

УДК 004.056

Логико-вероятностно-информационный подход к формированию единого алгоритма исследований информационной безопасности объектов защиты

Жидко Е. А.

Постановка задачи: В доктрине информационной безопасности РФ отмечаются недостатки в её обеспечении на современном этапе. Один из них, это: «противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере, что приводит к серьезным негативным последствиям для личности, общества, государства. **Целью работы** является возможность создания единого логического подхода к исследованиям информационной безопасности объекта защиты при наличии угроз её нарушения с неприемлемыми последствиями. **Используемые методы:** методологию исследований по проблеме образуют методы вложений, аналогий, ассоциаций и асимптотического приближения теоретических и эффективных логико-лингвистических, семантических, математических методов моделирования, которые базируются на комплексировании методов моделирования по формуле Бэкуса-Наура. **Новизна:** формирование единого подхода к терминам информационной безопасности объекта базируется на синтаксическом, семантическом и математическом моделировании условно взаимосвязанного развития внешней и внутренней среды объекта теоретическими, эвентологическими и эмпирическими методами, скоординированными по цели, месту и времени, диапазону условий и полю проблемных ситуаций. **Результат:** формируется теоретический подход к системному математическому описанию понятий информационной безопасности. **Практическая значимость:** единый подход к логическому описанию понятий в исследованиях информационной безопасности позволяет достоверно разрешать технические проблемы обеспечения их методами и средствами полезными с точки зрения достижения главной цели - защиты от угроз нарушения информационной безопасности объекта и обеспечения их устойчивого (антикризисного) развития в реально складывающейся и прогнозируемой обстановке XXI века.

Ключевые слова: объект защиты, информационная безопасность, методы и системы моделирования.

Актуальность

На современном этапе одной из актуальных проблем обеспечения безопасного и устойчивого (антикризисного) развития хозяйствующих субъектов является их защищённость от угроз нарушения информационной безопасности (ИБ) с негативными последствиями для личности, общества, государства (ЛОГ) и самих субъектов [1]. Проблема должна решаться в контексте противоборства договаривающихся сторон на политической арене и конкурентной борьбы в социально-эколого-экономическом аспекте в условиях информационной войны (информационно-психологической, идеологической, кибернетической).

В интересах разрешения проблемы необходимо разработать научно-методическое обеспечение программы исследований ИБ приоритетных объектов защиты (ОЗ), заданных доктриной [1], на основе единого алгоритма и единой шкалы оценки защищённости объекта от названных угроз.

С этой целью следует максимально использовать достоинства накопленной базы знаний и ресурса в информационной сфере при сведении к минимуму её недостатков с точки зрения достижения целей. Базу образуют

работы таких ведущих отечественных и зарубежных учёных в информационной сфере, как: Колмогоров А.Н. и Харкевич А.А., Валдайцев С.В., Ефремов В.С. и Саркисян С.А., Бажин И.И., Воробьев О.Ю., Заде Л. и Мазур М., Ансофф И. и Котлер Ф., Дойль П., Стрикленд А. и Томпсон А.А, Скрыль С.В., Киселев В.В., Джоган В.К, других [2-10].

В число приоритетных объектов защиты, согласно Доктрине [1], входят *системы управления экологически опасными и экономически важными производствами. Экономически важными производствами* (объектами) целесообразно считать те из них, которые способны обеспечить: потребности ЛОГ в необходимом и достаточном уровне, качестве и безопасности жизни; их устойчивое антикризисное развитие в новых условиях XXI века. *Экологически опасными* являются те экономически важные производства, которые оказывают на окружающую среду антропогенное воздействие, уровень которого превышает нормы экологической безопасности, создаёт угрозы качеству и безопасности жизни человека и природы.

Методология формирования единого алгоритма

Предпрогнозные исследования современной теории и практики математического моделирования взаимосвязанного развития внешней и внутренней среды ОЗ в интересах обеспечения устойчивости их развития показали следующее [11-16].

1. Методологию разрешения проблемы ИБ приоритетных ОЗ целесообразно строить на основе комплексирования методов теории четких и нечетких множеств, четкой и нечёткой логики, интеллектуальных систем, возможностей и риска, прогнозирования и принятия решений, оптимального управления. Методология должна обеспечить решение задач анализа ситуации и синтеза адекватной реакции на угрозы нарушения устойчивости развития объекта как функции его защищенности от угроз нарушения ИБ с негативными последствиями для ЛОГ.

На современном этапе решение такого класса задач базируется на синтаксическом, семантическом и математическом моделировании взаимосвязанного развития внешней и внутренней среды объектов теоретическими, эвентологическими и эмпирическими методами, представленными в таблице 1 [14, 17].

Методы имеют различное целевое и функциональное назначение, а результаты их применения взаимно дополняют друг друга и базируются на основе применения норм ИБ ОЗ, принимающих следующий вид:

«эталон \pm погрешности (допустимые, критические и/или неприемлемые)» адекватно степени секретности охраняемых сведений, относимых к государственной и/или коммерческой тайне.

Достоверность и полезность таких норм проверяются эмпирически с помощью численных методов. По результатам таких исследований при необходимости вводятся соответствующие корректировки и поправки в теоретические и эвентологические методы моделирования.

Таблица 1 – Комплекс методов моделирования

Классы методов и моделей	Назначение методов и моделей
Теоретические методы	Предназначены для обоснования требований к адекватности реакции на угрозы нарушения ИБ ОЗ, его системы информационной безопасности (СИБ). Моделирование ИБ базируется на внедрении методов системного анализа возможных исходов дуэли между сторонами А и В в заданном контексте, аспектах и условиях с позиции ER концепции (сущности исследуемых событий, отношения между ними, влияющая на них атрибутика) на основе логико-вероятностно-информационного подхода и ветвлении главной цели ОЗ, его СИБ на частные. Результаты такого системного анализа представляют в виде синтаксической модели ИБ ОЗ в виде скобочной конструкции, разработанной по правилу составления формулы Бэкуса-Наура.
Эвентологические методы	Предназначены для учёта влияния человеческого (промахи и ошибки), природного, других объективных и субъективных факторов на ситуацию и результаты (исходы дуэли). Моделирование базируется на методах теории нечётких множеств и нечёткой логики, интеллектуальных систем, возможностей и риска, прогнозирования и принятия решений, оптимального управления.
Эмпирические методы	Предназначены для оценки достоверности и полезности разработанных теоретических основ системного математического моделирования ИБ ОЗ, его СИБ. Моделирование базируется на векторной статистике и численных методах.
Синтаксические модели	Предназначены для выявления <i>сущности</i> реально складывающейся и прогнозируемой обстановки во внешней и внутренней среде объекта защиты в условиях XXI века. Исследования базируются на методах системного анализа, а его <i>результаты</i> оформляются <i>по правилу составления формулы Бэкуса-Наура</i> .
Семантические модели	Предназначены для выявления отношений между сущностями на основе <i>логико-вероятностно-информационного</i> подхода и <i>ветвления</i> главной цели защиты от рассматриваемых угроз (устойчивость развития) на локальные цели, адекватно принятой скобочной конструкции таких отношений
Математические модели	Разрабатываются по методу вложений критериев, методов и систем защиты информации адекватно формуле Бэкуса-Наура с учётом разработанной системы отношений между сущностями условно взаимосвязанного развития внешней и внутренней среды объекта защиты по ситуации и результатам в условиях XXI века.

2. В этом случае общая методология формирования единого алгоритма анализа ИБ объекта и синтеза адекватной реакции на угрозы её нарушения базируется на использовании для моделирования: ER концепции (сущность изучаемых процессов, отношение между ними, влияющая на них атрибутика), логико-вероятностно-информационного подхода к оценке защищенности ОЗ от угроз нарушения его ИБ и ветвления интегральной цели объекта (устойчивость его развития) на частные в заданном контексте, аспектах и условиях [14].

В едином алгоритме предусматривается выполнение следующей последовательности операций [18, 19]:

- моделирование ИБ ОЗ и прогнозирование последствий ее нарушений;
- мониторинг состояний внешней среды и контроль состояний внутренней среды ОЗ;

- диагноз состояний защищенности объекта от нарушений его ИБ, экспертиз состояний на соответствие требуемым, задание требований к эффективности методов и систем информационной безопасности (СИБ) ОЗ;
- оптимизация проектов облика ОЗ, его СИБ и траектории их устойчивого развития по ситуации и результатам в статике и динамике условий XXI века;
- управленческое консультирование по адекватной реакции на угрозы нарушения ИБ ОЗ в статике и динамике условий XXI века;

Реализация такого алгоритма базируется на введении лингвистической переменной, математическая модель которой по определению включает пять факторов, которая используется в теории эвентологии [4]. В нашем случае ими являются следующие.

2.1. Имя интегрального состояния объекта в виде скобочной конструкции: безопасность и устойчивость развития (БУР) ОЗ, как функция его конкурентоспособности (КСП), аргументом которой является качественное информационное обеспечение (ИО), необходимое и достаточное для достижения целей объекта. ИО в условиях информационной войны рассматривается как функция защищённости объекта от угроз нарушения его ИБ. Требования к уровню ИБ устанавливаются исходя из заданных норм защиты охраняемых сведений об объекте, которые относятся к государственной (особой важности, совершенно секретно, секретно) и/или коммерческой («ноу-хау») тайне. При этом на основе принципа обеспечения коллективной безопасности и взаимовыгодного сотрудничества договаривающихся сторон целесообразно учитывать возможность разрешения информационного конфликта (ИК), возникающего между ними из-за противоречий в их интересах. В результате названную выше скобочную конструкцию можно представить в виде аббревиатуры: БУР(КСП(ИО(ИБ(ИК))) ОЗ и его системы информационной безопасности (СИБ). Раскрыть сущности составляющих такой аббревиатуры, отношения между ними и влияющую на них атрибутику (согласно ER концепции) возможно в виде формулы Бэкуса-Наура по известному правилу, $G_{БНФ}$ [14]:

«в левой части указывается нетерминальное слово «имя состояния» ОЗ, его СИБ в рассматриваемой предметной области ::= (по определению есть) далее приводится функционал и/или оператор (алгоритм), который отражает: *сущность* процессов, протекающих в трёхуровневой модели в виде скобочной конструкции БУР(КСП(ИО(ИБ(ИК))) ОЗ, его СИБ; *отношения* между процессами внутри и между уровнями; влияющую на них *атрибутику*»

Другими словами, следуя данному правилу, разрабатывается синтаксическая модель заданной скобочной конструкции БУР(КСП(ИО(ИБ(ИК))) ОЗ, его СИБ. Фактически формула Бэкуса-Наура отражает *алгоритм системного синтаксического моделирования сущности* (то есть логики оценки).

Следует заметить, что данная формула является методом эвентологических системных исследований. Однако, она редко применяется на практике из-за недостаточной разработанности методологии системных исследований по проблеме с позиций логико-вероятностно-информационного подхода [3, 11].

2.2. Полный набор имён в заданном контексте, аспектах и условиях, который образует функционал $X(X_1, X_2, X_3)$. Формирование такого набора имён базируется на методологии [3], предусматривающей: ветвление «целей объекта по способам и средствам их достижения»; фильтрацию тех ветвей, которые близки к оптимальным по ситуации и результатам в статике и динамике условий XXI века; комментирование последствий от реализации различных ветвей по ситуации и результатам.

2.3. Вводятся градации имён возможных состояний объекта внутри предметных областей X_1 (противоборство), X_2 (конкурентная борьба), X_3 (информационная война). Градации образуют классификаторы $T(x) \in X_1$ «И» $T(x) \in X_2$ «И» $T(x) \in X_3$ по основаниям:

- цель, место и время действий, диапазон условий, поле проблемных ситуаций;
- природа и масштабы объекта, сложность его внешних и внутренних структурных связей, детерминированность и цикличность исследуемых процессов в заданном контексте, аспектах и условиях; их ИБ;
- причинно-следственные связи, движущие силы, генеральные цели, законы и закономерности взаимосвязанного развития внешней и внутренней среды ОЗ, его СИБ.

2.4. Правила образования имён, G , в каждой группе исходя из синтаксической модели БУР(КСП(ИО(ИБ(ИК))) ОЗ, его СИБ, следуя правилу $G_{БНФ}$, и на основе разработки семантической модели отношений между состояниями внешней и внутренней среды ОЗ в статике и динамике условий XXI века.

2.5. Правила ассоциирования имён состояний объекта с адекватной реакцией на угрозы нарушения его ИБ, M_{AP} , в заданном контексте, аспектах и условиях. Правила устанавливаются по результатам исследований на математической модели ИБ ОЗ, его СИБ, которая разрабатывается на основе логико (синтаксис)-вероятностно-информационного (семантика) подхода к математическому моделированию взаимосвязанного развития внешней и внутренней среды ОЗ, его СИБ. Методология разработки таких правил базируется на решении выше названных задач анализа и синтеза.

В результате введения лингвистической переменной по пунктам 2.1–2.5 намечился путь системного математического моделирования ИБ объекта с целью адекватной реакции на угрозы её нарушения. Реализация этого пути базируется на следующих предпосылках.

Объект исследований – информационная безопасность объекта защиты.

Предмет исследований – возможность обеспечения ИБ объекта в условиях XXI века.

Цель исследований – создание базы знаний, необходимой и достаточной для информационной и интеллектуальной поддержки требуемого уровня защищённости объекта от угроз нарушения его ИБ в реально складывающейся и прогнозируемой обстановке в статике и динамике условий XXI века [20-22].

Система ограничений на выбор адекватной реакции устанавливается в результате исследований по логической схеме:

- в статике: цель – ситуация – проблема – реакция на неё – побочные эффекты – их предупреждение и ликвидация негативных последствий, в том числе на основе корректировок и пересмотра целей, места и времени действий в заданном контексте, аспектах и условиях;
- в динамике: действие – противодействие – ответные меры и т.д.

В процессе системного моделирования необходимо учитывать также атрибутику, которая существенно влияет на исходы противоборства, конкурентной борьбы и информационной войны. В качестве такой атрибутики рассматриваются: внешняя и внутренняя политики договаривающихся сторон, действующие механизмы государственного регулирования и санкции за нарушения требований нормативно-правовых документов, человеческий и природный факторы, другие объективные и субъективные причины [13].

Задача исследований – создание теоретических основ формирования научно-методического обеспечения программы исследований ИБ приоритетных ОЗ, базирующейся на едином алгоритме и единой шкале оценки защищённости объекта от угроз нарушения его ИБ [23, 24].

Методическое обеспечение формирования единого алгоритма

Следуя принципу максимального использования накопленной базы знаний и ресурса по проблеме, приходим к следующим выводам.

Для научного обоснования правил образования имён состояний объекта G , в рассматриваемой предметной области целесообразно на этапе синтаксического моделирования воспользоваться методами:

- *PEST анализа* (политика, экономика, социум, технологии) в заданном контексте в интересах прогноза исходов противоборства договаривающихся сторон на политической арене и адекватной реакции на них по ситуации и результатам. Здесь состояния экономики, социума и технологий оцениваются по уровням их развития в высокоразвитых, развитых, развивающихся и слаборазвитых странах, согласно грациям, принятым в ООН;
- *SEET анализа* (социум, экология, экономика, технологии) в заданных аспектах в интересах прогноза исходов конкурентной борьбы договаривающихся сторон в социально-эколого-экономической сфере, адекватной реакции на них. Здесь состояния социума, экологии, экономики и технологий рассматриваются применительно к конкретной стране на национальном, корпоративном и местном уровнях;

- *IT (IDEF) технологий* для менеджмента в интересах прогноза исходов информационной войны между договаривающимися сторонами, адекватной реакции на них.

Изучение закономерностей взаимосвязанного развития внешней и внутренней среды ОЗ в этом случае показало, что имя исходов в предметной области целесообразно ассоциировать с адекватными им градациями имён состояний этих сред в заданном контексте, аспектах и условиях, несущих угрозы устойчивости развития объекта, как функции его защищённости от угроз нарушения ИБ (Таблица 2).

Таблица 2 – Градации имен состояний ОЗ

Градации имен состояний ОЗ, его СИБ в вопросах:				
внешней политики	социума	экологии	экономики	технологий
взаимовыгодное сотрудничество	процветание по уровню жизни	гармонизация отношений человека и природы	монополия	абсолютное превосходство в развитии
мирное сосуществование	стабильность общества	антропогенное воздействие на природу	лидерство	лидерство в развитии науки и технологий
нейтралитет	неопределенность	неопределенность	неопределенность	неопределенность
холодные войны	социальная напряженность	превышение норм экологической безопасности	предкризисное состояние	отставание в КСП развития технологий
вооруженные конфликты	социальный взрыв	природные катаклизмы	банкротство, кризис, крах	неразвитость

В результате получены следующие выводы [14]:

- градации исходов противоборства ассоциируются с именами: наличие договорённостей о коллективной безопасности и взаимовыгодном сотрудничестве; мирное сосуществование стран с различным общественным и политическим устройством; «холодные» информационные войны с угрозой их перерастания в военные конфликты;
- градации исходов конкурентной борьбы в экономическом аспекте ассоциируются с монопольным или лидирующим состоянием объекта, его предкризисным состоянием или банкротством, угрозой перерастания локального кризиса в мировой;
- градации исходов конкурентной борьбы в экологическом аспекте ассоциируются с гармонизацией отношений человека с природой или стабильностью таких отношений, которая регулируется нормами

экологической безопасности; антропогенное воздействие человека на природу, превышающее нормы; природные катаклизмы;

- градации исходов конкурентной борьбы в социальной сфере ассоциируются с процветанием социума; наличием гражданского общества, в котором основная масса населения – это счастливые люди, которые «живут как все» (закон «10-80-10»); социальная напряжённость; социальный взрыв, несущий угрозу смены общественного и политического строя в стране. Сказанное иллюстрирует содержание таблицы 3.

Адекватная реакция на выше названные угрозы, согласно федеральному закону [25], ассоциируется с предупреждением ошибок вида упущенная выгода, причинённый ущерб лицами, принимающими решения (ЛПР).

Таблица 3 – Характеристики моделей в области противоборства, конкурентной борьбы, информационной войны

Виды моделей функционала БУР(КСП(...ИБ...))	Характеристики моделей в области			Итог
	противоборства	конкурентной борьбы	Информационной войны	
Синтаксические модели по формуле Бэкуса-Наура	PEST ₁₁ анализ Комплекс имен состояний X_1	SEET ₁₂ анализ Комплекс имен состояний X_2	IT(IDEF) ₁₃ Комплекс имен состояний X_3	Полный набор имен, $X(X_1, X_2, X_3)$
Семантические модели: (иерархические, функциональные, процессные)	SWOT ₂₁ анализ Правила образования имен G_1	SWOT ₂₂ анализ Правила образования имен G_2	SWOT ₂₃ анализ Правила образования имен G_3	Полный набор правил образования имен, $G(G_1, G_2, G_3)$
Математические модели в виде скобочных конструкций функционала БУР(КСП(...ИБ...))	Формула правила ассоциирования имен с целью, M_{AP1} , по формуле Бэкуса-Наура ₃₁	Формула правила ассоциирования имен с целью, M_{AP2} , по формуле Бэкуса-Наура	Формула правила ассоциирования имен с целью, M_{AP3} , по формуле Бэкуса-Наура	Полный набор правил ассоциирования имен с целями M_{AP} ($M_{AP1}, M_{AP2}, M_{AP3}$)
Итог	Комплекс моделей противоборства	Комплекс моделей конкурентной борьбы	Комплекс моделей информационной войны	Система моделей ИБ ОЗ, его СИБ

В этом случае с целью научного обоснования правил ассоциирования имён с адекватной реакцией на угрозы нарушения ИБ объекта, M_{AP} , следует на этапе семантического моделирования воспользоваться методами:

- выявления причинно-следственных связей, движущих сил, генеральных целей, законов и закономерностей взаимосвязанного развития внешней и внутренней среды ОЗ в заданном контексте, аспектах и условиях [26, 27];
- SWOT анализа (сильные и слабые стороны, возможности и угрозы) и диагноза на этой основе состояний защищённости объекта от угроз

нарушения его ИБ, а затем экспертизы установленных состояний на соответствие требуемым. Выявленные диспропорции и результаты их сопоставления с допустимыми, критическими и неприемлемыми – основа для обоснования правил принятия решений по адекватности реакции на угрозы;

- введения системы показателей адекватности: чувствительность к мере информации, функция принадлежности градации состояния объекта к функции его полезности с точки зрения возможности достижения целей его защиты. Такая возможность реализуется на основе: предупреждения промахов и ошибок ЛПР; ликвидации их негативных последствий вида: причинённый ущерб, упущенная выгода, отсутствие необходимой реакции на них в реально складывающейся и прогнозируемой обстановке XXI века.

В результате сущность логико-вероятностно-информационного подхода принимает вид, приведенный в табл. 4.

Таблица 4 – Сущность логико-вероятностно-информационного подхода

Сущности подхода:		
логико	вероятностно	информационного
Синтаксическая модель по формуле Бекуса-Наура (ситуация)	Вероятности достижения целей объекта (семантика и математика)	Критерии оптимизации меры информации, адекватной заданному значению вероятности
Правила образования имен состояний объекта	Диагностика состояний, их экспертиза на соответствие требуемым	Экспертиза потенциально возможной и реально полученной меры информации на соответствие требуемой
Правила ассоциирования имён с адекватностью реакции на угрозы нарушения ИБ ОЗ	Требования к адекватности реакции на угрозы нарушения ИБ ОЗ	Задание на прогноз недостающей и малодостоверной информации

Реализация такого подхода базируется на проведении аналогий между ситуацией и теоремами о вероятности логически связанных событий как функции меры информации: необходимой, потенциально возможной, реально полученной и практически использованной ЛПР. В этом случае критерий оптимизации меры информации, необходимой к практическому использованию для адекватной реакции на угрозы нарушения ИБ объекта принимает следующий вид [14].

Рассматривая выражение БУР(КСП(ИО(ИБ(ИК))) ОЗ в качестве генеральной цели развития объекта, следует провести сравнительный анализ следующих количественно-качественных логико-вероятностно-информационных характеристик:

- необходимо (H) обеспечить состояние (требуемое имя) ::= (по определению есть) его количественно-качественные характеристики по форме: область их определения, $\Omega_{ГЦ}^{(H)}$, заданная для оценки

вероятности достижения генеральной цели объекта, $P_{ГЦ}^{(H)}$, аргументом которой является область определения необходимой и достаточной меры исходной информации, $M(I_{ГЦ}^{(H)})$:

$$\text{Имя состояния} ::= P_{ГЦ}^{(H)}(M(I_{ГЦ}^{(H)})) \in \Omega_{ГЦ}^{(H)}; \quad (1)$$

- «И» потенциальных возможностей (ПВ) при накопленной в мире базе знаний и ресурса по проблеме:

$$ПВ ::= P_{ГЦ}^{(ПВ)}(M(I_{ГЦ}^{(ПВ)})) \in \Omega_{ГЦ}^{(ПВ)}; \quad (2)$$

- «И» реальная достижимость цели (РД) при имеющейся у объекта базе знаний и ресурса по проблеме ::= функция принадлежности способов и средств достижения цели $\mu_{ГЦ}^{(РД)}$, к функции их полезности в рассматриваемых контексте, аспектах и условиях:

$$РД ::= \mu_{ГЦ}^{(РД)} \in P_{ГЦ}^{(РД)}(M(I_{ГЦ}^{(РД)})) \in \Omega_{ГЦ}^{(РД)}. \quad (3)$$

Мера информации в выражениях (1)–(3) распознаётся на основе проведения аналогий между теоремами о вероятностях логически связанных событий и теоремами о мере информации (по ситуации), необходимой, потенциально возможной, реально полученной и практически использованной по ситуации и результатам для адекватной реакции на угрозы нарушения ИБ ОЗ. При наличии диспропорций между названными мерами: выявляются объективные и субъективные причины их появления; оценивается приемлемость последствий, вызванных установленными диспропорциями; принимаются адекватные меры по предупреждению порождающих их причин, ликвидации негативных последствий.

Заключение

Таким образом, системное математическое моделирование ИБ ОЗ, его СИБ базируется на эффективном решении задач анализа ситуации и синтеза адекватной реакции на неё [14, 28]. Системообразующим фактором является процедура, которая базируется на ER концепции и усовершенствованном логико-вероятностно-информационном подходе к исследованиям, включает операции: ветвления целей объекта по средствам их достижения; фильтрации ветвей, близких к оптимальным по ситуации и результатам; управленческое консультирование по проблеме. Фактор реализуется с помощью аналогий, ассоциаций и асимптотического приближения практически используемой «И» реально достижимой «И» потенциально возможной меры информации к необходимой. Математическая модель такого процесса базируется на применении теорем о вероятностях логически связанных событий в статике, Байеса, принципа Беллмана и метода динамического программирования в динамике условий XXI века.

В результате формируются теоретические основы системного математического моделирования ИБ ОЗ как аргумента его устойчивого развития в условиях XXI века.

Литература

1. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 9 сентября 2000 г., № Пр-1895. URL: <http://www.scrf.gov.ru/documents/6/5.html> (дата обращения 30.01.2016).
2. Валдайцев С. В. Антикризисное управление на основе инноваций: учеб. пособие. – СПб.: Изд-во С.-Петербур. ун-та, 2001. – 232 с.
3. Саркисян С. А., Лисичкин В. А., Минаев Э. С., Каспин В. И., Пасенчник Г. С. Теория прогнозирования и принятия решений. – М.: Высшая школа, 1977. 351 с.
4. Воробьев О. Ю. Эвентология. – Красноярск: СФУ, 2007. 434 с.
5. Ефремов В. С. Стратегическое планирование в бизнес-системах. – М.: Финпресс, 2001. 240 с.
6. Бажин И. И. Информационные системы менеджмента. – М.: ГУ-ВШЕ, 2000. 688 с.
7. Заде Л. А. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. 167 с.
8. Мазур М. Качественная теория информации. – М.: Мир, 1974. 326 с.
9. Харкевич А. А. О ценности информации // Проблемы кибернетики. 1960. № 4. С. 53-57.
10. Скрыль С. В., Киселев В. В., Джоган В. К., Багаев М. А., Финько В. Н., Шимон Н. С., Хаустов С. Н., Мещеякова Т. В. Распознавание и оценка угроз информационной безопасности территориальным сегментам Интегрированной мультисервисной телекоммуникационной системы органов внутренних дел: теоретические и организационно-методические основы: монография. – Воронеж: Воронежский институт МВД России, 2012. 134 с.
11. Жидко Е. А. Методология системного математического моделирования информационной безопасности // Интернет-журнал Науковедение. 2014. № 3 (22). URL: <http://naukovedenie.ru/PDF/67TVN314.pdf> (дата обращения 27.01.2016).
12. Жидко Е. А., Попова Л. Г. Методологические основы обеспечения информационной безопасности инновационных объектов // Информация и безопасность. 2012. Т. 15. № 3. С. 369-376.
13. Жидко Е. А. Методические основы системного моделирования информационной безопасности // Интернет-журнал Науковедение. 2014. № 3. URL: <http://naukovedenie.ru/PDF/68TVN314.pdf> (дата обращения 27.01.2016).
14. Жидко Е. А. Методология исследований информационной безопасности экологически опасных и экономически важных объектов: монография. – Воронеж: ВГАСУ, 2015. 180 с.
15. Сазонова С. А. Решение задач обнаружения утечек систем газоснабжения и обеспечение их безопасности на основе методов математической статистики // Вестник Воронежского института высоких технологий. 2015. № 14. С. 51-55.
16. Сазонова С. А. Информационная система проверки двухальтернативной гипотезы при диагностике утечек и обеспечении

безопасности систем газоснабжения // Вестник Воронежского института высоких технологий. 2015. № 14. С. 56-59.

17. Жидко Е. А. Методология формирования единого алгоритма исследований информационной безопасности // Вестник Воронежского института МВД России. 2015. № 1. С. 62-69.

18. Жидко Е. А. Научно-обоснованный подход к классификации угроз информационной безопасности // Информационные системы и технологии. 2015. № 1 (87). С. 132-139.

19. Жидко Е. А., Попова Л. Г. Логико-вероятностно-информационное моделирование информационной безопасности // Вестник Казанского государственного технического университета им. А.Н. Туполева. 2014. № 4. С. 136-140.

20. Жидко Е. А. Высокие интеллектуальные и информационные технологии интегрированного менеджмента XXI века: монография. Изд-во ВУНЦ ВВС ВВА имени профессора Н. Е. Жуковского и Ю. А. Гагарина. Воронеж, 2013. 76 с.

21. Барковская С. В., Жидко Е. А., Попова Л. Г. Высокие интеллектуальные технологии интегрированного менеджмента XXI века // Вестник Воронежского государственного технического университета. 2010. Т. 6. № 9. С. 28-32.

22. Жидко Е. А., Попова Л. Г. Информационная и интеллектуальная поддержка управления развитием социально-экономических систем // Вестник Иркутского государственного технического университета. 2014. № 10 (93). С. 12-19.

23. Жидко Е. А. Методология формирования системы измерительных шкал и норм информационной безопасности объекта защиты // Вестник Иркутского государственного технического университета. 2015. № 2 (97). С. 17-22.

24. Жидко Е. А., Кирьянов В. К. Формирование системы координат и измерительных шкал для оценки состояний безопасного и устойчивого развития хозяйствующих субъектов // Научный журнал. Инженерные системы и сооружения. 2014. № 1 (14). С. 60-68.

25. Гражданский кодекс РФ. (В редакции Федерального закона от 21 июля 2014 г. № 222-ФЗ). URL: <http://1gkrf.ru> (дата обращения 30.01.2016).

26. Жидко Е. А., Попова Л. Г. Концепция системного математического моделирования информационной безопасности // Интернет-журнал Науковедение. 2014. № 2 (21). URL: <http://naukovedenie.ru/PDF/157EVDN214.pdf> (дата обращения 30.01.2016).

27. Жидко Е. А., Попова Л. Г. Принципы системного математического моделирования информационной безопасности // Интернет-журнал Науковедение. 2014. № 2 (21). URL: <http://naukovedenie.ru/PDF/169EVDN214.pdf> (дата обращения 30.01.2016).

28. Сазонова С. А. Обеспечение безопасности функционирования систем газоснабжения при реализации алгоритма диагностики утечек без учета помех от стохастичности потребления // Вестник Воронежского института высоких технологий. 2015. № 14. С. 60-64.

References

1. *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii: utverzhdena Prezidentom RF 9 sentiabria 2000 g, № Pr-1895* [The Doctrine of Information Security of the Russian Federation: approved by The President of the Russian Federation on 9 September 2000. No. PR-1895]. Available at: <http://www.scrf.gov.ru/documents/6/5.html> (accessed 30 January 2016) (in Russian).
2. Valdaitsev S. V. *Antikrizisnoye upravleniye na osnove innovatsiy*. [Anti-crisis management through innovation]. Saint-Petersburg, St. Petersburg. University Publ., 2001. 232 p. (in Russian).
3. Sarkisian S. A., Lisichkin V. A., Minaev E. S., Kaspin V. I., Pasenchnik G. S. *Teorija prognozirovaniya i prinjatija resheniy*. [The Theory of Forecasting and Decision Making]. Moscow, Vysshaya Shkola Publ., 1977. 351 p. (in Russian).
4. Vorobyev O. Y. *Eventologiya* [Eventology]. Krasnoyarsk, SibFU Publ., 2007. 434 p. (in Russian).
5. Efremov V. S. *Strategicheskoye planirovaniye v biznes-sistemah* [Strategic Planning in Business Systems]. Moscow, Finpress Publ., 2001. 240 p. (in Russian).
6. Bazhin I. I. *Informacionnyye sistemy menedjmenta* [Information Systems Management]. Moscow, Higher School of Economics – National Research University Publ., 2000. 688 p. (in Russian).
7. Zade L. A. *Ponjatiye lingvisticheskoy peremennoy i yego primeneniye k prinjatiyu priblizhennykh resheniy* [The Concept of a Linguistic Variable and its Application to Approximate Reasoning]. Moscow, Mir Publ., 1976. 167 p. (in Russian).
8. Mazur M. *Kachestvennaya teorija informacii* [Qualitative Theory of Information]. Moscow, Mir Publ., 1974. 326 p. (in Russian).
9. Kharkevich A. A. About the value of information. *Problemy kibernetiki*, 1960, no. 4, pp. 53-57 (in Russian).
10. Skryl S. V., Kiselev V. V., Johan V., Bagaev M. A., Finko V. N., Shimon N. S., Khaustov S. N., Meshcheryakova T. V. *Raspoznavaniye i ocenka ugroz informatsionnoi bezopasnosti territorialnym segmentom integrirovannoy multiservesnoy telekommunikacionnoy sistemy organov vnutrennih del* [Recognition and Assessment of Information Security Threats to Territorial Segments of Integrated Multi-Service Telecommunication System of Internal Affairs of Russian Federation. Theoretical, organizational and methodological foundations]. Voronezh, Voronezh Institute of the Ministry of internal Affairs of Russia Publ., 2012. 134 p. (in Russian).
11. Zhidko E. A. The methodology of the system of mathematical modeling of information security. *Naukovedenie*, 2014, vol. 22, no. 3. Available at: <http://naukovedenie.ru/PDF/67TVN314.pdf> (accessed 27 January 2016) (in Russian).

12. Zhidko E. A., Popova L. G. Methodological foundations of information security innovation of information security. *Information and security*, 2012, vol. 15, no. 3, pp. 369-376 (in Russian).

13. Zhidko E. A. Methodological foundations of systems modeling of information security. *Naukovedenie*, 2014, vol. 22, no. 3. Available at: <http://naukovedenie.ru/PDF/68TVN314.pdf> (accessed 27 January 2016) (in Russian).

14. Zhidko E. A. *Metodologija issledovaniy informacionnoy bezopasnosti ekologicheski opasnyh i ekonomicheski vazhnyh obektov* [Methodology of Research of Information Security of Environmentally Hazardous and Economically Important Objects]. Voronezh, Voronezh State University of Architecture and Civil Engineering Publ., 2015. 183 p (in Russian).

15. Sazonova S. A. The Solution of Problems of Leak Detection Systems Gas Supply and Security on the Basis of Methods of Mathematical Statistics. *Vestnik Voronezhskogo instituta vysokikh tekhnologii*, 2015, no. 14, pp. 51-55 (in Russian).

16. Sazonova S. A. The Information System Checks Dualtime Alternative Hypotheses when Diagnosing Leaks and Providing Security of Gas Supply Systems. *Vestnik Voronezhskogo instituta vysokikh tekhnologii*, 2015, no. 14, pp. 56-59 (in Russian).

17. Zhidko E. A. The methodology of Forming a Single Algorithm Information Security Research. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia*, 2015, no 1, pp. 62-69 (in Russian).

18. Zhidko E. A. Research-based Approach to the Classification of Threats to Information Security. *Information systems and technologies*, 2015, vol. 87, no. 1, pp. 132-139 (in Russian).

19. Zhidko E. A., Popova L. G. Logical-and-Probabilistic-Informational Modeling of Information Security. *Vestnik KGTU im. A.N. Tupoleva*, 2014, no. 4, pp. 136-140 (in Russian).

20. Zhidko E. A. *Vysokiye intrllectualnyje I informacionnyje tehnologii integrirovannogo menedgmenta XXIveka* [High Intellectual and Information Technologies Integrated Management of XXI Century]. Voronezh, Voenno-vozdushnaia akademiia im. professora N. E. Zhukovskogo i Iu. A. Gagarina Publ., 2013. 76 p. (in Russian).

21. Barkovskaya S V., Zhidko E. A., Popova L. G. High intellectual technologies of integrated management of the XXI century. *The Bulletin of Voronezh State Technical University*, 2010, vol. 6, no. 9, pp. 28-32 (in Russia).

22. Zhidko E. A., Popova L. G. Information and Intellectual Support of Management of Development of Socio-Economic Systems. *Bulletin of Irkutsk State Technical University*, 2014, vol. 93, no 10, pp. 12-19 (in Russian).

23. Zhidko E. A. Formation Methodology for the System of Protected Object Measuring Scales and Information Security Standards. *Bulletin of Irkutsk State Technical University*, 2015, vol.97, no. 2, pp. 17-22 (in Russian).

24. Zhidko E. A., Kiryanov V. K. Formirovanie sistemy koordinat i izmeritel'nykh shkal dlia otsenki sostoianii bezopasnogo i ustoichivogo razvitiia khoziaistvuiushchikh sub"ektov [The Formation of coordinate systems and measuring scales for the assessment of safe and sustainable development of economic entities]. *Engineering systems and constructions*, 2014, vol. 14, no. 1, pp. 60-68 (in Russian).

25. The Civil Code of the Russian Federation. (As Amended by Federal Law of July 21, 2014 No. 222-FZ). Available at: URL: <http://1gkrf.ru> (accessed 27 January 2016) (in Russian).

26. Zhidko E. A., Popova L. G. The Concept of Systematic Mathematical Modelling Information Security. *Naukovedenie*, 2014, vol. 21, no. 2. Available at: <http://naukovedenie.ru/PDF/157EVN214.pdf> (accessed 27 January 2016) (in Russian).

27. Zhidko E. A., Popova L. G. The principles of the system of mathematical modeling of information security. *Naukovedenie*, 2014, vol. 21, no. 2 Available at: URL: <http://naukovedenie.ru/PDF/169EVN214.pdf> (дата обращения 30.01.2016).

28. Sazonova S. A. The security of functioning of systems of gas supply during the implementation of the algorithm for the diagnosis of leakage without taking into account interference from the stochasticity of consumption . *Vestnik Voronezhskogo instituta vysokikh tekhnologii*, 2015, no. 14, pp. 60-64 (in Russian).

Статья поступила 29 декабря 2015 г.

Информация об авторе

Жидко Елена Александровна – кандидат технических наук, доцент. Профессор кафедры пожарной и промышленной безопасности. Воронежский государственный архитектурно-строительный университет. Область научных интересов: проблема обеспечения безопасного и устойчивого (антикризисного) развития хозяйствующих субъектов, как функции их конкурентоспособности. В качестве аргумента конкурентоспособности рассматривается экологическая и информационная безопасность этих субъектов. Тел.: +7 910 345 46 13. E-mail: lenag66@mail.ru

Адрес: 394006, Россия, г. Воронеж, ул.20-летия Октября, д.84.

Logical-and-probabilistic-informational approach to the formation of a unified algorithm of research of information security protection

E. A. Zhidko

Problem statement: in the doctrine of information security of the Russian Federation have shown shortcomings in its provision at the present stage. One of them is: "the inconsistency and poor legal

*regulation of social relations in the information sphere, which leads to serious negative consequences for the individual, society, state. **The aim of this** is the ability to create a single logical approach to the research of information security of the object of protection in the presence of threats of violations with unacceptable consequences. **Methods used:** the methodology of research on the problem form methods of attachment, analogies, associations and asymptotic approximations of the theoretical and effective linguistic, semantic, mathematical modeling methods, which are based on a combination of modeling methods by the formula Backus-Naur form. **Novelty:** the formation of a unified approach in terms of information security of object is based on syntactic, semantic and mathematical modeling of conventionally interconnected development of the external and internal environment of object theoretical event logical and empirical methods, coordinated by objective, place and time, the range of field conditions and problematic situations. **Result:** formed a theoretical approach to the system mathematical description of the concepts of information security. **Practical relevance** a unified approach to the logical description of concepts in the research of information security can reliably solve the technical problem of providing methods and means useful from the point of view of achieving the main goal - protection from threats of violation of information security of the object and sustained (anti-crisis) development in shaping and projected environment of the twenty-first century.*

***Keywords:** object protection, information security, methods and systems modeling.*

Information about Author

Elena Aleksandrovna Zhidko – Ph.D. of Engineering Sciences, Associate Professor. Professor of the Department of Fire and Industrial Safety. Voronezh State University of Architecture and Construction. Field of research: the problem of providing safe and sustainable (anti-crisis) development of economic entities, as a function of their competitiveness. As the argument of the competitiveness of the ecological and information security of these subjects. Tel.: +7 910 345 46 13. E-mail: lenag66@mail.ru

Address: Russia, 394006, Voronezh, St. 20th anniversary of October, d. 84.