УДК 004.9:65.012.8

НЕЧЕТКИЙ АНАЛИЗ УГРОЗ И ВЫБОР ВАРИАНТОВ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИННОВАЦИОННОГО ПРОЕКТА

[1]Ломазов В.А., [2]Гостищева Т.В., [2]Климова Н.А.

[1]Белгородский государственный аграрный университет имени В.Я. Горина, Белгород, e-mail: vlomazov@yandex.ru;

[2]Белгородский университет кооперации, экономики и права, Белгород

Статья посвящена проблеме выбора вариантов системы информационной безопасности инновационного проекта. Рассмотрены теоретические аспекты применения методологического аппарата нечеткого теоретико-множественного анализа для поддержки принятия организационных решений. Предложено нечеткое описание ситуаций с точки зрения возможных угроз информационной безопасности. На основе понятий точных граней (применяемых к упорядоченным множествам нечетким множествам ситуаций) построены нечеткие теоретико-множественные операции над ситуациями. Это позволило сформулировать задачу выбора системы защиты не для отдельной угрозы, а для совокупности возможных ситуаций. Задача обобщена на случай возможной смены вариантов защиты информации на различных этапах периода реализации инновационного проекта. Предложены стратегии сокращения области выбора вариантов системы защиты информации и приведены примеры их использования. Предварительные результаты применения основанной на предложенном подходе процедуры поддержки принятия решений по составлению плана развития системы информационной безопасности показали ее эффективность.

Ключевые слова: информационная безопасность, нечеткий теоретико-множественный анализ, проблема выбора

FUZZIY ANALYSIS OF THREATS AND SELECTION OF VARIANTS OF THE INFORMATION SECURITY SYSTEM OF THE INNOVATIVE PROJECT

[1]Lomazov V.A., [2]Gostischeva T.V., [2]Klimova N.A.

[1]Belgorod State Agricultural University named after V.Ya. Gorin, Belgorod, e-mail: vlomazov@yandex.ru;

[2]Belgorod University of Cooperation, Economics and Law, Belgorod

The article deals with the problem of choice of information security for innovation project. Theoretical aspects of application of the methodologies of fuzzy set-theoretic analysis for decision making support. The fuzzy description of situations from the point of view of possible threats to information security is suggested. Based on the concepts the precise edges (applied to an ordered set of fuzzy sets of situations) a fuzzy set-theoretic operations on situations are constructed. This allowed to formulate the problem of selecting the protection systems not for specific threats, but for a set of possible situations. The problem is generalized to the case of a possible change of variants of information protection at different stages of the implementation period of the innovation project. The strategies of reducing the field of choice of variants are proposed and examples of their use are constructed. Preliminary results of the use the procedure, based the on the proposed approach, showed its effectiveness.

Keywords: information security, fuzzy set-theoretic analysis, the problem of choice

Одним из обязательных условий успешности реализации инновационного производственно-экономического проекта является надежное обеспечение его информационной безопасности [1]. Специфика инновационной и венчурной деятельности, как правило, предполагает широкое использование современных информационных технологий управления организационными и производственно-технологическими процессами, что (при несовершенстве системы защиты информации) может быть связано с определенными рисками. Это делает актуальным развитие методологического аппарата анализа угроз и поддержки принятия управленческих решений по обеспечению информационной безопасности инновационных проектов. Однако появившиеся в последнее время научные работы в этой области ограничиваются в основном исследованиями теоретико-методологических экономических (с точки зрения обеспечения безопасности интеллектуального капитала [2] и защиты информации в условиях недобросовестной конкуренции [3], а также применительно к отдельным сферам экономической деятельности: например, инновациям в промышленном производстве [4] и коммерции [5]), организационно-правовых ([6]) и информационно-аналитических ([7]) аспектов проблемы, тогда как не меньшее значение имеют разработки, ориентированные на непосредственное использование в практической деятельности предприятий и организаций, осуществляющих инновационную деятельность.

Целью настоящей работы является разработка инструментария анализа ситуаций (совокупностей внешних условий), возникающих при реализации инновационного

проекта и рассматриваемых с точки зрения возможных угроз информационной безопасности. Применяемый подход основан на использовании аппарата нечетких множеств и отношений [8] и методологии теории принятия решений [9], что дает новые возможности для выбора вариантов системы информационной безопасности проекта. Прикладное значение работы связано с необходимостью минимизации затрат негосударственных предприятий и организаций (в том числе малых предприятий [10]), для которых система мер защиты информации не является строго регламентированной и может быть выбрана из соображений разумной достаточности.

Нечеткий теоретико-множественный анализ угроз информационной безопасности

Под угрозой информационной безопасности инновационного проекта в соответствии с [1] будем понимать событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты информационной системы может привести к нанесению ущерба субъектам, занимающимся инновационной деятельностью.

Пусть $Threat = \{Threat_1, Threat_2,..., Threat_I\}$ – конечное множество предполагаемых независимых угроз информационной безопасности рассматриваемого инновационного проекта. Текущая (рассматриваемая с точки зрения угроз информационной безопасности проекта) ситуация $Sit(t_k)$, в которой реализуется проект, может быть представлена в виде определенного на универсуме нечеткого множества

$$\tilde{T}\ hreatSit(t_k) = \{(Threat_i, \mu_i(t_k))|\ i = 1,2,...,I\},$$

где определенная на отрезке [0, 1] функция принадлежности $\mu_i(t_k)$ характеризует уровень угрозы $Threat_i$ ($i = 1,2,...,I$) в ситуации Sit на этапе t_k ($k = 1,2,..., K$) реализации проекта. Для определения $\mu_i(t_k)$ может быть использован предложенный в [11] подход, в рамках которого уровень риска угрозы находится на основе определяемых экспертами значений вероятности угрозы и последствий при реализации этой угрозы (в соответствии с ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.). Возможен также подход (например, [12]), когда уровень угрозы непосредственно оценивается экспертами в вербальной шкале, после чего определяется относительное числовое значение показателя с использованием неравномерной шкалы соответствия, пример которой приведен в табл. 1.

Таблица 1

Пример шкалы соответствия между вербальными и относительными числовыми значениями уровня угрозы

№ п/п	Вербальное значение	Относительное числовое значение
1	Угроза отсутствует	0
2	Очень низкий уровень угрозы	0,1
3	Низкий уровень угрозы	0,3
4	Средний уровень угрозы	0,6
5	Высокий уровень угрозы	0,8
6	Очень высокий уровень угрозы	1,0

При этом возможны промежуточные значения показателя. Если в экспертизе участвует несколько специалистов, то общее относительное значение уровня угрозы может быть получено как взвешенное среднее индивидуальных значений (весовые коэффициенты отражают соотношения квалификаций экспертов). В случаях, когда эксперты затрудняются в непосредственной оценке угрозы, может быть применен метод парных сравнений Саати [13].

Носителем нечеткого множества $\tilde{T}\ hreatSit(t_k)$ является совокупность угроз, присутствующих в ситуации $Sit(t_k)$:

$$Supp\ (\tilde{T}\ hreatSit(t_k)) = \{Threat_i, \mu_i(t_k))| \mu_i(t_k)) > 0, i = 1,2,...,I\}$$

Ядро нечеткого множества нечеткого множества $\tilde{T}\ hreatSit(t_k)$ представляет собой совокупность угроз высокого уровня в ситуации $Sit(t_k)$:

$$Kern\ (\tilde{T}\ hreatSit(t_k)) = \{Threat_i, \mu_i(t_k))| \mu_i(t_k)) = 1, i = 1,2,...,I\}.$$

Рассмотрим множество всех возможных ситуаций

$$ST = \{Sit(t_k)|\ \tilde{T}\ hreatSit(t_k) = \{(Threat_i, \mu_i(t_k)), i = 1,2,...,I, 0 \le \mu_i(t_k)) \le 1\}\ ,k = 1,2,..., K\}.$$

Определенная на ST операция нестрогого включения нечетких множеств порождает отношение нестрогого доминирования ситуаций $\angle$ в соответствии с правилом:

для любых Sit^*, $Sit^* \angle\ S$ выполняется $Sit^* \angle\ Sit^{**}$, если

$$\mu_i{}^*(t_k) \le \mu_i{}^{**}(t_k) \text{ при всех } i = 1,2,...,I, \quad k = 1,2,..., K.$$

Введенное отношение нестрогого доминирования ситуаций будет отношением частичного порядка на множестве ситуаций ST, поскольку (как нетрудно видеть) для него выполняются требуемые условия:

– рефлексивность: $Sit^* \angle\ Sit^*$;

– антисимметричность:

$Sit^* \angle Sit^{**}, Sit^{**} \angle Sit^* \Rightarrow Sit^* = Sit^{**};$

– транзитивность:

$Sit^* \angle Sit^{**}, Sit^{**} \angle Sit^{***} \Rightarrow Sit^* \angle Sit^{***}.$

При решении практических задач, связанных с обеспечением информационной безопасности инновационных проектов, целесообразно рассматривать конечное (состоящее из N элементов) множество возможных ситуаций $ST^*: ST^* \subseteq ST, |\, ST^* \,| = N$.

Применительно к введенному отношению частичного порядка множество верхних граней для ST^* будет состоять из ситуаций $Sit^{**} \in ST$, нестрого доминирующих все ситуации из множества ST^*, т.е.

$$ST^{**} = \{Sit^{**} \mid Sit \angle Sit^{**}, \forall Sit \in ST^*\}.$$

Точная верхняя грань (supremum) представляет собой минимальную верхнюю грань, которая (в силу конечности множества ST^*) всегда существует

$$sup\ ST^* = Sit^* : Sit^* \angle Sit, \forall Sit \in ST^{**}.$$

Если ситуация Sit^*, представляющая собой точную верхнюю грань множества ST^*, является элементом этого множества, то она является также максимальным элементом множества ST^*, т.е.

$$\max ST^* = sup\ ST^* \text{ при } sup\ ST^* \in ST^*.$$

Понятия точной нижней грани (*inf*) и минимума (min) применительно к множеству ситуаций (с учетом введенного отношения частичного порядка $\angle$) определяются аналогичным образом. Основываясь на введенных понятиях точных граней, естественно ввести операции над ситуациями угроз информационной безопасности проектов.

Объединением ситуаций Sit^* и Sit^{**} назовем точную верхнюю грань множества, состоящего из двух этих ситуаций:

$$Sit^* \cup Sit^{**} = sup\ \{Sit^*, Sit^{**}\}.$$

Пересечением ситуаций Sit^* *и* Sit^{**} назовем точную нижнюю грань множества, состоящего из двух этих ситуаций:

$$Sit^* \cap Sit^{**} = inf\ \{Sit^*, Sit^{**}\}.$$

Упорядочение ситуаций в соответствии с уровнями угроз информационной безопасности проектов и введение операций над ситуациями позволяют формулировать и решать задачи выбора вариантов системы информационной безопасности.

Выбор вариантов системы информационной безопасности инновационного проекта

Будем полагать, что для совокупности ситуаций $<Sit_1, Sit_2, \ldots, Sit_M>$ известны решения по обеспечению информационной безопасности (в виде вариантов системы организационных мероприятий, технологий, технических средств и т.д.) $Variants = <Var_1, Var_2, \ldots, Var_M> : Var_m \sim Sit_m$ $(m = 1,2,\ldots,M)$, из которых нужно выбрать вариант, подходящий для множества возможных (при реализации рассматриваемого инновационного проекта) ситуаций $ST^* = \{Sit_1^*, Sit_2^*, \ldots, Sit_J^*\}$, исходя из желательной минимальности различного рода издержек и затрат при создании и эксплуатации системы информационной безопасности $f(Var)$:

$$f(Var) \rightarrow \min,\ Var \in Variants^*.$$

Для сокращения области выбора $Variants$ до совокупности подходящих для ST^* вариантов $Variants^* \subseteq Variants$ предлагается использовать следующие стратегии:

1. Гарантированная стратегия:

$$Variants^* = \{Var \mid Var \in Variants,\ Var \sim Sit: sup\ Sit^* \angle Sit\}.$$

2. Байесовская стратегия:

$$Variants^* = \{Var \mid Var \in Variants,\ Var \sim Sit: Sit^B \angle Sit\}.$$

где Sit^B – байесовская ситуация, характеризуемая нечетким множеством угроз

$$\tilde{T}\ hreatSit^B(t_k) = \{(Threat_i, \sum_{j=1}^{J} \mu_{ij}(t_k) p_j \mid i = 1,2,\ldots,I\},$$

p_j – вероятность возникновения ситуации Sit_j^* $(j = 1,2,\ldots,J)$. Если вероятности p_j неизвестны, то (в соответствии с принципом неопределенности Лапласа можно предположить что все ситуации равновероятны, и положить $p_j = 1/J$ $(j = 1,2,\ldots,J)$.

3. Взвешенная стратегия (аналог подхода Гурвица в теории игр с природой [10]):

$$Variants^* = \{Var \mid Var \in Variants,\ Var \sim Sit : Sit^G \angle Sit\},$$

где Sit^G – взвешенная ситуация, характеризуемая нечетким множеством угроз

$$\tilde{T}\ hreatSit^G(t_k) = \{(Threat_i, (\lambda \mu_i(t_k)^{Inf} + (1-\lambda)\mu_i(t_k)^{Sup})) \mid i = 1,2,\ldots,I\},$$

λ – коэффициент оптимизма/пессимизма при оценке угроз $(0 \le \lambda \le 1)$,

$$\tilde{T}\ hreatSit^{Inf}(t_k) = \{(Threat_i, \mu_i(t_k)^{Inf}) \mid i = 1,2,\ldots,I\} \sim sup\ Sit^*,$$

$$\tilde{T}\ hreatSit^{Sup}(t_k) = \{(Threat_i, \mu_i(t_k)^{Sup}) \mid i = 1,2,\ldots,I\} \sim inf\ Sit^*.$$

Общим для всех предлагаемых стратегий является построение на основе множества возможных ситуаций *ST** некоторой базовой ситуации (характеризуемой своим нечетким множеством угроз), после чего из множества *Variants* выделяется подмножество *Variants**, включающее в себя варианты, соответствующие ситуациям, нестрого доминирующим базовую ситуацию.

Рассмотрим пример выбора варианта системы информационной безопасности на основе применения предложенных стратегий. Пусть имеющийся набор вариантов системы информационной безопасности, соответствующих определенным ситуациям, и набор ситуаций, для которых необходимо выбрать соответствующий вариант, характеризуются данными, приведенными в табл. 2, 3.

В рамках рассматриваемого примера определяемые в соответствии с предложенными стратегиями базовые ситуации приведены в табл. 4.

Используя данные табл. 2–4, нетрудно видеть, что:

– при использовании гарантированной стратегии: $Variants^* = \{Var_3, Var_5\}$,

– при использовании Байесовской стратегии ($p_j = 0{,}2$, $j = 1,2,...,5$): $Variants^* = \{Var_3, Var_5, Var_7\}$,

– при использовании взвешенной стратегии ($\lambda = 0{,}5$): $Variants^* = \{Var_3, Var_5, Var_6\}$.

Таблица 2

Значения функции принадлежности угроз, учитываемых имеющимися вариантами системы информационной безопасности

	$Threat_1$	$Threat_2$	$Threat_3$	$Threat_4$	$Threat_5$
Var_1	0,5	0,0	0,8	0,5	0,7
Var_2	0,2	0,1	0,8	0,0	0,4
Var_3	0,6	0,4	0,8	0,5	0,7
Var_4	0,3	0,7	0,8	0,2	0,9
Var_5	0,5	0,5	0,8	0,6	0,75
Var_6	0,4	0,25	0,7	0,3	0,6
Var_7	0,5	0,2	0,75	0,4	0,65
Var_8	0,2	0,5	0,3	0,1	0,5
Var_9	0,45	0,1	0,2	0,9	0,5
Var_{10}	0,6	0,2	0,1	0,7	0,4

Таблица 3

Значения функции принадлежности угроз, присущих ситуациям, для которых необходимо выбрать вариант системы информационной безопасности

	$Threat_1$	$Threat_2$	$Threat_3$	$Threat_4$	$Threat_5$
Sit_1	0,5	0,1	0,8	0,4	0,7
Sit_2	0,3	0,1	0,6	0,5	0,3
Sit_3	0,4	0,1	0,2	0,3	0,4
Sit_4	0,3	0,1	0,2	0,3	0,3
Sit_5	0,3	0,4	0,4	0,1	0,5

Таблица 4

Значения функции принадлежности угроз для базовых ситуаций

	$Threat_1$	$Threat_2$	$Threat_3$	$Threat_4$	$Threat_5$
Inf Sit	0,2	0,1	0,2	0,1	0,3
Sup Sit	0,5	0,4	0,8	0,5	0,7
Sit^B	0,45	0,2	0,55	0,4	0,55
Sit^G	0,35	0,25	0,5	0,3	0,5

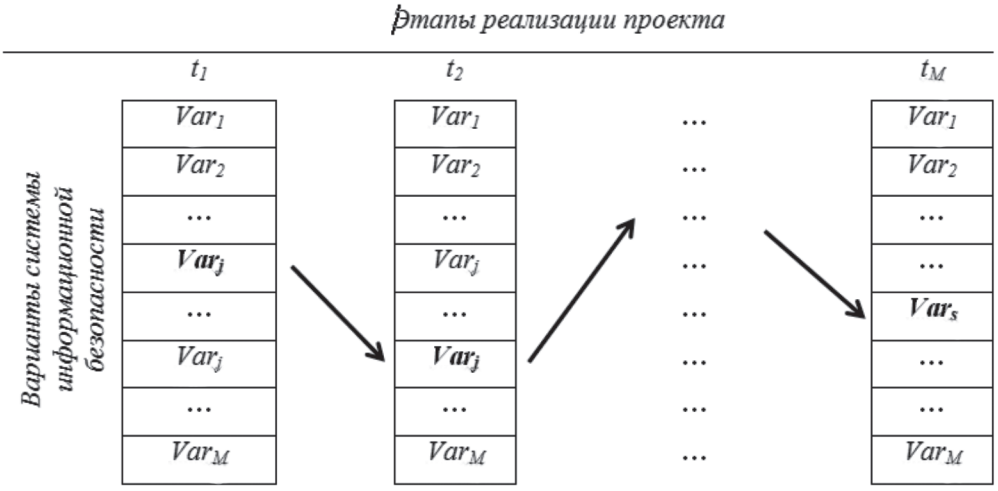

Схема переходов между реализованными в разные периоды проекта вариантами системы информационной безопасности в рамках составного варианта

Окончательный выбор варианта системы информационной безопасности проекта производится лицом, принимающим решение (ЛПР), с учетом принципа минимальности затрат на основе собственных (зачастую неформализуемых) представлений или путем проведения опытной эксплуатации системы.

В качестве обобщения задачи выбора одного варианта системы информационной безопасности, постоянно используемого в течение всего периода реализации проекта, рассмотрим возможность перехода от одного варианта системы информационной безопасности к другому. При этом будем полагать, что ранее рассмотренная задача решается K раз для каждого этапа реализации проекта t_k (k = 1,2,..., K). Это увеличивает общее количество возможных составных вариантов системы информационной безопасности с M до M^K (рисунок).

Таким образом, составной вариант (план развития) системы информационной безопасности *Plan* можно представить в виде кортежа вариантов

$$Plan = (Var_1, Var_2,\ldots, Var_K),$$
$$Plan \in Plans = (Variants)^K,$$

после чего множество выбора *Plans* может быть (с использованием одной из приведенных стратегий) сокращено до $Plans^* = (Variants^*)^K$, где $(Variants)^K$, $(Variants^*)^K$ – декартовы степени соответствующих множеств.

Обобщенная задача выбора состоит в определении минимального по затратам плана развития системы информационной безопасности

$$F(Plan) \rightarrow \min,\ Plan \in Plans^*,$$

где общие затраты составного варианта определяются не только затратами простых вариантов, но и «ценой перехода» от одного варианта к другому:

$$F(Plan) = \sum_{Var_k \in Varients^*} f_k(Var_k) + \sum_{(k,r)\in L} g_{kr},$$

где g_{kr} – затраты, связанные с переходом от варианта системы информационной безопасности Var_j к варианту Var_r, а L – список планируемых переходов.

В обобщенном случае (хотя возможность сокращения области выбора здесь имеет еще большее значение) задача сводится к синтезу больших дискретных систем с заданным конечным набором возможных состояний и переходов, и для ее решения (чтобы уйти от полного перебора вариантов) целесообразно использовать эвристические процедуры на базе генетических алгоритмов [14].

Предлагаемая процедура поддержки принятия решений по составлению плана развития системы информационной безопасности включает в себя следующие этапы:

1. Формирование перечня ситуаций с указанием входящих в их состав угроз информационной безопасности проекта.

2. Экспертная оценка ситуаций и определение уровней угроз для разных ситуаций на каждом этапе реализации проекта.

3. Сокращение общего числа ситуаций за счет объединения (пересечения) отдельных ситуаций.

4. Построение базовых ситуаций с использованием выбранных стратегий для каждого этапа реализации проекта.

5. Формирование перечня имеющихся вариантов системы информационной безопасности и соответствующих им ситуаций.

6. Сокращение перечня вариантов с использованием построенных базовых ситуаций.

7. Определение минимального по затратам (возможно, составного) варианта на основе сокращенного перечня вариантов системы информационной безопасности.

Заключение

Предложенный подход к проблеме выбора вариантов системы информационной безопасности проектов, основанный на применении нечеткого теоретико-множественного аппарата и методов теории принятия решений, позволил структурировать совокупность возможных ситуаций (рассматриваемых с точки зрения угроз информационной безопасности) и сформулировать постановку задачи выбора минимального по затратам варианта, обеспечивающего достаточную (в соответствии с выбранными стратегиями) информационную безопасность инновационного проекта. Предварительные результаты применения основанной на этом подходе процедуры поддержки принятия решений по составлению плана развития системы информационной безопасности показали ее эффективность.

Работа выполнена при финансовой поддержке РФФИ в *рамках научного проекта №* 15-07-01711.

Список литературы

1. Паринов А.В. Анализ проблем системы защиты инновационных проектов и основных направлений их решения / А.В. Паринов, А.С. Паринова // Вестник Воронежского института ФСИН России. – 2013. – № 2. – С. 80–83.

2. Ершов А.С. Безопасность интеллектуального капитала малых инновационных предприятий/ А.С. Ершов // Наука и бизнес: пути развития. – 2012. – № 4. – С. 69–73.

3. Лапсарь А.П. Обеспечение безопасности инновационных разработок в условиях конкурентного противостояния/ А.П. Лапсарь, С.А. Лапсарь // Финансы и кредит. – 2017. – Т. 23, № 1 (721). – С. 49–62.

4. Мирских И.Ю. Информационные аспекты реализации и защиты инноваций на промышленных предприятиях / И.Ю. Мирских, Ж.А. Мингалева // Экономика и предпринимательство. – 2016. – № 5 (70). – С. 374–376.

5. Северин В.А. Теоретико-методологические основы обеспечения безопасности коммерческих структур в информационной сфере / В.А. Северин // Информационное право. – 2016. – № 4. – С. 13–19.

6. Любченков А.В. Проблемы организационно-правовой защиты конфиденциальной информации в инновационных процессах/ А.В. Любченков // Информация и безопасность. – 2012. – Т. 15, № 3. – С. 337–344.

7. Стерхов А.П. Проблемы информационно-аналитического обеспечения безопасности инновационного бизнеса / А.П. Стерхов // Вестник Иркутского государственного технического университета. – 2015. – № 8 (103). – С. 213–220.

8. Zadeh L.A. Fuzzy Sets / L.A. Zadeh // Information and Control. – 1965. – Vol. 8. – P. 338–353.

9. Ларичев О.И. Теория и методы принятия решений / О.И. Ларичев. – М.: Логос. – 392 с.

10. Ляпина И.Р. Информационная безопасность малых инновационных предприятий / И.Р. Ляпина, Е.В. Сибирская, Е.В. Петрухина, О.А. Строева // Теоретические и прикладные вопросы экономики и сферы услуг. – 2013. – № 9. – С. 84–89.

11. Бельфер Р.А. Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств / Р.А. Бельфер, Д.А. Калюжный, Д.В. Тарасова // Вопросы кибербезопасности. – 2014. – № 1(2) – С. 33–39.

12. Ломазов А.В. Формирование иерархии оценочных показателей сложных динамических систем на основе экспертных технологий / А.В. Ломазов, В.А. Ломазов, Д.А. Петросов // Фундаментальные исследования. – 2015. – № 7–4. – С. 760–764.

13. Саати Т.Л. Принятие решений. Метод анализа иерархий / Т.Л. Саати. – М.: Радио и связь, 1989. – 316 с.

14. Petrosov D.A. Large discrete systems evolutionary synthesis procedure / D.A. Petrosov, V.A. Lomazov, A.I. Dobrunova, S.I. Matorin, V.I. Lomazova // Biosciences Biotechnology Research Asia. – 2015. – Т. 12, № 2. – P. 1767–1775.