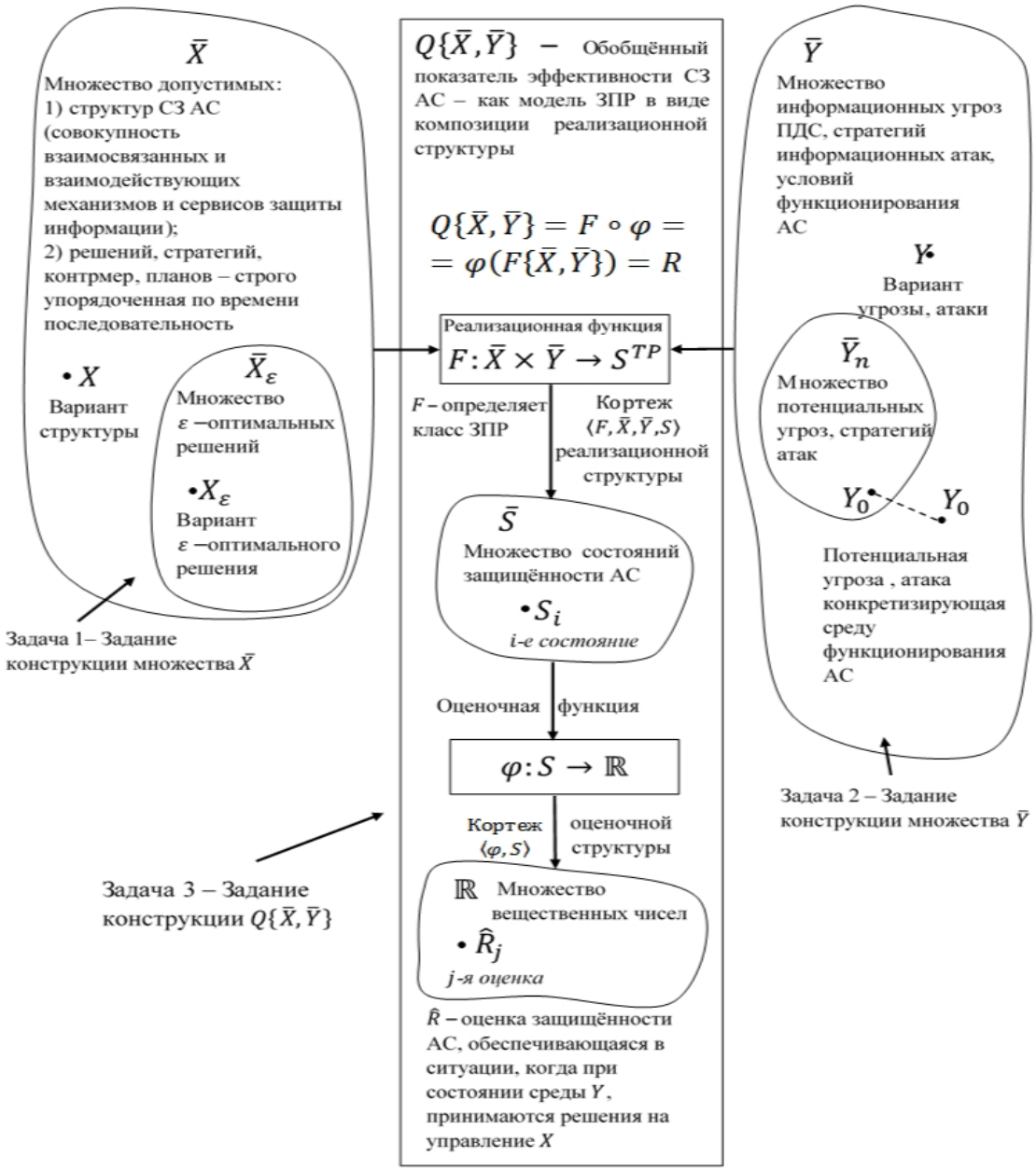

Рисунок 1 – Функциональная структура задачи принятия решения при синтезе защиты АС в условиях оптимизированной атаки

Полное или частичное снятие неопределённости возложено на подсистему контроля состояния защиты АС.

Концепция задачи контроля и оценки текущего состояния защищенности АС. Реализационная структура задачи принятия решения на стратегию управления определяет требуемое и текущее состояние защиты АС. Оценочная структура указывает оценку этого результата с точки зрения ЛПР на управление ЗИ.

Если ЛПР оценивает эффективность каждого состояния ЗИ АС некоторым числом $\varphi(S)$, то оценочную структуру зададим в виде кортежа $< \bar{S}, \varphi >$, где оценочная функция $S \to \mathbb{R}$.

Вариантом оценочной структуры является система отношений предпочтений для всех вариантов построения системы ЗИ, в частности для пары $(s_1; s_2)$, $s_1 > s_2$ и s_1 и предпочтительней s_2 [17]. Предлагается введение оценочных структур на уровне оценивания состояния систем путём искусственного разбиения множества состояний $\bar{S}$, на подклассы допустимых $\bar{S}_д$, промежуточных $\bar{S}_п$ и неудовлетворительных $\bar{S}_н$ состояний системы ЗИ.

В общем случае оценочная структура задачи принятия решений о состоянии ЗИ носит субъективный характер, так как оценивание вариантов построения системы ЗИ производится по искусственным шкалам и с точки зрения принимающего решения,

Обобщённый показатель эффективности и состояния защищенности АС представим композицией функций F и φ, т.е. $Q = \varphi \circ F$ и, следовательно, $Q(X,Y) = \varphi(F(X,Y))$, где $X \epsilon \bar{X}$, $Y \epsilon \bar{Y}$.

Процедуры задания конструкций кортежа $< \bar{X}, \bar{Y}, Q >$ и их интерпретация составляют основу обобщенной формальной модели системы оперативного управления защитой АС. В дальнейшем конструкции модели используются для постановки и решения частных математических задач синтеза компонентов этой системы управления. Авторы утверждают, что решение задачи принятия решений об оценке защищенности АС и оптимизации плана защиты АС представляет собой многокритериальную задачу оптимизации и не сводимую к скаляризации вектора частных показателей в обобщенный для применения методов классической нелинейной оптимизации [17, 18].

Предлагается оценку состояния защищенности АС реализовать методами многокритериальной оптимизации, положенных в основу следующего обобщенного алгоритма [19]:

– обоснование множества допустимых планов защиты АС;

– обоснование множество потенциальных состояний ПДС;

– формирование существенных частных показателей эффективности системы защиты АС;

– обоснование предпочтений ЛПР;

– оценка ситуации, характеризующей поведение ПДС и текущее состояние защищенности АС;

– снятия неопределенности состояния ПДС на основе реализации критерия Байеса-Лапласа;

– оценка вариантов решения для каждого частного критерия оценки защищенности АС в условиях риска;

– выбор метода многокритериальной оптимизации для решения задачи в условиях определенности;

– определение оптимального плана защиты АС.

После снятия неопределённости применим методы классической оптимизации и математического программирования [17, 18]. Формально задача оптимизации примет вид: найти такой план защиты условиях функционирования защищенной АС (ЗАС) $Y = Y_0$, при котором ОПЭ $Q(X^*, Y_0)$ принимает максимальное значение:

$$Q(X^*, Y_0) \to \max_{X \epsilon \bar{X}}, \text{ где } Y_0 \epsilon \bar{Y} \qquad (1)$$

В качестве решения задачи (1) рассматриваются варианты стратегий защиты информации, при конкретном оценённом состоянии ПДС $Y_0 \epsilon \bar{Y}$.

Под состоянием ПДС понимаем совокупность значений характеристик преднамеренного воздействия информационными атаками в рассматриваемый период времени. Оно конкретизирует условия функционирования ЗАС и определяет множество допустимых ε–оптимальных планов защитных контрмер: $X_\varepsilon \epsilon \overline{X_\varepsilon}(X, Y_0)$, где $\varepsilon \geq 0$.
Из этого выражения следует, что

$$Q(X,Y) \leq Q(X_\varepsilon, Y_0) + \varepsilon, \quad \forall X \epsilon \bar{X} \qquad (2)$$

т.е. изменение плана ЗИ относительно ε–оптимального не может повысить эффективность защиты в условиях Y_0 более чем на величину ε.

В случае если $\varepsilon > 0$ необходимость рассмотрения ε–оптимальных решений обусловлена целесообразностью упрощения методов поиска и нахождения реализуемых решений, а в случае $\varepsilon = 0$ обусловлена принципиальным несуществованием оптимальных компонентов для определенных вариантов построения системы ЗИ, т.е. $\overline{X_\varepsilon}(X, Y_0) = \emptyset$ и задача поиска оптимального варианта теряет смысл.

Из (2) и определения ε–оптимальной системы X_ε также вытекает, что при её применении в условиях Y_0 обеспечивается следующее значение ОПЭ:

$$Q\{X_\varepsilon, \bar{Y}\} \geq \sup_{X \epsilon \bar{X}} Q\{\bar{X}, Y_0\} - \varepsilon \qquad (3)$$

При синтезе защиты АС в условиях неопределенности полагаем не полное задание условий Y_0, что определяет наполняемость множества $\bar{Y}$, в которых возможно функционирование ЗАС. Поэтому для формулировок математически корректной задачи, так или иначе, используются дополнительные сведения об условиях функционирования ЗАС, которые и порождают различные подходы к синтезу варианта СЗИ при заданной архитектуре АС и состояния ПДС.

Так как множество $\bar{Y}$ характеризуется свойством конфликтности, (противоборствующие системы ПДС и СЗИ имеют противоположные цели) полагаем, что основной обобщённой целью для ПДС будет стремление уменьшить ОПЭ $Q\{\bar{X}, \bar{Y}\}$ за счет выбора оптимальных стратегий информационной атаки.

Пусть для функционирования в конфликтных условиях $\bar{Y}$, разработана и внедрена СЗИ $X \epsilon \bar{X}$. Задачу оптимизации противодействия представим в виде:

$$Q\{X,Y\} \rightarrow \min_{Y \epsilon \bar{Y}}, \qquad (4)$$

решение, которой обеспечит ПДС возможность реализовывать атаку на ЗАС до уровня, определенного значением ОПЭ сколь угодно близким к величине

$$Q\{X, \bar{Y}\} \triangleq \inf_{Y \epsilon \bar{Y}} Q\{\bar{X}, \bar{Y}\} \qquad (5)$$

При построении корректной модели класс $\bar{Y}$ должен характеризовать потенциальную совокупность возможностей, реально имеющихся у ПДС, а функционал $Q\{X,Y\}$ учитывает, кроме того, предпочтительность такого выбора. Тогда, очевидно, величина $Q\{X, \bar{Y}\}$ определяет эффективность применения СЗИ *X* и задача синтеза СЗИ в конфликтных условиях формулируется в терминах минимаксной задачи вида [18]:

$$Q\{X, \bar{Y}\} = \inf_{Y \epsilon \bar{Y}} Q\{X,Y\} \rightarrow \max_{X \epsilon \bar{X}} \qquad (6)$$

В качестве решений задачи (6), по аналогии с выражением (4), рассматривается множество $\overline{X_\varepsilon}$-оптимальных систем X_ε $(\varepsilon \geq 0)$, которое формализуем выражением

$$X_\varepsilon \in \overline{X_\varepsilon}(\bar{X}, \bar{Y}) \Leftrightarrow \inf_{Y \epsilon \bar{Y}} Q\{X,Y\} \leq$$

$$\leq \inf_{Y \epsilon \bar{Y}} Q\{X_\varepsilon, Y_0\} + \varepsilon, \ \forall X \in \bar{X} \qquad (7)$$

Иначе, изменение варианта построения СЗИ относительно ε-оптимального не может повысить эффективность её функционирования в условиях оптимизированного противодействия более чем на ε.

Тогда, из определения ε-оптимальной системы следует, что при её применении в классе условий $\bar{Y}$ гарантирует значение ОПЭ $r \in \mathbb{R}$, равное:

$$r_0\{X_\varepsilon\} = \inf_{Y \epsilon \bar{Y}} r\{X_\varepsilon, Y\} \geq Q\{\bar{X}, \bar{Y}\} - \varepsilon, \qquad (8)$$

где $Q\{\bar{X}, \bar{Y}\} \triangleq \sup_{X \epsilon \bar{X}} \inf_{Y \epsilon \bar{Y}} Q\{X,Y\}$.

Предлагаемая концептуальная формализованная модель (8) позволяет перейти к конкретизации кортежа конструкции модели $\langle \bar{X}, \bar{Y}, Q \rangle$ с целью построения обобщенной модели взаимодействия противодействующих систем и математического моделирования компонентов системы управления защищенностью автоматизированной системы.

Список литературы

1. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537

2. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

3. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. – М.: Синтег, 1999. – 232 с.

4. Расторгуев С.П. Информационная война. – М.: Радио и связь, 1999. – 416 С.

5. Приоритетные направления развития науки, технологий и техники в Российской Федерации. Утверждены Указом Президента Российской Федерации от 7 июля 2011 г. №899

6. Перечень критических технологий Российской Федерации. Утверждены Указом Президента Российской Федерации от 30 марта 2002 года № Пр-576.

7. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Российская газета» от 29 июля 2006 г.

8. Зегжда Д.П., Иваненко А.М. Основы безопасности информационных систем. – М.: Горячая Линия – Телеком, 2000. – 452 с.

9. Зегжда Д.П. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1996. – 300 с.

10. Сухарев Е.М. Общесистемные вопросы защиты информации. Под ред. Е.М. Сухарева. Кн. 1. – М.: Радиотехника, 2003. – 296 с.: ил.

11. Сухарев Е.М. Модели технических разведок и угроз безопасности информации. Под ред. Е.М.Сухарева. Кн. 3. – М.: Радиотехника, 2003. – с.: ил.

12. Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении: Учебное пособие / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; Под ред. А.А. Емельянова. - М.: Финансы и статистика, 2002. – 368 с.

13. Русаков С.А. Основы управленческой деятельности: учеб. пособие / С.А. Русаков. – М.: Гелиос АРВ. 2010. – 240 с.

14. Граков В.И., Меденец В.В., Песков М.В. Динамическая модель системы связи защищенной автоматизированной системы с управляемыми структурами // Тезисы докладов, Материалы II Международной НПК «Актуальные проблемы современной науки». – Ставрополь: Фабула, 2013.

15. Граков В.И. Задача синтеза систем в конфликтных условиях как минимаксная задача // Тезисы докладов 1-й международной НТК. – Белгород: 2009.

16. Егоров А.И. Основы теории управления. – М.: Физматлит, 2007. – 504 с.

17. Черноруцкий И.Г. Методы принятия решений. – СПб.: БХВ – Петербург, 2005. – 416 с.

18. Сухарев А.Г., Тихов А.В., Федоров В.В. Курс методов оптимизации. Учебное пособие. – М.: Физмалит, 2005. –368 с.

19. Хабарова Д. С. Обзор программных комплексов многокритериальной оптимизации для оценки параметров информационной системы // Прикладная информатика. – 2013. – №2 (44), – Москва. – 102-112 с.