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.

Принципы системного математического моделирования информационной безопасности

Аннотация: С целью реализации предложенной концепции системного математического моделирования информационной безопасности в статье формулируются основные принципы исследования по проблеме, которыми необходимо руководствоваться.

К ним относятся следующее. 1. Необходимо выявить требования по информационной безопасности объектов, систему ограничений на выбор способов и средств их обеспечения, достоинства и недостатки накопленной базы знаний и ресурса по проблеме. 2. Обосновать целевое и функциональное назначение новых разделов теоретических основ системного математического моделирования информационной безопасности. 3. Целесообразно принять за основу принцип максимального использования достоинств накопленной базы знаний и ресурса по проблеме при условии сведения к минимуму их недостатков. 4. С целью повышения достоверности результатов исследования по проблеме необходимо обеспечить верификацию результатов синтаксического, семантического и математического моделирования взаимосвязанного развития внешней и внутренней среды объектов защиты, которое разработано теоретическими, эмпирическими и эвенталогическими методами. 5. Исследования на такой системе моделей должны обеспечить идентификацию системы управления объекта по результатам экспертизы ее эффективности на соответствие требуемому. 6. На этой основе обеспечить управление циклами информационной и интеллектуальной поддержки устойчивости развития объекта защиты в реально складывающейся и прогнозируемой обстановке XXI века.

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

Идентификационный номер статьи в журнале 169EVN214

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

На современном этапе научные исследования по любой проблеме, как правило, базируются на парадигме, включающей концепцию, принципы и методологию. Принципы (в переводе с латинского «основополагающая идея») это то, чем обязательно следует руководствоваться в теоретической (познавательной, методологической, исследовательской и т.д.) и/или практической деятельности.

С целью реализации концепции системного математического моделирования информационной безопасности приоритетных объектов защиты в заданном контексте, аспектах и условиях сформулируем основные принципы исследований по проблеме.

Принцип 1. В результате анализа состава, содержания и структуры пакета нормативно-правовых документов по информационной безопасности Российской Федерации [2,3,8,9]необходимо установить:

- требования по защите приоритетных объектов (по отраслям) от угроз нарушения их информационной безопасности с негативными последствиями для личности, общества, государства;
- систему ограничений на выбор способов и средств обеспечения таких требований (угрозы, их источники по цели, месту, времени, диапазону условий и полю проблемных ситуаций, возникающих во внешней и внутренней среде объекта);
- достоинства и недостатки накопленной базы знаний и ресурса по проблеме [4,5,6,7].

Принцип 2. На этой основе обосновать целевое и функциональное назначение новых разделов математического моделирования, численных методов и комплексов программ, необходимых и достаточных для эффективных исследований по проблеме информационной безопасности объекта защиты в реально складывающейся и прогнозируемой обстановке XXI века.

Принцип 3. Принять за основу принцип максимального использования достоинств накопленной базы знаний и ресурса по проблеме при условии сведения к минимуму их недостатков. С этой целью следует воспользоваться современной технологией системного моделирования, которая обеспечивает универсализацию и автоматизацию исследований по проблеме. Это значит, что системное математическое моделирование информационной безопасности должно базироваться на разработке комплексов синтаксических, семантических и адекватных им математических моделей взаимосвязанного развития внешней и внутренней среды объекта защиты теоретическими, эмпирическими и эвентологическими методами. На основе верификации результатов исследований, полученных такими методами, формируется система математических моделей требуемого целевого и функционального назначения по проблеме.

Принцип 4. С цельюразработки алгоритма верификации целесообразно воспользоваться технологией комплексного прогнозирования,которая базируется на методах сбора и первичной обработки исходной информации (необходимое информационное обеспечение), её вторичной обработке методами исследовательского (эволюционное развитие) и нормативного (скачки в развитии, проектные методы) прогнозирования. Методы исследовательской технологии базируются на ретроспективной, текущей и экспертной информации о причинно-следственных связях, движущих силах, целях, законах и закономерностях взаимосвязанного развития внешней и внутренней среды объекта защиты. За основу методов нормативной технологии прогнозирования принимаются известные и прогнозируемые проектные отношения между количественно-качественными

характеристиками состояний внешней и внутренней среды объекта защиты. В качестве проектных принимаются отношения, которые известны по состоянию на рассматриваемые горизонты ретроспекции и заданные горизонты прогноза при достигнутом в мире к тому периоду уровне развития образования, науки, техники и технологий по проблеме. Проектные отношения отражают потенциальные возможности разрешения проблемы по состоянию на рассматриваемый период времени для объектов защиты, различных по природе и масштабам, сложности их внешних и внутренних структурных связей, детерминированности процессов взаимосвязанного развития, их цикличности и информационной обеспеченности.

Реальные возможности проявляются в намерениях и действиях договаривающихся сторон в реально складывающейся и прогнозируемой обстановке по состоянию на рассматриваемый период по цели, месту, времени, диапазону условий и полю проблемных ситуаций.

Разработанный на такой основе алгоритм верификации предназначается для оценки эффективности, качества и надежности разработанной системы математических моделей как одного из видов сложных систем.

Принцип 5. Исследования на такой системе математических моделей должны обеспечить идентификацию системы управления объекта защиты по результатам экспертизы её состояния на соответствие требуемому в заданном контексте, аспектах и условиях. При наличии диспропорций между необходимыми, потенциально возможными и реально достижимыми состояниями системы управления объекта устанавливаются: степень опасности возникающих угроз нарушения его информационной безопасности и адекватных им информационных рисков, приемлемость их последствий в заданном контексте, аспектах и условиях. Оценку приемлемости целесообразно осуществлять с позиций: допустимые, критические, неприемлемые. Тогда при наличии критических и/или неприемлемых последствий порождающие их диспропорции рассматриваются как движущие силы развития объекта защиты, его системы управления. Она предназначается для обеспечения устойчивости развития объекта на основе оптимизации его облика и программно-целевого планирования траектории устойчивого развития по ситуации и результатам в реально складывающейся и прогнозируемой обстановке XXI века.

Принцип 6. Реализация предложенных принципов должна обеспечить

управление циклами информационной и интеллектуальной поддержки устойчивости развития объекта защиты в заданных контексте, аспектах и условиях. В условиях неопределённости такая поддержка базируется на известных и вновь устанавливаемых законах и закономерностях взаимосвязанного развития внешней и внутренней среды приоритетных объектов защиты с целью эффективного решения заданных первоочередных задач по обеспечению их информационной безопасности. Для реализации необходимой и достаточной поддержки управления целесообразно включить в состав объекта систему его информационной безопасности. Её можно организовать, как с помощью его собственных сил, так и за счёт привлечения внешних консалтинговых служб требуемого целевого и функционального назначения.

Принцип 7. С целью обеспечения эффективного управления циклами информационной и интеллектуальной поддержки устойчивости развития объекта защиты необходимо в состав системы моделей включить комплексыиерархических, функциональных и процессных синтаксических и семантических моделей взаимосвязанного развития его внешней и внутренней среды.

В условиях неопределённости разработку названных комплексов различными методами целесообразно осуществлять на основе применения таких законов, как:

- единство и борьба противоположностей, отрицание отрицания, переход количества в качество;
- кто владеет информацией, тот владеет миром; недостаток информации, её избыток в равной мере приводят к негативным результатам;
- экономические законы управления производством по форме хозяйствования 4С (самоопределение, самоокупаемость, самофинансирование, самоуправление) [7];
- антикризисное управление на основе инноваций;
- отношения между ними образуют причинно-следственные связи перехода объекта защиты из одного устойчивого состояния в другое в заданном контексте, аспектах и условиях. Поэтому такие переходы целесообразно рассматривать как возможные исходы противоборства и конкурентной борьбы договаривающихся сторон, информационной войны между ними.

Распознавание исходов, их последствий осуществляется на основе введения градации состояний объекта защиты, адекватных им областей определения логико-вероятностно-информационных характеристик его внешней и внутренней среды в статике и динамике условий XXI века. С этой целью целесообразно воспользоваться следующими эмпирически установленными закономерностями:

- нормальное состояние социально-эколого-экономической системы государства достигается при условии формирования в нём гражданского общества, расслоение которого по уровню, качеству и безопасности жизни подчиняется отношению «10–80– 0». 80% населения это по определению основная масса счастливых граждан, которые живут «как все» при сложившихся нормах морали, образе жизни, культуре и религии, исповедуемой нацией;
- отклонения от нормального состояния вызываются нарушениями такого отношения. В этом случае вектор отклонения разграничивает области выгоды и ущерба, граница между которыми лежит в зоне полной неопределённости ситуации;
- получить выгоду возможно в состоянии лидерства и/или абсолютного превосходства одной из договаривающихся сторон над другой в заданном контексте, аспектах и условиях. В случае превосходства появляется угроза применения антимонопольного закона и др. мер политического, экономического, идеолого-психологического характера;
- ущерб возникает в процессе утраты лидерства, отставания в уровне развития, появления проблемы 4Б (безработица, бедность, болезни, беззащитность). Возникает угроза предкризисного и/или кризисного состояния, банкротства, ликвидации объекта;
- наличие таких эффектов, как физическое и моральное старение достижений образования, науки, техники и технологий по проблеме, действующих производств и производимой ими продукции, а также ограниченность ресурса, становятся причиной цикличности процесса создания, эксплуатации, роста и развития объекта, его защиты, реорганизации и/или ликвидации.

Существенное влияние на проявление таких закономерностей оказывают политики, проводимые государством во внешней и внутренней среде объекта защиты, их нормативно-правовое обеспечение, человеческий и природный факторы. Влияние человеческого фактора на ситуацию и результаты проявляется в мотивации поведения отдельных личностей, толпы, общественных и оппозиционных организаций. Влияние природного фактора проявляется в специфике и изменениях состояний каналов связи, ограниченности и неравномерности распределения природных ресурсов, наличии природных катаклизмов, которые нередко порождаются антропогенным воздействием человека на природу, превышающим нормы экологической безопасности.

Принцип.8. С целью определения области значений количественно-качественных логико-вероятностно-информационных характеристик, которые гарантируют достижение о сохранение заданного состояния устойчивости развития объекта защиты, систему математических моделей информационной безопасности следует дополнить системой координат и измерительных шкал. Их разработку целесообразно осуществить на основе известных приёмов:

- введение начала отсчёта возможных состояний устойчивости развития объекта в виде нормального закона распределения вероятности с центральной симметрией для оценки возможности достижения цели по ситуации и результатам;
- для определения координат особых точек в графиках закона (плотность вероятности в статике; вероятность в динамике) применяются известные методы математического и/или графического анализа. Такими точками являются: предельные значения вероятности [0, 1] и точка перегиба 0,5 – граница разграничения областей выгоды и ущерба; точки выпуклости 0,75 в области выгоды и вогнутости 0,25 в области ущерба. Они принимаются за эталонные значения градаций возможных состояний объекта, его внешней и/или внутренней среды в заданном контексте, аспектах и условиях;
- для оценки допустимых, критических и неприемлемых отклонений вероятностей от эталонных значений применяется следующий подход. Названные отклонения рассматриваются как функция требуемого уровня защищённости объекта от угроз (определяется адекватно режиму секретности), адекватных ему требований к эффективности методов и систем защиты (т.е. к их качеству), способов и средств обеспечения устойчивости развития объекта по ситуации и результатам в статике и динамике условий XXI века;
- предельные границы таких отклонений устанавливаются с помощью координат точек касания линии сопряжения соседних близких к линейным участков в графике принятого нормального закона с центральной симметрией. Тогда принятые значения координат особых точек приводятся в виде диапазонов: [0 + 0,025; 1 – 0,025]; (0,5 ± 0,025); (0,75± 0,025); (0,25 ± 0,025).

Дальнейшая градация состояний (допустимые, критические, неприемлемые отклонения) во многом носит концептуальный характер. Он существенно зависит от выбранного принципа компромисса, адекватного ему принципа оптимизации способов и средств достижения интегральной и частных целей объекта защиты, их приоритетности в реально складывающейся и прогнозируемой обстановке XXI века.

Принцип 9. Реальный закон распределения вероятностей, как правило, отличается от нормального. Это является одной из основных причин появления противоречий в результатах теоретических, эмпирических и эвентологических методов разработки системы моделей. С

целью их ликвидации применяется принцип «практика – критерий истины». Для его реализации целесообразно воспользоваться аппаратом математической статистики в комплексе с численными методами и проведением аналогий, ассоциаций, асимптотического приближения реально достигнутого и потенциально возможного к необходимому и достаточному. Фактически на этом принципе и должно строиться антикризисное управление на основе инноваций.

В такой ситуации следует: исследовать промахи и ошибки лиц, принимающих решения, вскрывать породившие их причины, порождаемые ими угрозы, их последствия; синтезировать на этой основе адекватные меры по предупреждению причин и ликвидации их негативных последствий.

Заметим, что отклонения реального закона распределения от нормального целесообразно трактовать как его искажения. Тогда системное математическое моделирование на основе асимптотического приближения эмпирики к другим известным законам распределения вероятностей позволяет воспользоваться известными для них логико-аналитическими выражениями при расчётах математического ожидания, дисперсии и среднеквадратических ошибок, коэффициентов корреляции и др. характеристик состояния объекта.

Принцип 10. В отдельную проблему выливается решение задачи глобальной оптимизации способов и средств достижения интегральной цели объекта защиты в заданном контексте, аспектах и условиях. Её решение выходит за рамки данных исследований. Однако, предпрогнозные исследования по этой проблеме позволили сделать вывод, что её разрешение возможно на основе дальнейшего совершенствования и развития математических моделей, разработка которых базируется на принципах наискорейшего спуска и подъёма (аналоги: классический метод Ньютона, метод формирования вторичных приближённых моделей по И.И. Бажину, др.) [1].

При этом целесообразно результаты системного математического моделирования информационной безопасности объекта защиты рассматривать как аргумент для глобальной оптимизации и воспользоваться методом их вложений при постановке и решении такой задачи.

Принцип 11. Теоретические основы системного математического моделирования информационной безопасности, отвечающие предложенной концепции и принципам, целесообразно проверить на практике. Например, применительно к системам управления экологически опасных и экономически важных объектов ЦЧР, а также городского округа Воронеж [4]. По результатам таких исследований вносятся корректировки и изменения в эти основы,формируется научно-методическое и научно-практическое обеспечение программы исследований информационной безопасности объекта защиты, разрабатываются рекомендации по их распространению на объекты различной природы и масштабов, сложности структурных связей, детерминированности и цикличности изучаемых процессов, их информационной обеспеченности.

Принцип 12. С целью автоматизации исследований по проблеме на основе их универсализации целесообразно программу строить на едином алгоритме с использованием единой шкалы оценки состояний устойчивости развития объекта защиты в заданном контексте, аспектах и условиях. В качестве базового комплекса показателей эффективности методов и систем защиты информации целесообразно воспользоваться сложившимся в эвентологии подходом. В комплекс целесообразно включить показатели:

- чувствительность системы управления объекта защиты к мере реально получаемой информации;

- функцию принадлежности методов и систем защиты информации к функции их полезности с точки зрения своевременного достижения и сохранения требуемого уровня устойчивости развития объекта в статике и динамике условий XXI века;
- вероятность достижения локальных и интегральной целей объекта в заданном контексте, аспектах и условиях.

Тогда представляется возможным автоматизировать исследования по проблеме информационной безопасности на основе формирования системы проблемно-ориентированных программ, используя накопленную базу знаний и ресурса. В этом случае в качестве аналогов таких программ целесообразно использовать известные географические информационные системы (GIS и её специальные предложения), CASE(IDEF) технологии и др.

Реальность такого подхода можно также проверить на примере системы управления экологически опасных и экологически важных объектов ЦЧР и городского округа Воронеж.

ЛИТЕРАТУРА

1. Бажин И.И. Информационные системы менеджмента.- М.: ГУ-ВШЕ, 2000. – 688 с.
2. Государственная информационная политика компании
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., 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.
8. Международные нормы и стандарты, правила и права
9. Международный стандарт ISO / IEC (серия стандартов информационной безопасности).

Рецензент: Николай Николаевич Толстых, 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
The Federal Autonomous institution "State scientific-research Institute of technical protection of information of the Federal service for technical and export control
Russia, Voronezh

Principles of the system of mathematical modeling information security

Abstract: The purpose of the proposed concept of the system of mathematical modeling of information security in the article formulates the basic principles of research on a problem that guide it.

These include the following. 1. It is necessary to identify the requirements for information security objects, the system of restrictions on the choice of methods and facilities, advantages and disadvantages accumulated knowledge base and resource on the problem. 2. To justify the target and functional purpose of the new sections of the theoretical foundations of the system of mathematical modeling of information security. 3. It is advisable to adopt as a basis the principle of maximum use of the advantages of the accumulated knowledge base and resource on the issue provided to minimize their weaknesses. 4. With the purpose of increase of reliability of the results of research on a problem you must provide verification of the results of the syntactic, semantic and mathematical modeling of interconnected development of the external and internal environment protection facilities developed theoretical, empirical and eventlogentry methods. 5. Research on such a system models must ensure identification of control system of the object of the examination of its efficiency against a required. 6. On this basis, to ensure the control loops of information and intellectual support sustainable development of the object of protection in really developing and predictable environment of the XXI century.

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

Identification number of article 169EVN214

REFERENCES

1. Bazhin I.I. Informacionnye sistemy menedzhmenta.- M.: GU-VShE, 2000. – 688 s.
2. Gosudarstvennaja informacionnaja politika kompanii
3. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii.
4. Zhidko E.A. Jekologicheskij menedzhment kak faktor jekologo-jekonomicheskoj ustojchivosti predprijatija v uslovijah rynka: monografija /E.A. Zhidko; Voronezh. gos.arh.-stroit. un-t.-Voronezh, 2009.-160 s.
5. Zhidko E.A. Integrirovannyj menedzhment HHI veka: paradigma bezopasnogo i ustojchivogo (antikrizisnogo) razvitija: monografija/ S.V. Barkovskaja, E.A. Zhidko, V.I. Morozov, L.G. Popova; Voronezh. gos. arh-stroit. un-t. –Voronezh, 2011. -168 s.
6. 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.
7. 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.
8. Mezhdunarodnye normy i standarty, pravila i prava
9. Mezhdunarodnyj standart ISO / IEC (serija standartov informacionnoj bezopasnosti).