УДК 338.2

Жидко Елена Александровна
ФГБОУ ВПО «Воронежский государственный архитектурно-строительный университет»
Россия, Воронеж[1]
Профессор кафедры пожарной и промышленной безопасности
Кандидат технических наук, доцент
E-Mail: lenag66@mail.ru

Попова Лариса Георгиевна
ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)
Россия, Воронеж
Старший научный сотрудник, доктор технических наук
E-Mail: Larisa.popova.38@mail.ru

Концепция системного математического моделирования информационной безопасности

Аннотация: На современном этапе одной из актуальных проблем безопасного и устойчивого (антикризисного) развития Российской Федерации является обеспечение её информационной безопасности в новых условиях XXI века. В результате оценки состояния вопроса в доктрине сделаны выводы о наличии противоречий в нормативно-правовой базе информационной безопасности объектов защиты, её несовершенстве, а также об отставании в уровне развития отечественных информационных технологий от уровня, достигнутого в мире.

В статье сформирована обобщённая система взглядов (утверждения 1 – 12) на путь разрешения проблемы информационной безопасности объектов защиты в контексте: безопасность и устойчивость развития как функция его информационного обеспечения, аргументом которого является защищённость объекта от угроз нарушения информационной безопасности. При изучении последней предлагается учитывать факторы, которые активно и существенно влияют на информационную безопасность (человеческий и природный, несовершенство научно-методического обеспечения, возможности и угрозы разрешения информационного конфликта).

Разработанная обобщённая система взглядов базируется на выполнении требований национального пакета нормативно-правовых документов по информационной безопасности РФ, на современном подходе к исследованиям по проблеме, учитывает влияние на постановку и решение задач политик интеграции РФ в мирохозяйственные связи и глобализации экономики, внедрение в ней модели государственно регулируемой инновационной экономики.

Ключевые слова: Информационная безопасность; нормативно-правовая база; устойчивость развития; защищенность; мера информации; информационной обеспечение; концепция.

Идентификационный номер статьи в журнале 157EVN214

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

На современном этапе, научные исследования по любой проблеме, как правило, базируются на парадигме, включающей концепцию, принципы и методологию. По определению концепция (в переводе с латинского «понимание») это обобщённая система взглядов на изучаемые объекты и явления, то есть представление о том, как надо подходить к их восприятию и изучению.

С этих позиций сформулируем основные теоретические положения парадигмы безопасного и устойчивого (антикризисного) развития хозяйствующих субъектов Российской Федерации как функции его информационного обеспечения в реально складывающейся и прогнозируемой обстановке XXI века.

Предпрогнозные исследования [6] показали, что информационное обеспечение устойчивости развития хозяйствующих субъектов должно осуществляться с учётом политики интеграции Российской Федерации в мирохозяйственные связи и глобализации экономики, перехода на модель государственно регулируемой социальной инновационной экономики. Как показывает опыт, реализация такой политики и модели сталкивается с противоречиями в интересах сторон (т.е. отдельных стран, их интеграционных блоков и хозяйствующих субъектов), договаривающихся о коллективной безопасности и взаимовыгодном сотрудничестве. Разрешение противоречий базируется на приоритетах собственных интересов каждой стороны, дополняется их состязательностью в конкурентоспособности, сопровождается информационной («холодной») войной между ними. Она охватывает идеологическую, информационно-психологическую и кибернетическую сферы, сопровождается информационными конфликтами между сторонами. Основными способами ведения информационной войны являются хищения, разрушения и модификация информации, циркулирующей во внешней и внутренней среде хозяйствующих субъектов. В результате появляются угрозы дезинформации, утраты и/или искажения информационного обеспечения, необходимого и достаточного для достижения и сохранения устойчивого развития субъекта. Такие угрозы рассматриваются как нарушение его информационной безопасности с негативными последствиями для внешней и внутренней среды. Ими могут стать локальные кризисы и военные конфликты с угрозой их перерастания в мировые [6,7].

Известно, что в рассматриваемых условиях меры по разрешению конфликтов мирным путём носят информационно-консенсусный характер и базируются на согласовании интересов договаривающихся сторон, формировании общих для них деловых сетей, а также обмене информацией, имеющейся в распоряжении этих сторон. При положительном исходе таких мер требования к их защищённости от угроз нарушения информационной безопасности уменьшаются. Поэтому информационную безопасность целесообразно рассматривать как функцию информационного конфликта.

Особенность развития таких процессов в реально складывающейся и прогнозируемой обстановке усугубляется неравномерностью развития отдельных стран, их интеграционных блоков и хозяйствующих субъектов. Согласно градациям, принятым в ООН, выделяют страны высокоразвитые и развитые, переходного периода, развивающиеся и слаборазвитые. Это создаёт дополнительные проблемы интеграции стран в мирохозяйственные связи, как показано в [6,7]. Например. Высокоразвитые и развитые страны стремятся поглотить развивающиеся и слаборазвитые. Те, понимая негативные последствия для себя таких угроз, предпринимают меры по их предупреждению и ликвидации. Сущность таких мер и их последствий для нападающей стороны вызывает у неё опасения из-за реальной угрозы потерять свои вложения в партнёров, ничего не получив взамен.

С целью достижения и сохранения безопасного и устойчивого развития мирового сообщества на основе координации действий его членов требования к информационному обеспечению изложены [12] в Повестке дня ООН на XXI век, теории и практике маркетинга

менеджмента XXI века, исследованиях мирового рынка (прогнозирование, проектирование, планирование, управление и координация). Такие требования приводятся в виде перечня сведений, необходимых и достаточных для своевременного принятия правильных управленческих решений в различных областях деятельности хозяйствующих субъектов. Анализ накопленной базы знаний по методологии и нормативно-правовому обеспечению устойчивости развития [8,9] позволяет конкретизировать названные перечни сведений, классифицировать их по целевому и функциональному назначению, ввести понятие меры информации.

Под мерой информации будем понимать количественные и качественные характеристики перечня сведений требуемого целевого и функционального назначения, операции над которыми позволяют установить имя состояния устойчивости объекта, его логико-вероятностно-информационные характеристики в контексте ER концепции (сущности событий и явлений, отношения между ними, влияющая на них атрибутика).

С учётом вышесказанного приходим к следующим концептуальным выводам.

Утверждение 1. Безопасность и устойчивость развития хозяйствующего субъекта это функция его информационного обеспечения, аргументом которой является защищённость субъекта от угроз нарушения его информационной безопасности.

Утверждение 2. Требования по информационной безопасности, способам и средствам их обеспечения существенно зависят от возможностей разрешения информационного конфликта между договаривающимися сторонами в реально складывающейся и прогнозируемой обстановке XXI века.

Утверждение 3. С целью количественно-качественной оценки состояния устойчивости целесообразно ввести их градации в контексте *ER*концепции с позиции логико-вероятностно-информационного подхода на основе системного математического моделирования взаимосвязанного развития внешней и внутренней среды объекта защиты, численных методов ведения исследований на моделях, их автоматизации.

Утверждение 4. Согласно основным положениям теории интеллектуальных систем, физические и юридические лица, принимающие решения по реакции на угрозы нарушения информационной безопасности объекта, должны воспринимать и пониматьсущность происходящих событий, уметь мыслить, т.е. анализировать степень опасности угроз и их последствий, синтезировать эффективные меры по предупреждению таких угроз, ликвидации их негативных последствий.

Утверждение 5. Реализация положений, высказанных выше, существенно зависит от осведомленности названных лиц о реально складывающейся и прогнозируемой обстановке, их интеллектуального потенциала и мотивации с учётом влияния на них действующих механизмов регулирования и санкций по предупреждению противоправных действий.

В свете принятых утверждений основные положения концепции системного математического моделирования информационной безопасности вытекают из требований действующих нормативно-правовых документов по информационной безопасности Российской Федерации [4,10,11].

Согласно Доктрине [4], под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Под сбалансированностью интересов будем понимать такое соотношение информированности личности, общества, государства о результатах принимаемых ими

решений и политик, проводимых в различных сферах деятельности, которая гарантирует формирование гражданского общества в России, её безопасное и устойчивое (антикризисное) развитие в реально складывающейся и прогнозируемой обстановке XXI века.

Согласно сложившейся мировой практике, формирование гражданского общества отвечает закону «10 – 80 – 10». Это значит, что:

- 80% населения находятся на разумно достаточном уровне, качестве и безопасности жизни;
- 10% населения оказываются на минимально необходимом уровне жизни и ниже, т.е. за гранью выживания;
- 10% населения достигают элитного уровня жизни.

Нарушение таких соотношений грозит дестабилизацией общества, создаёт угрозу социального взрыва, его трансформации в революции, гражданские войны, государственные перевороты.

Отсюда цель защиты РФ, её хозяйствующих субъектов от угроз нарушения их информационной безопасности – достижение и сохранение требуемого уровня безопасности и устойчивости развития.

Путьдостижения цели – предупреждение причин, порождающих внешние и внутренние угрозы нарушения устойчивости с неприемлемыми последствиями для личности, общества, государства, своевременная ликвидация таких последствий.

В интересах достижения цели намеченным путём в Доктрине заданы приоритетные объекты защиты и первоочередные задачи по обеспечению ихинформационной безопасности, установлены виды и источники угроз её нарушения, дана оценка состояния вопроса на начало XXI века, отмечены основные недостатки накопленной базы знаний и ресурса по информационной безопасности. В ней также приведены основные положения государственной информационной политики, направления создания и развития нормативно-правовой базы по её реализации.

В результате их изучения можно сделать следующие общие выводы.

Проблема информационной безопасностиРоссийской Федерации и её хозяйствующих субъектов состоит в том, что её необходимо обеспечить в:

- контексте достижения и сохранения требуемого уровня безопасного и устойчивого (антикризисного) развития объектов защиты как функции его информационной обеспеченности. Её аргументом является информационная безопасность объектов как функция информационного конфликта между договаривающимися сторонами;
- аспектах: политическом, нормативно-правовом, социально-эколого-экономическом, технологическом и информационном с учётом существенного влияния на них человеческого, природного, других объективных и субъективных факторов;
- условиях информационной войны между договаривающимися сторонами в реально складывающейся и прогнозируемой обстановке XXI века на международном, межстрановом, внутристрановом и корпоративном уровнях (отрасль, подотрасль, предприятие) в названном контексте и аспектах.

Это сложная многоцелевая, многоразмерная и многофакторная задача, которая имеет многоальтернативные решения [саркесян]. Постановка и решение таких задач должно осуществляться в условиях неопределённости, ограниченного ресурса, выявленных недостатков накопленной база знаний [4,5,7], в том числе:

- противоречивость и несовершенство нормативно-правовой базы;
- отставание от мирового уровня развития образования науки, техники и информационных технологий;
- несовершенство системы сквозной подготовки специалистов (среднее профессиональное образование, высшее профессиональное образование, научные кадры) в области информационной безопасности.

Предпрогнозные исследования сложившегося положения показали [4,5]:

- причиной возникновения противоречивости и несовершенства нормативно-правовой базы являются промахи и ошибки, которые возникли в процессе математического моделирования взаимосвязанного развития внешней и внутренней среды приоритетных объектов защиты;
- причиной отставания в развитии информационных технологий явилась сложившаяся на ретроспективном периоде практика асимптотического приближения необходимого и потенциально возможного к реально достижимому, а не наоборот;
- причиной несовершенства сквозного образования по проблеме информационной безопасности является тот факт, что научно-методическое обеспечение антикризисного управления ориентировано на режим реального и близкого к нему масштабу времени и/или на краткосрочный период (1 – 3 года); в расчётах принимаются реально имеющиеся материальные ресурсы и практически игнорируются интеллектуальные.

В такой ситуации реализация названного пути достижения цели защиты возможна в результате устранения названных причин, ликвидации их негативных последствий. Согласно требованиям Доктрины [4], это необходимо для создания научно-методического обеспечения подготовки специалистов по информационной безопасности в рамках Единой системы сквозного образования по проблеме.

Главная задача на этом пути разработка новых:

- математических методов моделирования объектов и явлений, порождающих выше названные угрозы;
- математических методов и алгоритмов проверки адекватности математических моделей объектов на основе данных натурного эксперимента;
- реализация эффективных численных методов и алгоритмов в виде комплексов проблемно-ориентированных программ для проведения вычислительного эксперимента.

На постановке и решении таких задач должна базироваться теория и методология обеспечения информационной безопасности и защиты информации. В свою очередь, такая теория и методология должны стать основой для системного анализа, оптимизации,

управления, принятия решений и обработки информации. Для его реализации необходимо располагать:

- методами и алгоритмами прогнозирования и оценки эффективности, качества и надежности сложных систем, которые базируются на идентификации систем управления на основе ретроспективной, текущей и экспертной информации, а также на интеллектуальной поддержке управления;
- методами и алгоритмами анализа и синтеза организационных структур, проблемно-ориентированных систем управления, принятия решений и оптимизации экономических и социальных систем.
- новыми информационными технологиями в решении задач управления и принятия решений в социальных и экономических системах.

Отличительной чертой такого системного анализа является необходимость учета существенного активного влияния человеческого фактора на процесс управления. Кроме того, согласно Доктрине [4], при решении задач противодействия иностранным техническим разведкам необходимо учитывать влияние природного, других объективных и субъективных факторов.

К объективным факторам по И.Ансоффу [1] будем относить потенциально возможный уровень осведомлённости лиц (физических и юридических), принимающих решения о возможных изменениях состояний внешней и внутренней среды объекта защиты. К субъективным – влияние осведомлённости, интеллектуального потенциала и мотивации таких лиц на адекватность принимаемых ими решений по защите объекта от угроз нарушения его информационной безопасности с негативными последствиями для личности, общества, государства. Согласно теории интеллектуальных систем [15], такой потенциал определяется способностью названных лиц воспринимать и понимать сущность событий, происходящих во внешней и внутренней среде объекта защиты, умение мыслить с позиций ER концепции (сущности, отношения между ними, влияющая на них атрибутика). Под атрибутикой будем понимать механизмы регулирования и санкции, предназначенные для предупреждения противозаконных действий лиц, принимающих решения.

Утверждение 6. С позиций логико-вероятностно-информационного подхода адекватность реакции на угрозы нарушения информационной безопасности объектов защиты целесообразно оценивать по критерию: необходимо и потенциально возможно и реально достижимо по ситуации и результатам в реально складывающейся и прогнозируемой обстановке XXI века.

Утверждение 7. Нормы на область определения количественных и качественных характеристик адекватной реакции целесообразно устанавливать по критерию: *имя состояния устойчивости* развития объекта ::= (т.е. по определению равно*) градации лингвистической переменной при допустимых, критических и/или неприемлемых информационных рисках, их последствиях* (т.е. эталонные значения области определения и погрешности её измерения).

Утверждение 8. Методология принятия решений об адекватности реакции должна базироваться на распознавании ситуации и прогнозе последствий внедрения решений, а также оценке их приемлемости для личности, общества, государства в краткосрочном (1 – 3 года), среднесрочном (5 – 10 лет) и долгосрочном (15 – 20 лет и более) периодах XXI века. Правила принятия решений целесообразно строить на основе построения приоритетного ряда их альтернативных вариантов, выбора оптимальных и близких к ним решений по ситуации и результатам в статике и динамике условий XXI века.

Утверждение 9. С целью восполнения недостающей исходной информации, повышения достоверности и точности прогнозов, обеспечения своевременности принятия адекватных решений, их количественной и качественной обоснованности необходимо и достаточно разработать систему математических моделей информационной безопасности объекта защиты теоретическими, эмпирическими и эвентологическими методами, предусмотреть верификацию результатов исследований на таких моделях.

Утверждение 10. С целью введения градации имён состояний на основе нормирования области определения их качественных и количественных характеристик необходимо ввести систему координат и измерительных шкал как инструментарий исследований на математических моделях информационной безопасности объекта защиты.

Утверждение 11. Особенность реализации приведенных положений на современном этапе состоит в том, что:

- накопленная база знаний и ресурса по проблеме системного математического моделирования информационной безопасности обладает целым рядом недостатков, отмеченных в Доктрине [4] и Политике информационной безопасности компаний [3], их нормативно-правовом обеспечении (противоречивость, несовершенство, отставание в уровне развития от достигнутого в мире уровня и тенденций развития образования, науки, техники и технологий по проблеме);

- практически отсутствуют теоретические основы системного математического моделирования информационной безопасности [2], которое базируется на глобальной оптимизации способов и средств защиты информации в заданном контексте, аспектах и условиях;

- недостаточно разработано научно-методическое и научно-практическое обеспечение Программы исследований информационной безопасности объекта защиты, необходимое и достаточное для количественного и качественного обоснования перечня охраняемых сведений об объекте, которые составляют государственную и/или коммерческую тайны [14].

С целью универсализации и автоматизации исследований усовершенствованная программа должна базироваться на едином алгоритме и единой шкале оценки защищённости объекта.

Утверждение 12. В процессе исследований, направленных на устранение указанных недостатков, необходимо учитывать иерархическую структуру пакета нормативно-правовых документов по информационной безопасности [10]. Предпрогнозные исследования показали следующее.

Иерархия структуры по вертикали устанавливает, с одной стороны, требования по делегированию функций (спуск) в области информационной безопасности от общенационального уровня к отраслевому и корпоративному, а, с другой стороны, осуществляется контроль результатов исполнения этих функций (подъём). Экспертиза результатов на соответствие требуемым для достижения и сохранения необходимого и достаточного уровня национальной безопасности Российской Федерации позволяет установить диспропорции между необходимым, потенциально возможным и реально достижимым на каждом уровне и в целом (интегральный эффект). После чего прогнозируется приемлемость последствий таких диспропорций с позиций «допустимые, критические, неприемлемые» в реальном и близком к нему масштабе времени, в краткосрочном, среднесрочном и долгосрочном периодах. Это даёт основу для оперативных и стратегических

решений по управлению информационной безопасностью объекта защиты в реально складывающейся и прогнозируемой обстановке XXI века.

Иерархию структуры документов по горизонтали на каждом уровне по вертикали образуют федеральные законы, стандарты и нормы, адекватные им внутренние системы документационного обеспечения управления информационной безопасностью объектов защиты.

В заключение отметим, что принятые утверждения определяют сущность дальнейших исследований по проблеме устойчивости развития приоритетных объектов защиты на основе создания теоретических основ системного математического моделирования их информационной безопасности в заданном контексте, аспектах и условиях.

ЛИТЕРАТУРА

1. Ансофф И. Стратегическое управление /И. Ансофф. М.;1989. – 358 с.
2. Бажин И.И. Информационные системы менеджмента.- М.: ГУ-ВШЕ, 2000. – 688 с.
3. Доктрина информационной безопасности Российской Федерации.
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. Интегрированный менеджмент XXI века: парадигма безопасного и устойчивого (антикризисного) развития: монография/ С.В. Барковская, Е.А. Жидко, В.И. Морозов, Л.Г. Попова; Воронеж. гос. арх-строит. ун-т. –Воронеж, 2011. -168 с.
6. 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.
7. Жидко Е.А. Менеджмент. Экологический аспект: курс лекций /Е.А. Жидко; Воронеж. гос.арх.-строит. ун-т.-Воронеж., 2010.-180 с.
8. 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.
9. Международные нормы и стандарты, правила и права.
10. Международный стандарт ISO / IEC (серия стандартов информационной безопасности).
11. Повестка дня ООН на XXI век.
12. 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.
13. Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне"
14. Яндекс: учение о ноогенезе, экология интеллектуальных систем, информационная гигиена.

Рецензент: Толстых Н.Н., Начальник службы координации программ (СКП), ОАО «Концерн «Созвездие», Доктор технических наук, профессор.

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

Larisa Popova
FAI «State scientific-research Institute of technical protection of information of the Federal service for technical and export control»
E-Mail: Larisa.popova.38@mail.ru

The concept of the system of mathematical modeling information security

Abstract: At the present stage one of the urgent problems of safe and sustainable (anti-crisis) development of the Russian Federation is ensuring information security in the new conditions of the XXI century. Assessment of the status of the issue in the doctrine of the conclusions about contradictions in the legal framework of information security of objects of protection, its imperfection, and also about the gap in the level of development of national information technologies from the level reached in the world.

The article generated a generalized system of views (claims 1 to 12) on the way of solving the problem of information security of objects in a security context: safety and sustainability as a function of information, an argument which is the protection of the object from the threat of a security breach. When studying the past is invited to consider the factors that are actively and significantly affect information security (human and natural, the imperfection of the scientific-methodical support, opportunities and threats of the information conflict resolution).

The developed generalized system of views based on the requirements of the national package of legal documents on information security of the Russian Federation, the modern approach to the research on the problem, consider the impact on the formulation and solution of policies of integration of Russia into the world economy and the globalization of the economy, introduction of the model of state regulated innovative economy.

Keywords: information security; legal framework; sustainable development; protection; measure data; information support; the concept.

Identification number of article 157EVN214

REFERENCES

1. Ансофф И. Стратегическое управление /И. Ансофф. М.;1989. – 358 с.
2. Бажин И.И. Информационные системы менеджмента.- М.: ГУ-ВШЕ, 2000. – 688 с.
3. Доктрина информационной безопасности Российской Федерации.
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. Интегрированный менеджмент XXI века: парадигма безопасного и устойчивого (антикризисного) развития: монография/ С.В. Барковская, Е.А. Жидко, В.И. Морозов, Л.Г. Попова; Воронеж. гос. арх-строит. ун-т. –Воронеж, 2011. -168 с.
6. 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.
7. Жидко Е.А. Менеджмент. Экологический аспект: курс лекций /Е.А. Жидко; Воронеж. гос.арх.-строит. ун-т.-Воронеж., 2010.-180 с.
8. 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.
9. Международные нормы и стандарты, правила и права.
10. Международный стандарт ISO / IEC (серия стандартов информационной безопасности).
11. Повестка дня ООН на XXI век.
12. 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.
13. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне».
14. Яндекс: учение о ноогенезе, экология интеллектуальных систем, информационная гигиена.