

УДК 338.2

Жидко Елена Александровна

ФГБОУ ВПО «Воронежский государственный архитектурно-строительный университет»

Россия, Воронеж¹

Профессор кафедры пожарной и промышленной безопасности

Кандидат технических наук, доцент

E-Mail: lenag66@mail.ru

Методология системного математического моделирования информационной безопасности

Аннотация. В Доктрине информационной безопасности Российской Федерации отмечается: противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере; отставание отечественных информационных технологий от мирового уровня их развития; отсутствие политики информационной безопасности у отечественных компаний.

Все они приводят к негативным последствиям для личности, общества, государства, предупреждение и ликвидация которых выливается в серьёзную научную и практическую проблему в реально складывающейся и прогнозируемой обстановке XXI века. Актуальность необходимости разрешения такой проблемы определяется тем, что информационная безопасность Российской Федерации рассматривается как один из главных аргументов нашей национальной безопасности.

В результате создания теоретических основ системного математического моделирования информационной безопасности приоритетных объектов защиты, заданных доктриной, в статье предлагается логическая схема методологии такого моделирования. Она базируется на технологии комплексного прогнозирования возможных исходов взаимосвязанного развития внешней и внутренней среды объекта защиты по ситуации и результатам в статике и динамике условий XXI века.

В статье сделан акцент на нормативную технологию прогнозирования безопасности и устойчивости развития объекта как функции его информационного обеспечения, аргументом которого является его защищённость от угроз нарушения информационной безопасности с критическими и/или неприемлемыми последствиями

Ключевые слова: информационная безопасность; системное математическое моделирование; информационная и интеллектуальная поддержка защищенности; риски; модели взаимосвязанного развития.

Идентификационный номер статьи в журнале 67TVN314

¹ 394006 г. Воронеж, ул.20-летия Октября, д.84

Согласно принятым концепции и принципам, объектом исследования является информационная безопасность (ИБ) приоритетного объекта защиты (ОЗ) (например, системы управления экологически опасного и экономически важного производства [1]).

Предмет исследований – управление циклами информационной и интеллектуальной поддержки защищённости (ИИПЗ) объекта от угроз нарушения его ИБ с негативными последствиями в условиях противоборства сторон на политической арене, конкурентной борьбы в социально-эколого-экономической сфере и информационной войны между ними в социальной.

Цель исследований – создание теоретических основ системного моделирования ИБ объекта в интересах обеспечения его устойчивого развития в заданных условиях по ситуации и результатам в статике и динамике XXI века.

Особенность в постановке и решении задач по достижению цели состоит в том, что безопасность и устойчивость развития объекта защиты рассматривается как функция его информационного обеспечения, аргументом которого является информационная безопасность объекта. Учитывается: существенное и активное влияние на неё человеческого, природного, других объективных и субъективных факторов, а также необходимость предупреждения информационных войн на основе разрешения информационных конфликтов, возникающих между сторонами.

Предпрогнозные исследования состояния вопроса по проблеме ИБ объектов защиты [2] привели к следующим выводам.

На современном этапе комплексные исследования научных и технических проблем с применением современной технологии математического моделирования и вычислительного эксперимента базируется на последовательном выполнении операций над потоками входной информации, как показано в логической схеме рис.1[Составлено автором]. Схема построена по методу структурных матриц.

Цель первого шага комплексных исследований по проблеме на основе использования приведенной методологии – выявление диспропорций между необходимым, потенциально возможным и реально достижимым. С этой целью:

- в диагональных элементах называются имена операций;
- в элементах ниже диагонали по принципу «каждый с каждым» содержатся: требования к результатам выполнения операции; приводятся ограничения на выбор способов и средств их достижения; сведения о накопленной базе знаний и ресурса, необходимого целевого и функционального назначения. Они образуют прямые информационные потоки

Моделирование и прогнозирование взаимосвязанного развития внешней и внутренней среды объекта, его системы ИБ 1.1	Ошибки	Задание на прогноз	Требования по корректировке прогнозов	Задание на информационную поддержку управления
Теоретические	Мониторинг состояний внешней среды и контролинг состояний внутренней среды объекта 2.2	Задание на отслеживание обстановки	Требования по созданию базы данных о реально складывающейся обстановке	Требования максимального приближения реально достижимого к необходимому
Информационные	Ошибки	Диагноз состояний объекта, его системы ИБ и их экспертиза на соответствие требуемым 3.3	Задание на экспертизу	Задание на отслеживание результатов
Риски (ГИР)	Ошибки	Эффективные риски и угрозы (ЭРУ)	Оптимизация устойчивости развития объекта по ситуации и результатам и адаптация их облика 4.4.	Задание на интеллектуальную поддержку управления устойчивостью развития
ГИР	Ошибки	ЭРУ	Эвентологические риски, меры по предупреждению угроз, ликвидации их негативных последствий	Управленческое консультирование по перспективным направлениям деятельности и устойчивого развития объекта 5.5
R_{гг}-априори , (Н-П)	Реально складывающаяся обстановка, эмпирически установленные ошибки	R_{гг}-апостериори , поле проблемных ситуаций (Р-П) и (П-Р)	Приоритетные ряды адекватных ответных мер по ситуации и результатам	Идентификация ситуации, адекватные ответные меры и следующий шаг

Рис. 1. Методология информационной и интеллектуальной поддержки проектного управления ИБ объекта, его системой ИБ

Цель второго шага комплексных исследований – оценка (диагноз) степени опасности таких диспропорций по критерию: допустимые, критические, неприемлемые. Принимается решение о необходимости и целесообразности корректировки и/или пересмотра требований по информационной безопасности объекта, системы ограничений на выбор способов и средств их обеспечения, дальнейшего развития и совершенствования накопленной базы знаний и ресурса по проблеме. Принятие таких решений базируется на поиске оптимальных и близких к ним способов и средств достижения целей объекта защиты по ситуации и результатам в реально складывающейся и прогнозируемой обстановке в его внешней и внутренней среде. Строится приоритетный ряд таких способов и средств, приводятся комментарии по ожидаемым результатам их внедрения. Это основа для управленческого консультирования лиц, принимающих решения.

Цель третьего шага – обоснование и принятие управленческих решений, адекватных реально складывающейся и прогнозируемой обстановке во внешней и внутренней среде хозяйствующего субъекта в заданном контексте, аспектах и условиях XXI века. Адекватность устанавливается по критерию:

- необходимо «И» потенциально возможно «И» реально достижимо;
- «ПРИ» допустимых, критических «И/ИЛИ» неприемлемых угрозах нарушения информационной безопасности объекта защиты, информационных рисках, их последствиях.

Результаты таких исследований – основа для количественного и качественного обоснования охраняемых сведений о намерениях и действиях объекта защиты. Требования к качеству приводятся в виде имени состояния защищённости объекта от угроз нарушения его информационной безопасности. Оно устанавливается пропорционально заданному уровню защищенности сведений об объекте защиты, относимых [6] к государственной и/или

коммерческой тайне. Количественное обоснование области определения характеристик методов и систем защиты информации требуемого целевого и функционального назначения рассматривается как комплексные исследования научных и технических проблем с применением современной технологии математического моделирования и вычислительного эксперимента. Такие исследования базируются на логико-вероятностно-информационном подходе к математическому моделированию объектов и явлений по проблеме в комплексе с вычислительным экспериментом.

Такой подход должен обеспечить формирование системы моделей, координат и измерительных шкал по проблеме защиты. На современном этапе в систему моделей взаимосвязанного развития внешней и внутренней среды объекта защиты должны войти комплексы синтаксических, семантических и адекватных им математических моделей, которые разработаны теоретическими, эмпирическими и эвентологическими методами.

Комплексы синтаксических моделей предназначены для выявления сущности исследуемых объектов и явлений по логическим основаниям [1,3]:

- цель, место и время действий, диапазон условий и поле проблемных ситуаций, возникающих во внешней и внутренней среде объекта защиты. Это необходимо для распознавания ситуации;
- природа и масштабы объекта, сложность его внешних и внутренних связей, детерминированность и цикличность явлений, их информационная обеспеченность. Это необходимо для выбора комплекса эффективных методов исследования по методологии схемы рис.1;
- причинно-следственные связи, движущие силы, цели, законы и закономерности взаимосвязанного развития внешней и внутренней среды объекта защиты. Это необходимо для эффективного решения задач ИБ объекта на основе применения комплексных исследований научных и технических проблем с применением современной технологии математического моделирования и вычислительного эксперимента.

Комплексы семантических моделей предназначены для определения отношений между сущностями объектов и явлений в заданном контексте, аспектах и условиях. Они устанавливаются по основаниям [1]:

- политика, экономика, социология, технологии (PEST анализ);
- социология, экология, экономика, технологии (SEEI анализ);
- сильные и слабые стороны, возможности и угрозы (SWOT анализ).

Логико-вероятностно-информационный подход в этом случае базируется на методах [7]:

- ветвления цели защиты по основаниям, принятым в синтаксической модели;
- фильтрации, т.е. оптимизации способов и средств достижения цели, построения их приоритетных рядов по основаниям, принятым в семантической модели;
- комментирования, т.е. оценки возможности достижения цели в намеченные плановые сроки с помощью различных методов и систем защиты информации по ситуации и результатам в статике и динамике условий XXI века.

Это значит, что семантическое моделирование базируется на использовании известных в теории проектных зависимостей между требованиями к уровню защищённости объекта от угроз нарушения его ИБ и техническими характеристиками методов, систем и средств защиты. Несовершенство таких зависимостей порождает промахи и ошибки в выборе внешних и внутренних политик в рассматриваемых сферах. Следствием их являются допустимые, критические и/или неприемлемые исходы:

- противоборства договаривающихся сторон на политической арене;
- конкурентной борьбы между ними в социально-эколого-экономической сфере;
- информационной войны в идеологической, информационно-психологической и кибернетической областях.

Имена таких исходов ассоциируются [1,2,3] с упущенной выгодой, полной неопределённостью ситуации, причинённым ущербом. В результате активного и существенного влияния на такие исходы человеческого, природного, др. объективных и субъективных факторов порождается неопределённость в распознавании ситуации и оценке результатов. Поэтому они носят вероятностный характер, который существенно зависит от меры реально получаемой информации в контексте логической схемы рис.1.

С целью парирования неопределённости результаты, полученные теоретическими проектными методами, проверяются на практике как с помощью натурального и/или имитационного, так и вычислительного эксперимента. Особенность состоит в том, что с помощью теоретических методов устанавливаются эталонные отношения между именем состояния защищённости и адекватными ему значениями технических характеристик методов и систем защиты информации. В результате эксперимента выявляются совершенные промахи и ошибки. С помощью эвентологических методов вскрываются причинно-следственные связи между такими ошибками и исходами взаимодействия сторон в реально складывающейся и прогнозируемой обстановке. Оценка приемлемости исходов по приведенному выше критерию позволяет установить допустимые, критические, неприемлемые погрешности в оценке уровня защищённости объекта. Отсюда обоснованные требования к перечню охраняемых сведений, количественным и качественным характеристикам методов и систем их защиты.

Система математических моделей предназначена для своевременного получения качественных результатов (т.е. полных, достоверных, точных и полезных) комплексных исследований по проблеме на основе парирования неопределённости, дальнейшего развития и совершенствования современной технологии математического моделирования и вычислительного эксперимента. С этой целью приведенную методологию исследований по схеме рис.1. целесообразно адаптировать к постановке и решению задач, названных в логической схеме рис. 2 [Составлено автором].

Прямые информационные связи (спуск) отражают делегирование функций от стратегического видения к целевому назначению подразделений объекта защиты в иерархии его структуры по вертикали. Обратные информационные связи (подъём) содержат результаты контроля эффективности выполнения заданных функций, в том числе:

- сведения о диспропорциях между требуемым, потенциально возможным и реально достижимым; порождающих их причинах и последствиях;
- необходимых и достаточных мерах по предупреждению таких причин, ликвидации их негативных последствий.

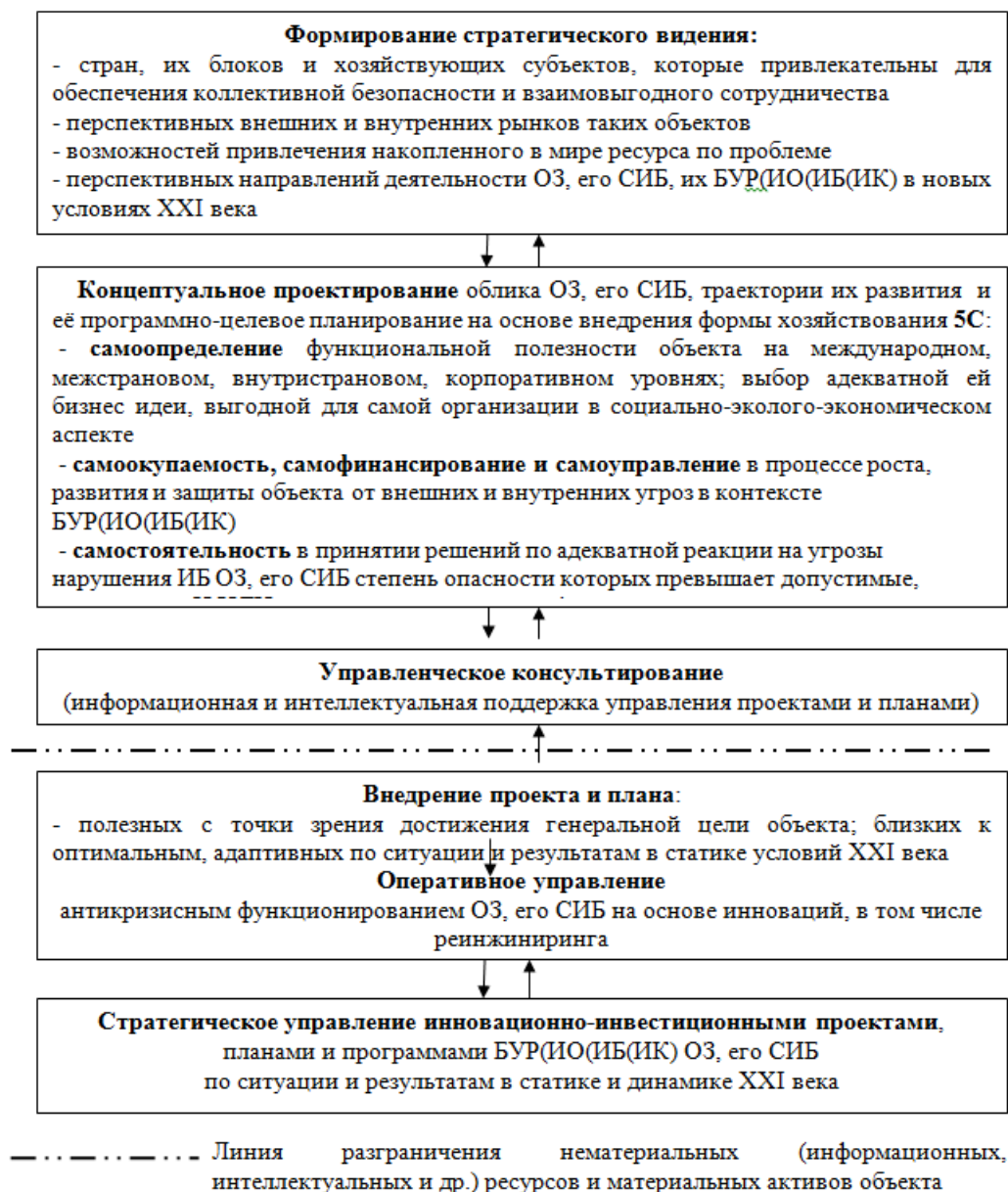


Рис. 2. Система задач управления проектами, решение которых базируется на комплексировании нематериальных и материальных ресурсов

С целью получения требуемых выходных результатов аналогично образуют прямые и обратные информационные связи на каждом уровне иерархии между необходимыми технологическими операциями (шаги в иерархии по горизонтали) над заданными входными воздействиями на объект.

Сведения о возникших диспропорциях на каждом уровне и шаге с помощью SWOT анализа позволяют выявить сильные и слабые звенья в структуре объекта защиты, оценить возможности и угрозы, степень их значимости и опасности в контексте: безопасность и устойчивость развития (БУР) ОЗ, его системы информационной безопасности (СИБ), как функция информационного обеспечения (ИО). Аргументом ИО является ИБ объекта. Она рассматривается как функция требований по разрешению информационного конфликта (ИК), который возникает между сторонами, договаривающимися о коллективной безопасности и взаимовыгодном сотрудничестве. Строятся приоритетные ряды сильных и слабых звеньев объекта, устанавливается значимость каждого из них для достижения его целей, выделяются

первоочередные задачи по поддержке и дальнейшему развитию сильных звеньев, ликвидации слабых. Общая методология решения таких задач приведена на схеме рис.3[Составлено автором].



Рис. 3. Схема логических прямых и обратных информационных связей «цели- средства»

В реально складывающейся и прогнозируемой обстановке XXI века реализация комплексных исследований по проблеме устойчивости развития ОЗ по методологиям рис. 1. – 3, должна осуществляться по логической схеме:

- статика: сложившаяся обстановка по месту и времени действий – цель – поле проблемных ситуаций – решение проблем – побочные эффекты – их устранение в интересах достижения цели по ситуации и результатам в реальном и близком к нему масштабе времени;
- динамика: прогнозируемая обстановка по месту и времени действий – цель – действие – противодействие – ответная мера и т.д. в интересах достижения цели в краткосрочном, среднесрочном и долгосрочном периодах XXI века.

В свете выше изложенного программа исследований по проблеме ИБ ОЗ приобретает вид, показанный на схеме рис.4[Составлено автором].

Решающим фактором для её реализации становится эффективное управление циклами информационной и интеллектуальной поддержки защищённости (ИИПЗ в рис.3.) объекта от угроз нарушения его ИБ с целью достижения и сохранения требуемого уровня БУР(ИО(ИБ(ИК) ОЗ, его СИБ в статике и динамике условий XXI века.

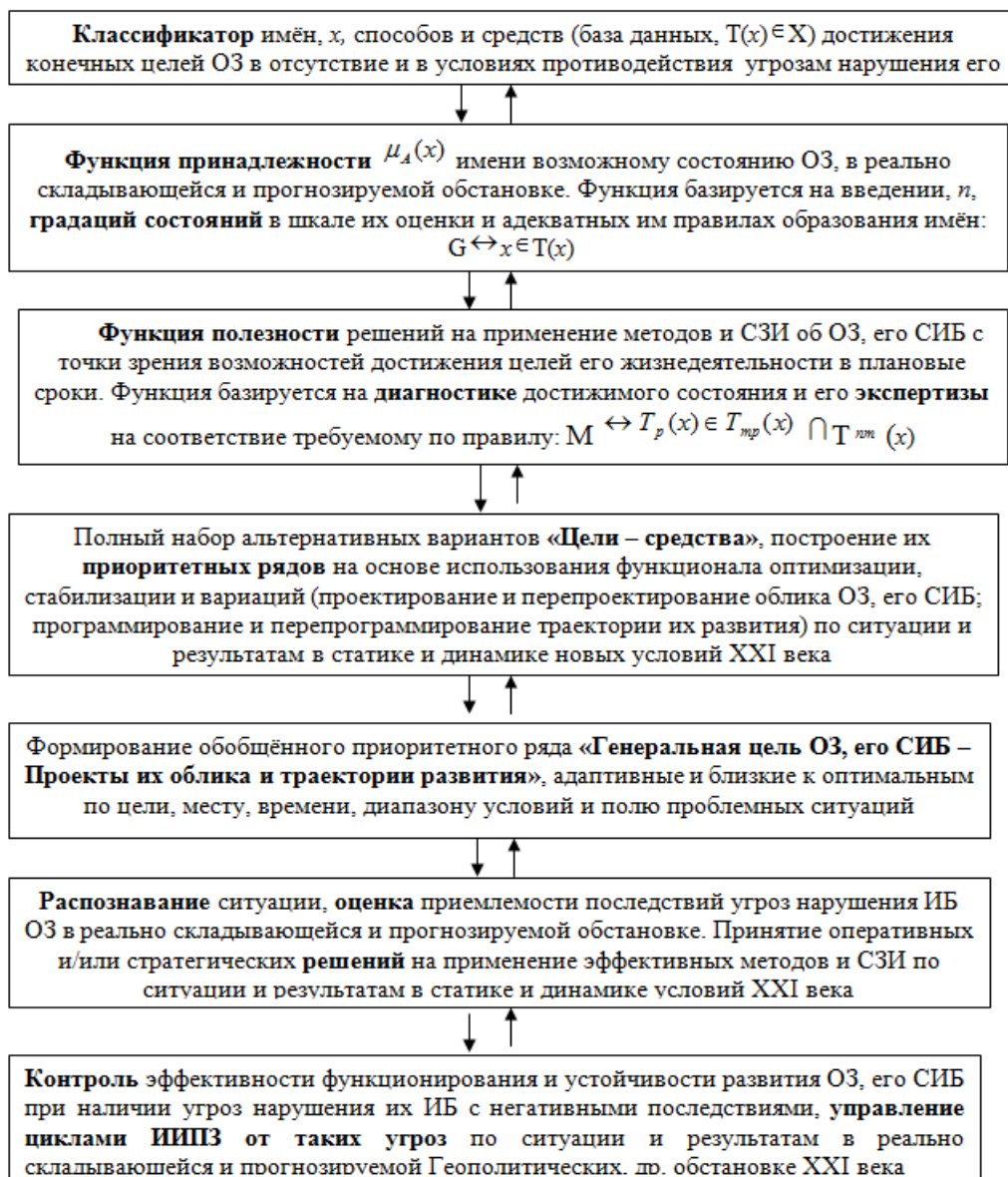


Рис. 4. Программа исследований ИБ ОЗ, его СИБ и управления ею

Нетрудно видеть, что возникающие приоритетные задачи по обеспечению ИБ ОЗ, его СИБ относятся к числу многоцелевых, многофакторных, многомерных и многокритериальных. Они имеют многоальтернативные решения, которые организуют в приоритетные ряды в условиях неопределённости, ограниченного ресурса, необходимости обеспечения устойчивости развития объекта в заданном контексте, аспектах и условиях XXI века. С целью эффективного решения задач по схемам рис.1.– 4 целесообразно разработать систему проблемно-ориентированных программ, приняв в качестве аналогов географические информационные системы (GIS), CASE(IDEF) технологии и др. требуемого целевого и функционального назначения.

Пример реализации такого подхода к автоматизации исследований по проблеме приведен на схеме рис.5 [Составлено автором]

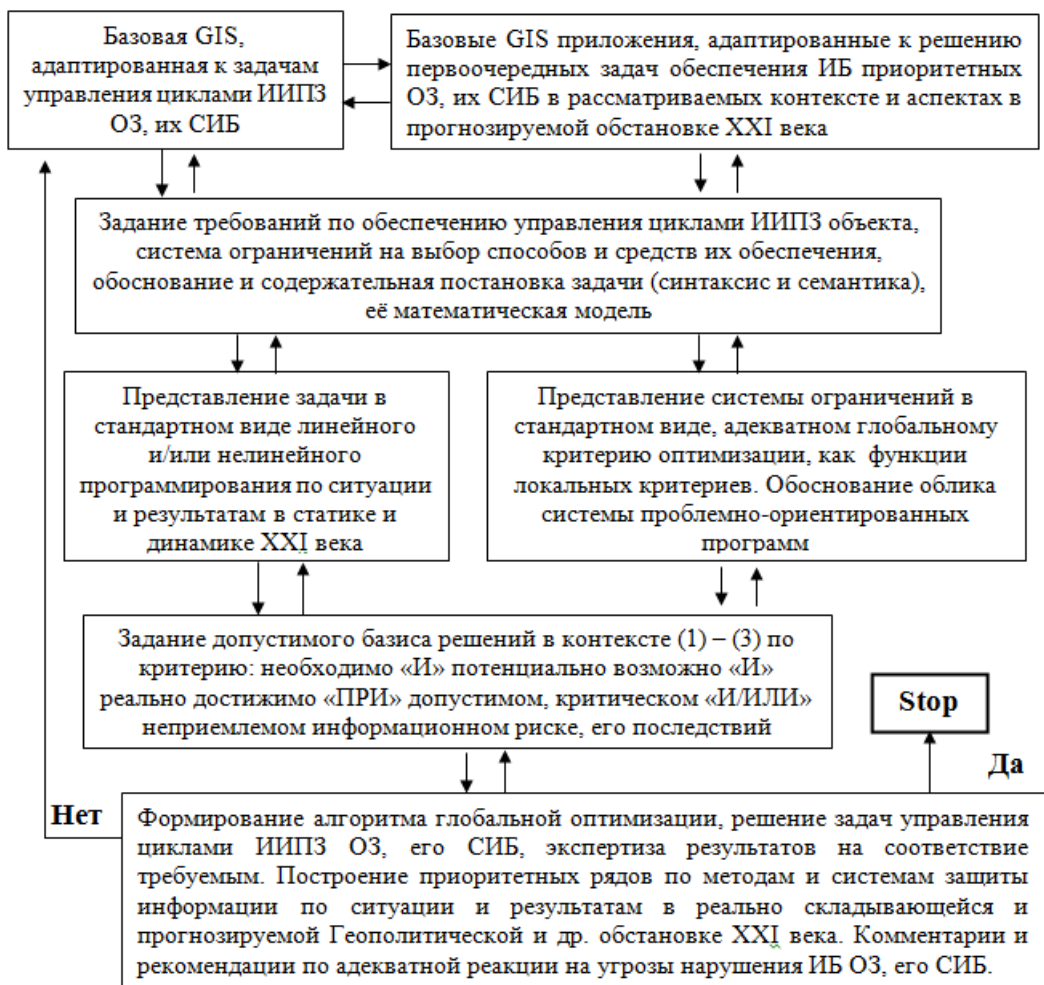


Рис. 5. Алгоритм глобальной оптимизации управления циклами ИИПЗ объекта

Заметим, что проблема глобальной оптимизации носит концептуальный характер. На современном этапе проводятся интенсивные исследования по поиску путей её разрешения.

В заключение отметим. Разработанный комплекс методологий ведения исследований по ИБ ОЗ требует своего вполне определённого методического обеспечения.

Например. Теоретические методы системного моделирования по проблеме базируются на методах вложений, аналогий, ассоциаций, асимптотического приближения и структурных матриц. Эмпирические методы базируются на методах математической статистики и численных методах. Эвентологические исследования основаны на моделировании по формуле Бэкуса-Наура, семантических диаграмм и скобочных конструкций.

С целью формирования системы координат и измерительных шкал эффективности реакции на угрозы нарушения ИБ ОЗ целесообразно воспользоваться следующими приёмами [1,2,3]:

- с целью введения градаций (норм, эталонных значений) возможных состояний устойчивости развития объекта в заданном контексте, аспектах и условиях принять в качестве начала отсчёта нормальный закон распределения вероятности достижения цели объекта с центральной симметрией;
- в интересах задания требований к допустимым, критическим и/или неприемлемым отклонениям от эталонных значений состояний следует их

ассоциировать с искажениями нормального закона распределения вероятностей с центральной симметрией. Тогда с помощью методов аналогий, ассоциаций и асимптотического приближения эмпирически установленной закономерности к адекватному ей закону распределения вероятностей, получим математическую модель реально складывающейся и/или прогнозируемой обстановки в условиях XXI века;

- с целью построения измерительных шкал для оценки состояния защищенности объекта от угроз нарушения его ИБ следует воспользоваться приемами нормализации критериев оптимизации способов и средств достижения целей объекта. Они базируются на концептуальном выборе схем компромисса, введении адекватного им функционала оптимизации, задании приоритетного ряда локальных критериев и методе учёта приоритетов.

С целью повышения достоверности таких исследований рекомендуется воспользоваться основными положениями теории ноосферы и ноогенеза, разработанными В.И. Вернадским, нормами экологической безопасности, действующими механизмами её регулирования и санкциями за нарушение норм. Проблему экологической безопасности следует рассматривать как аргумент социально-экономической безопасности по ситуации и результатам в статике и динамике условий XXI века [4,5].

ЛИТЕРАТУРА

1. Жидко Е.А., Попова Л.Г. Информационная безопасность: концепция, принципы, методология исследования: монография/ Е.А. Жидко, Л.Г. Попова; Воронеж. гос. арх-строит. ун-т. - Воронеж, 2013. - 175 с.
2. Жидко Е.А. Интегрированный менеджмент XXI века: проектное управление устойчивостью развития: учебное пособие / С.В. Барковская, Е.А. Жидко, В.И. Морозов, Л.Г. Попова; Воронеж. гос. арх-строит. ун-т. –Воронеж, 2011. -168 с.
3. Барковская С.В., Жидко Е.А., Морозов В.И., Попова Л.Г. Интегрированный менеджмент XXI века: парадигма безопасного и устойчивого (антикризисного) развития: монография/ С.В. Барковская, Е.А. Жидко, В.П. Морозов, Л.Г. Попова; Воронеж. гос. арх-строит. ун-т. –Воронеж, 2011. -168 с.
4. Жидко Е.А. Экологический менеджмент как фактор эколого-экономической устойчивости предприятия в условиях рынка: монография /Е.А. Жидко; Воронеж. гос.арх.-строит. ун-т.-Воронеж, 2009.-160 с.
5. Жидко Е.А. Менеджмент. Экологический аспект: курс лекций /Е.А. Жидко; Воронеж. гос.арх.-строит. ун-т.-Воронеж., 2010.-180 с.
6. Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне".
7. Саркисян С.А., Лисичкин В.А., Минаев Э.С. и др. Теория прогнозирования и принятия решений/ С.А. Саркисян, В.А. Лисичкин, Э.С.Минаев. М.: Высшая школа, 1977.

Рецензент: В.Г. Юрасов, Доктор технических наук, профессор кафедры «Системы автоматизированного проектирования и информационные системы» ВГТУ (Воронежский государственный технический университет).

Elena Zhidko

Voronezh State University of Architecture and Civil Engineering
Russia, Voronezh
E-Mail: lenag66@mail.ru

The methodology of the system of mathematical modeling of information security

Abstract. The information security Doctrine of the Russian Federation noted: the inconsistency and lack of legal regulation of social relations in the information sphere; the gap of domestic information technologies from the world of their level of development; lack of information security policy in domestic companies.

They all lead to negative consequences for the individual, society, state, prevention and elimination which results in serious scientific and practical problem in really developing and predictable environment of the XXI century. The urgency of the need to resolve this problem is determined by the fact that information security of the Russian Federation is considered as one of the main arguments of our national security.

In the theoretical foundations of the system of mathematical modeling of information security priority objects of protection specified by the doctrine, the article offers the logical scheme of the methodology of such modeling. It is based on technology of complex predict possible outcomes of interconnected development of the external and internal environment of the object of protection on the situation and results in static and dynamic conditions of the XXI century.

The article focuses on the normative forecasting technology security and sustainable development of the object as a function of information, an argument which is the security from threats of information security breach with critical and/or unacceptable consequences

Keywords: information security; system of mathematical modeling; information and intellectual support of security; risks; models of interrelated development.

Identification number of article 67TVN314

REFERENCES

1. Zhidko E.A., Popova L.G. Informacionnaja bezopasnost': koncepcija, principy, metodologija issledovanija: monografija/ E.A. Zhidko, L.G. Popova; Voronezh. gos. arh -stroit. un-t. Voronezh, 2013. 175 s.
2. Zhidko E.A. Integrirovannyj menedzhment HHI veka: proektnoe upravlenie ustojchivost'ju razvitija: uchebnoe posobie / S.V. Barkovskaja, E.A. Zhidko, V.I. Morozov, L.G. Popova; Voronezh. gos. arh-stroit. un-t. –Voronezh, 2011. -168 s.
3. Barkovskaja S.V., Zhidko E.A., Morozov V.I., Popova L.G. Integrirovannyj menedzhment HHI veka: paradigma bezopasnogo i ustojchivogo (antikrizisnogo) razvitija: monografija/ S.V. Barkovskaja, E.A. Zhidko, V.P. Morozov, L.G. Popova; Voronezh. gos. arh-stroit. un-t. –Voronezh, 2011. -168 s.
4. Zhidko E.A. Jekologicheskij menedzhment kak faktor jekologo-jekonomicheskoj ustojchivosti predpriyatija v uslovijah rynka: monografija /E.A. Zhidko; Voronezh. gos.arh.-stroit. un-t.-Voronezh, 2009.-160 s.
5. Zhidko E.A. Menedzhment. Jekologicheskij aspekt: kurs lekcij /E.A. Zhidko; Voronezh. gos.arh.-stroit. un-t.-Voronezh., 2010.-180 s.
6. Federal'nyj zakon ot 29 ijulja 2004 g. N 98-FZ "O kommercheskoj tajne".
7. Sarkisjan S.A., Lisichkin V.A., Minaev Je.S. i dr. Teorija prognozirovaniya i prinjatija reshenij/ S.A. Sarkisjan, V.A. Lisichkin, Je.S.Minaev. M.: Vysshaja shkola, 1977.