УДК 004.056

ИННОВАЦИИ В МЕТОДОЛОГИИ ИССЛЕДОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ

© 2017 Е. А. Жидко, К. А. Кирьянов

Воронежский государственный архитектурно-строительный университет
ВУНЦ ВВС «ВВА им. Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж)

Рассматривается возможность создания методологических основ обеспечения информационной безопасности ХС, отвечающая требованиям доктрины информационной безопасности Российской Федерации. Учитываются факторы, существенно влияющие на конкурентоспособность таких объектов в условиях состязательности конкурирующих сторон, информационно-психологической и др. войны между ними.

Ключевые слова: конкурентоспособность, инновации, информационная безопасность, методология, лингвистическое моделирование.

Информационная безопасность (ИБ) хозяйствующего субъекта (ХС) его системы информационной безопасности (СИБ) должна рассматриваться как аргумент их устойчивого (антикризисного) развития, с одной стороны, и как функция информационного конфликта между договаривающимися сторонами, с другой [1-8]. Ключевым моментом в реализации такого подхода является задание на прогноз взаимоувязанных требований, системы ограничений и ресурса по проблеме информационного обеспечения (ИО) безопасности и устойчивости развития ХС, его СИБ при наличии угроз нарушения их ИБ с неприемлемыми последствиями в условиях развития информационных конфликтов (ИК) и/или ведения информационных войн между договаривающимися сторонами. Каждый раздел такого задания составляется на уровнях: международном, межстрановом, внутристрановом и корпоративном [8].

Согласно сложившейся теории прогнозирования и принятия решений [8-11], типовая форма Задания на прогноз включает:

- **основания** для выполнения Задания на прогноз – гарантийное письмо и финансовый документ Заказчика, определяющий сроки и объёмы ассигнований на выполнение Задания;

- **цели и задачи** прогностических исследований;

- **перечень объектов прогноза и фона** их развития, применительно к которым требуется получить прогнозные характеристики;

- **требования** к перечню прогнозируемых характеристик, срокам получения прогнозов (горизонтам прогноза), их полноте, достоверности, точности и полезности;

- в форме таблицы задаются этапы прогностических исследований, наименование разделов и сроки их выполнения по этапам, указываются ответственные за них организации – юридические лица;

- устанавливается **необходимая** степень и продолжительность **защиты** прогностических исследований и их результатов (особой важности, совершенно секретно, секретно, для служебного пользования);

- приводятся **обязательства** Заказчика по обеспечению прогностических исследований необходимой **информацией** (т. е. перечень исходных данных и ограничений).

В свете вышесказанного в таблице приведена краткая характеристика сущности основных разделов задания на прогноз.

Исходными данными для формулировки требований по ИО на *международном* уровне являются сведения о реально складывающейся и прогнозируемой обстановке в мире и его отдельных регионах. Перечень таких сведений сформулирован в повестке дня ООН на XXI век [12].

На уровне *межстрановых* отношений такие перечни устанавливаются на основе определения состава и содержания входных информационных потоков, необходимых и достаточных для формирования стратегиче-

Жидко Елена Александровна – ВГАСУ, профессор кафедры пожарной и промышленной безопасности, канд. техн. наук, доцент, lenag66@mail.ru.

Кирьянов Константин Анатольевич – ВУНЦ ВВС «ВВА им. Н. Е. Жуковского и Ю. А. Гагарина», ст. преподаватель кафедры управления войсками и службы штабов, konst63224@mail.ru.

ского видения перспективных направлений деятельности и развития ХС, его СИБ. Задача решается в результате анализа состава и содержания аргументов, используемых в научно-методическом обеспечении Маркетинга Менеджмента XXI века, прогнозирования мировых рынков, стратегического планирования в бизнес системах, антикризисного управления на основе инноваций и инновационно-инвестиционного проектирования [8, 10, 11].

Таблица

Области определения показателей эффективности защиты и их аргументов

Требования	Система ограничений	Ресурс
1. Информационное обеспечение безопасного (устойчивого) развития ХС в различных сферах, направлениях и видах деятельности его членов. Задаются области определения, вероятности достижения их генеральной и частных целей.	Пределы роста населения планеты, исходя из реальных возможностей по обеспечению достойного уровня, качества и безопасности жизни ЛОГ. Задаются области определения таких возможностей по критерию «Необходимо и потенциально возможно и реально достижимо»	Накопленная в мире база знаний и ресурса по проб-леме ИО, SWOT-анализ их возможностей по предупреждению критических и неприемлемых последствий, порождающих их причин на основе выявления сильных и слабых сторон ресурса, угроз и возможностей по его дальнейшему наращиванию и развитию.
2. Обеспечение ИБ приоритетных ХС на межстрановом, внутристрановом и корпоративном уровнях в реально складывающихся и прогнозируемой обстановке. Задается область определения допустимых состояний ХС в различных сферах, направлениях и видах его деятельности.	Устанавливается применительно к: охраняемым сведениям и уровням их защиты от хищений, разрушения, модификации; адекватным им уровням области определения технических демаскирующих признаков ХС по природе, масштабам, сложности структурных связей, детерминированности, цикличности и ИО. Критерий оптимизации способов и средств обеспечения ИБ: «Необходимая- И потенциально возможная- И реально достижимая» мера информации для принятия адекватных решений по предупреждению угроз нарушения ИБ ХС, его СИБ по ситуации в статике и динамике новых условий XXI века .	Исходными являются: выявленные угрозы и возможности по ИО безопасного и устойчивого развития ХС, его СИБ; принятые политики, доктрины и нормативно-правовые документы по реализации таких возможностей, предупреждению угроз и ликвидации их негативных последствий. Устанавливается накопленная база знаний и ресурса по проблеме обеспечения ИБ ХС, их СИБ. Выявляются сильные и слабые стороны такого ресурса, адекватные им информационные риски, угрозы по нарушению ИБ. Намечаются пути дальнейшего совершенствования и наращивания ресурса по ИБ.
3. Задаются области определения допустимой, критической и неприемлемой мерой информации, обеспечивающей требуемые значения априорной и апостериорной вероятности достижения целей ХС и его СИБ по ситуации в статике и динамике новых условий XXI века	Поле проблемных ситуаций, возникающих во внешней и внутренней среде ОЗ, его СИБ с учетом влияния на них неопределенности ситуации, ограниченного ресурса, человеческого и природного факторов. Задаются области допустимых значений информационных рисков, адекватных им критических и неприемлемых последствий по ситуации и результатам.	Накопленная база знаний и ресурса по разрешению ИК, их эффективность и применимость в интересах достижения целей ИО и ИБ ХС, их СИБ. Предложения по направлениям дальнейшего развития и наращивания ресурса в интересах достижения и сохранения их безопасного и устойчивого развития в реально складывающейся и прогнозируемой обстановке.

На *внутристрановом* уровне требования к перечню защищаемых сведений устанавливаются исходя из Государственной информационной политики, Доктрины информационной безопасности Российской Федерации, Политики ИБ компании и других нормативно-правовых документов по проблеме обеспечения ИБ ОЗ, их СИБ [13, 14].

Детализация таких сведений, в том числе на *корпоративном* уровне, осуществляется в результате анализа состава и содержания аргументов, которые используются в научно-методическом обеспечении формы хозяйствования 5С, антикризисного управления функционированием объектов на основе инноваций, инновационно-инвестиционного проектирования *облика* объекта и *тренда* (т. е. траектории) его развития с учётом рисков [15-21].

Однако, накопленная база знаний в новых условиях XXI века требует своего дальнейшего развития и усовершенствования на основе комплексирования классических методов теории вероятностей, теории информации и эвентологии [22].

ЛИТЕРАТУРА

1. Барковская С. В. 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.
2. Жидко Е. А. Информационная безопасность модернизируемой России: постановка задачи / Е. А. Жидко, Л. Г. Попова // Информация и безопасность. – 2011. – Т. 14. – № 2. – С. 181-190.
3. Жидко Е. А. Информационная и интеллектуальная поддержка управления развитием социально-экономических систем / Е. А. Жидко, Л. Г. Попова // Вестник Иркутского государственного технического университета. – 2014. – № 10 (93). – С. 12-19.
4. Жидко Е. А. Формализация программы исследований информационной безопасности компаний на основе инноваций / Е. А. Жидко, Л. Г. Попова // Информация и безопасность. – 2012. – Т. 15. – № 4. – С. 471-478.
5. Жидко Е. А. Парадигма информационной безопасности компании / Е. А. Жидко, Л. Г. Попова // Вестник Иркутского государственного технического университета. – 2016. – № 1 (108). – С. 25-35.
6. Жидко Е. А. Теоретические основы проектирования и конструкции жидкостных пылеулавливающих устройств / Е. А. Жидко, В.В. Колотушкин, Э. В. Соловьева // Безопасность труда в промышленности. - 2004. – № 2. – С. 8-11.
7. Жидко Е. А. Научно-обоснованный подход к классификации угроз информационной безопасности / Е. А. Жидко // Информационные системы и технологии. – 2015. – № 1 (87). – С. 132-139.
8. Жидко Е. А. Логико вероятностно-информационный подход к моделированию информационной безопасности объектов защиты: монография / Е. А. Жидко; Воронеж. гос. арх -строит. ун-т. – Воронеж, 2016. – 123 с.
9. Сазонова С. А. Методы обоснования резервов проектируемых гидравлических систем при подключении устройств пожаротушения / С. А. Сазонова // Вестник Воронежского института ГПС МЧС России. – 2015. – № 4 (17). – С. 22-26.
10. Ефремов В. С. Стратегическое планирование в бизнес-системах / В. С. Ефремов. – Финпресс, 2001. – 240 с.
11. Котлер Ф. Маркетинг менеджмент; под ред. Л. А. Волковой, Ю. Н. Каптуревского. – СПб: Питер, 2000. – 752 с.
12. Повестка дня на XXI век. – ООН: Рио-де-Жанейро, 1992.
13. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 9 сентября 2000 г., № Пр-1895.
14. Государственная информационная политика компании.
15. Жидко Е. А. Человеческий фактор как аргумент информационной безопасности компании / Е. А. Жидко, Л. Г. Попова // Информация и безопасность. – 2012. – Т. 15. – № 2. – С. 265-268.
16. Жидко Е. А. Логико-вероятностно-информационное моделирование информационной безопасности / Е. А. Жидко, Л. Г. Попова // Вестник Казанского государственного технического университета им. А. Н. Туполева. – 2014. – № 4. – С. 136-140.
17. Жидко Е. А., Кирьянов В. К. Эмпирические методы измерения погрешностей при взаимосвязанном развитии внешней и внутренней среды хозяйствующих субъектов /Е. А. Жидко, В. К. Кирьянов // Инженерные системы и сооружения. – 2013. – № 4 (13). – С. 53-60.
18. Жидко Е. А. Методология формирования системы измерительных шкал и норм информационной безопасности объекта защиты/ Е.А. Жидко // Вестник Иркутско-

го государственного технического университета. – 2015. – № 2 (97). – С. 17-22.

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

20. Сазонова С. А. Обеспечение безопасности гидравлических систем при реализации задач управления функционированием

23.

и развитием / С. А. Сазонова // Вестник Воронежского института ГПС МЧС России. – 2016. – № 1 (18). – С. 22-26.

21. Сазонова С. А. Оценка надежности работы сетевых объектов / С. А. Сазонова // Вестник Воронежского института высоких технологий. – 2016. – № 1 (16). – С. 40-42.

22. Воробьев О. Ю. Эвентология / О. Ю. Воробьев, Сиб.фед. ун-т. – Красноярск, 2007. – 434 с.

INNOVATION IN THE METHODOLOGY OF RESEARCH OF INFORMATION SAFETY OF ECONOMIC SUBJECTS

© 2017 E. A. Zhidko, K. A. Kiryanov

Voronezh State Technical University
Air Force Academy named after Professor N. E. Zhukovsky and Y. A. Gagarin

The possibility of creating a methodological framework for the provision of information security of ChS, which meets the requirements of the doctrine of information security of the Russian Federation, is considered. Factors that significantly affect the competitiveness of such facilities in the competitive environment, information-psychological and other wars between them are taken into account.

Keywords: competitiveness, innovations, information security, methodology, linguistic modeling.