Разработка методов и алгоритмов проверки работы предприятия с точки зрения информационной безопасности его функционирования

Е.Н. Остроух[1], Ю.О. Чернышев[1], С.А. Мухтаров[2], Н.Ю. Богданова[1]

[1]Донской государственный технический университет, Ростов-на-Дону
[2]Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Аннотация: В работе рассмотрена проблема функционирования сложного инновационного предприятия, разрабатывающего современные наукоемкие технологии и изделия, поэтому вопросы, связанные с защитой информации на всех уровнях работы такого предприятия являются весьма актуальными и важными. Выделяются наиболее важные звенья и параметры контроля, регламентируется его периодичность. С математической точки зрения проблема сводится к решению оптимизационной задачи, поставленной в виде задачи оптимального распределения ресурсов со скалярным или векторным критерием оптимизации. Предложено несколько подходов (методов и алгоритмов) решения этой задачи. Используя предложенную методику, можно провести проверку работы предприятия с точки зрения обеспечения информационной безопасности в приемлемое время и с приемлемой точностью.

Ключевые слова: параметры контроля, скалярный, векторный критерий, тестирование, оптимизация.

Для инновационного предприятия должна быть обеспечена защищенность корпоративных информационных систем, служебной информации, а также интеллектуальной собственности от внешних посягательств. Система мер по защите информации требует комплексного подхода к решению вопросов защиты и включает не только применение технических средств, но и, в первую очередь, организационно-правовых мер защиты. Защита - система мер по обеспечению безопасности с целью сохранения коммерческих секретов. Защита обеспечивается соблюдением режима секретности, применением охранных систем сигнализации и наблюдения, использованием шифров и паролей. Защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть является процессом, направленным на достижение этого состояния [1].

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы идентификации. К биометрическим системам защиты информации относятся системы идентификации: по отпечаткам пальцев; характеристике речи; радужной оболочке глаза; по изображению лица; по геометрии ладони руки. Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными. Итак, перечислим виды защиты информации: от сбоев оборудования, от случайной потери и искажения информации, хранящейся на компьютере; от преднамеренного искажения (компьютерные вирусы, черви и т.д.); от несанкционированного доступа к информации (ее использования, изменения, распространения).

Вследствие сказанного выше, для периодического контроля систем, обеспечивающих безопасность информационных потоков различной природы на предприятии, следует выделить список направлений проверки: организационная работа руководителя; допуск к конфиденциальной информации; ведение конфиденциального делопроизводства; организация работ с инновационными ресурсами; режим секретности; использование биометрических средств защиты информации; защита от сбоев оборудования и т. д. Количество параметров направлений проверки регламентируется руководством предприятия, практически таких параметров порядка десяти. Обозначим их: H_1, $H_{2,\ldots,}$ H_k, $k \approx 10$. Каждый из параметров направлений проверки может быть проконтролирован по n показателям: режим конфиденциальности; разграничение по допуску к инновационной информации; степень защиты от сбоев и искажений; степень защиты от несанкционированного доступа, особенно к инновационной информации. Таких показателей обычно используется порядка 4-5 наименований. Обозначим их: P_1, P_2,…, P_n, $n \approx 4$.

На проведение контрольных мероприятий по k направлениям, каждое из которых характеризуется n показателями, требуются весьма большие временные затраты (8-48 часов), проверить абсолютно все показатели не представляется возможным в отведенный ресурс времени. Поэтому необходимо разработать оптимальную стратегию контроля, с учетом проверки доминирующих направлений (критерии оптимизации) и ограничений на ресурсы (качество показателей по направлениям должно быть приемлемым и дифференциально оцениваемым). Процесс контроля можно представить в виде рис.1.

Направления проверки	Показатели			
	P_1	P_2	P_3	P_4
Направление H_1	x_{11}	x_{12}	x_{13}	x_{14}
	a_{11}	a_{12}	a_{13}	a_{14}
Направление H_2	x_{21}	x_{22}	x_{23}	x_{24}
	a_{21}	a_{22}	a_{23}	a_{24}
Направление H_3	x_{31}	x_{32}	x_{33}	x_{34}
	a_{31}	a_{32}	a_{33}	a_{34}
Направление H_4	x_{41}	x_{42}	x_{43}	x_{44}
	a_{41}	a_{42}	a_{43}	a_{44}

Рис.1 - Направления и показатели контроля

Пусть x_{ij} – реальная оценка i-го направления проверки по j-му показателю, i=1,2,…,k; j=1,2,…,n; a_{ij} – предельная величина оценки i-го направления проверки по j-му показателю, i=1,2,…,k; j=1,2,…,n. При этом для $j \in J_1$: $x_{ij} \le a_{ij}$; $j \in J_2$: $x_{ij} \ge a_{ij}$; $J_1 \cup J_2 = n$. В зависимости от значимости показателей контроля можно выделить какой-либо показатель, с нашей точки зрения, наиболее значимый, в критерий оптимизации, остальные образуют систему ограничений. Получается задача со скалярным критерием. Если весьма значимых показателей несколько, то получаем оптимизационную задачу с векторным критерием. Итак, если оценка показателя осуществляется по направлениям H_1, H_2,…, H_k , k≈10,то x_{1j} соответствует проверке показателя P_1 по направлению проверки H_j, j=1,2,…,n.

В рассмотренной нами концепции и особенности типа предприятия при контроле показателей рассматриваются проблемы, связанные с человеческим фактором, поэтому целесообразно использовать тесты. При использовании тестовых технологий при контроле принято, исходя из 100-бальной шкалы, оценку “удовлетворительно” ставить при наборе 50-66 баллов, “хорошо”- при наборе 67-75 баллов, ”отлично”- при наборе 76 баллов и выше. Тесты, прежде чем их использовать при реальном контроле, должны быть неоднократно “прокручены” в экспериментальном режиме с различными группами экспертов. Это дает определенную гарантию их валидности и достоверности. Одновременно вычисляется “вес” каждого тестового задания [2,3]. Можно предложить несколько моделей контроля.

Рассмотрим модель для случая, когда показатели P_i весьма дифференцированы по значимости и экономическому ущербу: одни требуют очень высокой степени оценки, которая может быть приемлемой, если она не ниже, допустим, 80 баллов, в других же случаях, оценка в 50 баллов будет нормой. Поэтому, вследствие ограниченности времени контроля, следует выделить наиболее значимые показатели, проверка которых по различным направлениям гарантирует эффективность работы предприятия в целом, т.е., проведем сортировку показателей контроля P_i по их убыванию. Контроль начинается с проверки некоторого подмножества наиболее значимых показателей J_3 (на практике таких показателей 1-2). Только при получении приемлемых результатов при проверке этих показателей переходим к контролю следующих показателей. В случае хотя бы одного отрицательного результата контроля доминирующих показателей процесс контроля прекращается с общей оценкой для предприятия – “неудовлетворительно”. В случае положительных оценок на данном этапе переходим к контролю следующих (менее значимых) показателей. При контроле этой группы показателей допустимы отрицательные оценки для

каких-либо элементов x_{ij}, i= 3,4,…,k, (k=1,2 выбраны на предыдущем шаге). Конечно, регламентируется количество полученных отрицательных показателей на данном шаге. В зависимости от этого по окончанию контроля делается вывод об эффективности функционирования предприятия по контролируемым параметрам в целом. Блок-схема алгоритма, реализующего данную модель, представлена на рис.2. Здесь тестовые задания разбиты на два блока: D_1 (в данном массиве представлены тестовые задания для важнейших показателей P_i в количестве m из общего числа N; получение хотя бы одного неверного ответа на вопросы данного блока приводит к отрицательной оценке контроля в целом, прекращению тестирования, выдаче соответствующего сообщения и переаттестации) и D_2 (в данном массиве представлены тестовые задания для "менее важных" показателей P_2 в количестве N-m заданий; здесь $l_{пред}$- предельно допустимое число ошибочных ответов). В качестве исходной информации задаются следующие величины: c_{ij} – "цены" или "веса" тестовых заданий для контроля показателей i по направлению j; $T_{пред}$ – предельное время тестирования. Параметры, представленные в блок – схеме имеют следующий смысл: c – сумма набранных баллов при контроле; k-количество правильных ответов; T-суммарное время тестирования; l – число ошибочных ответов; τ_{ij} – время, потраченное на контроль соответствующего параметра.

Другим подходом может быть такой, когда значимость показателей контроля примерно одинакова. Количество тестовых заданий по каждому показателю i составляет не менее 50. Используется адаптивная стратегия тестирования, состоящая в том, что тесты разбиваются на 3 блока, самый

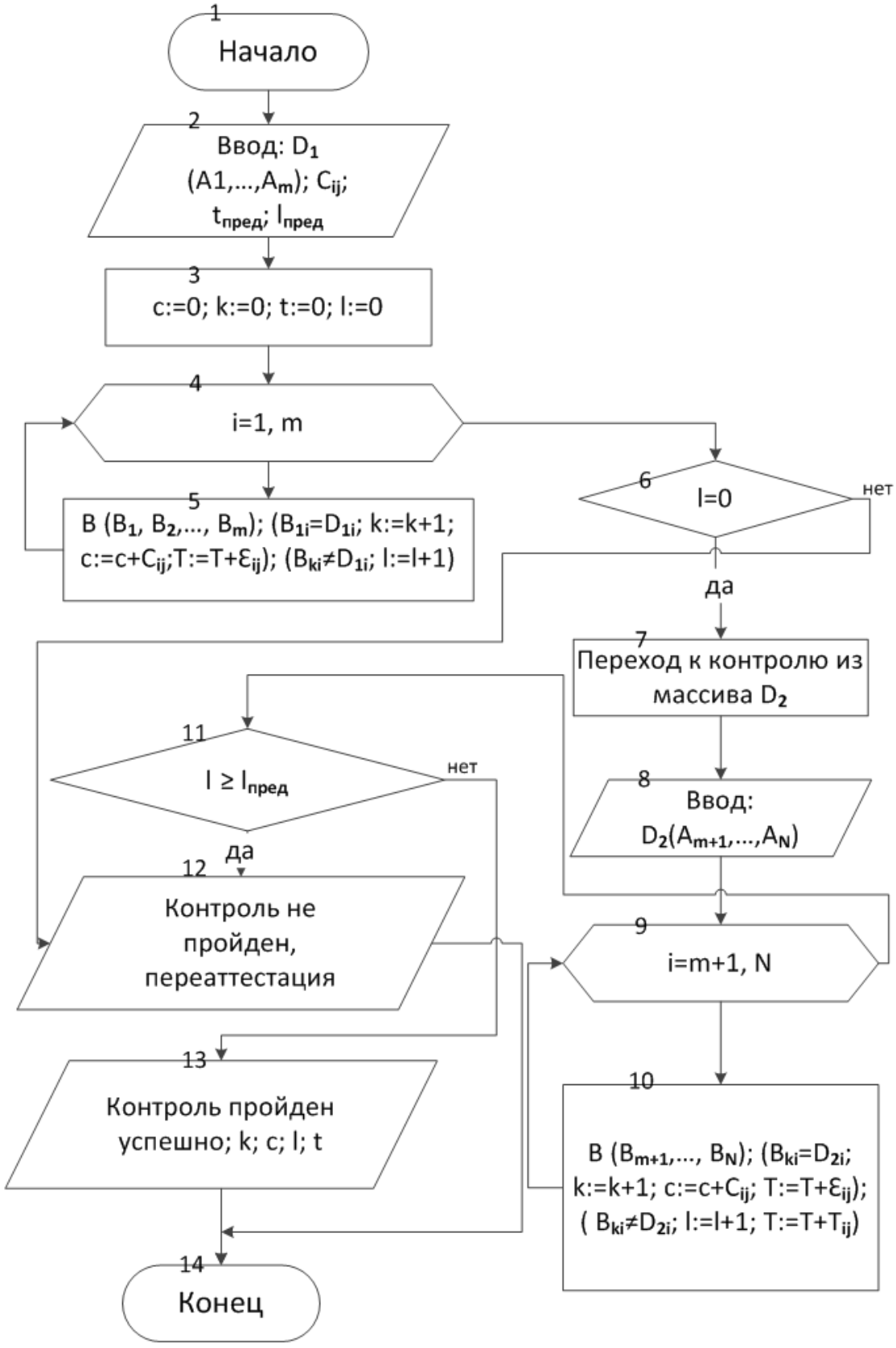

Рис. 2 – Схема контроля с учетом доминирующих показателей

“дорогой”- 1-й, затем 2-й и 3-й. Алгоритм (программа) сначала случайным образом вызывает тестовые задания из каждого блока. В случае 3-х правильных подряд ответов выбираются вопросы из 1-го и 2-го блока (более дорогие), затем процесс повторяется. Если ответы вновь являются удачными, то вопросы – только из 1-го блока. В случае 2-х подряд неудачных ответов возвращаемся к генерации вопросов из более простых блоков. На каждом этапе фиксируются неправильные ответы, а в целом вычисляется сумма набранных “весов”, соответствующих правильным ответам. Сочетание количества ошибок и суммы набранных баллов позволит сделать вывод об оценке работы предприятия по выбранным показателям в целом. Схему работы алгоритма можно несколько упростить, если разбить исходный массив тестовых заданий на два массива: D1 и D2.

В массиве D1- более сложные вопросы (тестовые задания), оцениваемые более “дорогими” баллами каждое, например, от 5 до 7 баллов, их число – m; в массиве D2 –вопросы (тестовые задания) проще, оцениваемые, например, от 1 до 4 баллов каждое, их число –N-m. Блок-схема алгоритма, реализующего данную модель, представлена на рис.3.

Здесь тестовые задания разбиты на блоки D_1 и D_2; c_{ij} – “цена” тестового задания для контроля показателя i по направлению j; τ_{ij} - время, реализации данного тестового задания; $T_{пред}$ - суммарное время, выделенное на контроль в целом. Параметры, представленные в блок – схеме, имеют следующий смысл: c – сумма набранных баллов при контроле; k-количество правильных ответов; T- суммарное время тестирования; l – число ошибочных ответов; τ_{ij} – время, потраченное на контроль соответствующего параметра.

Замечания:

- в блоке 6, если ответ B_i в задании D_i верен, то пополняется сумма набранных баллов c и количество правильных ответов k;

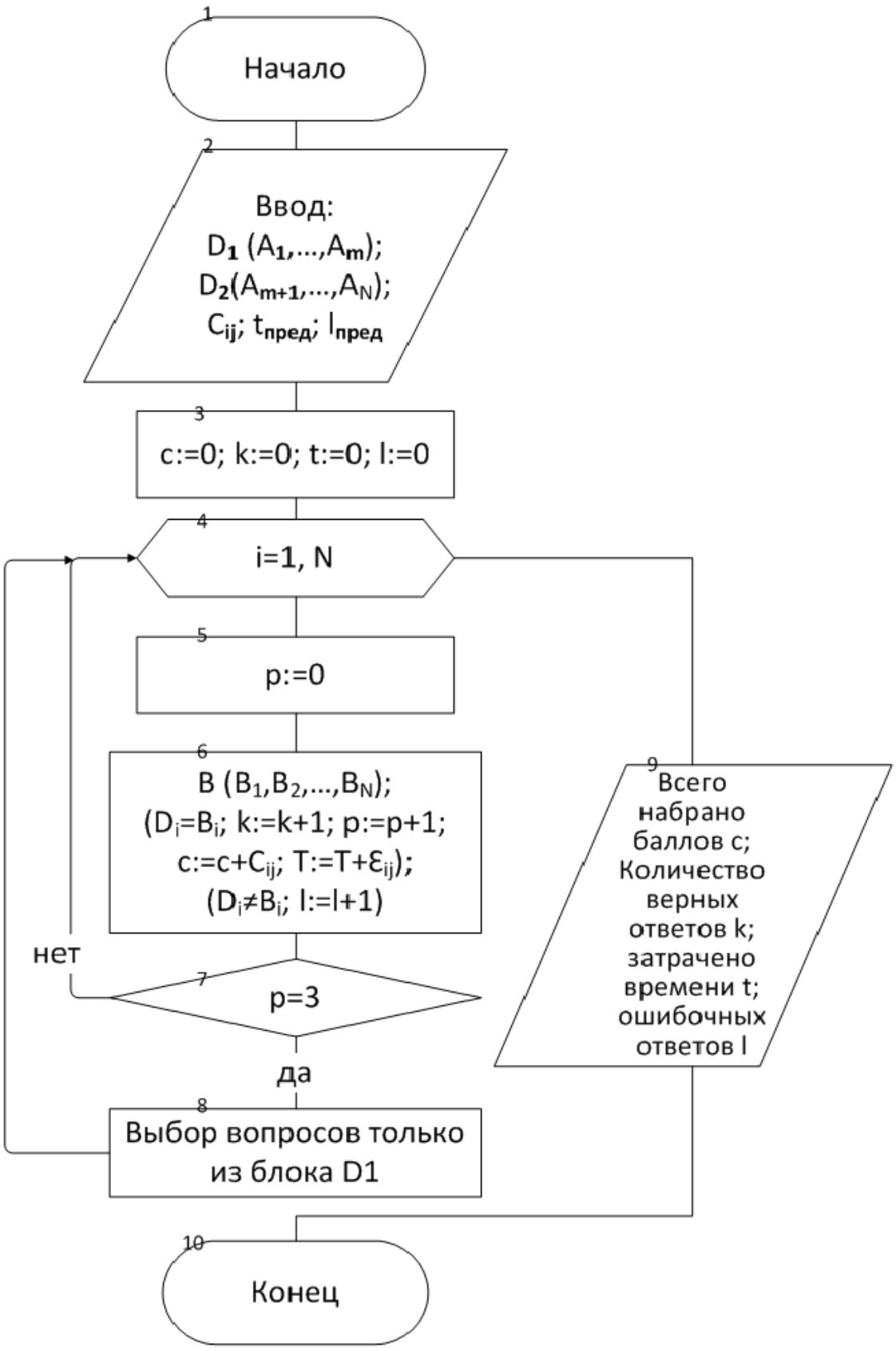

Рис. 3 – Блок-схема контроля (адаптивная модель тестирования)

- при выполнении условия (блок 7) в случае трех подряд правильных ответов, т.е., при p=3, переходим к вопросам только из “дорогого” блока D1, в противном же случае тестовые задания выбираются случайным образом из блоков D_1 и D_2.

В том случае, когда специфика предприятия предполагает использование для контроля сложных и громоздких тестов, а для реализации тестирования – больших затрат времени, вследствие чего невозможно провести проверку абсолютно всех показателей по всем направлениям, задача может быть сформулирована в виде задачи дискретного программирования с одним или несколькими критериями и булевыми переменными. В качестве исходной информации в задаче присутствуют временные характеристики контроля, т.е., задана матрица T= $[\![t_{ij}]\!]$ - время проверки показателя i по направлению j.

Итак, оптимизационная задача формулируется следующим образом:

$$\sum_{i=1}^{k}\sum_{j=1}^{n} c_{ij}x_{ij} \to \max, \qquad (1)$$

при наличии ограничений: $A \le \sum_{j=1}^{n} t_{ij}x_{ij} \le B$, i=1, 2,…, k, (2)

x_{ij}=1, если показатель P_i контролируется по направлению H_j и x_{ij}=0, если контроль не производится, i=1,2,…,k; j=1, 2,…,n. (3)

Из соображений практики следует, что A≈8 (часов), B≈12 (часов).

c_{ij} - оценка проверки показателя i по направлению проверки j, полученная в результате тестирования (“вес” тестовых заданий использованных валидных тестов).

Целевую функцию (1) можно представить также в таком виде:

$\sum_{j=1}^{n} c_j \sum_{i=1}^{k} x_{ij} \to \max$, если известны экспертные оценки значимости показателей c_j.

Оптимизационная задача организации контроля (в постановке (1)-(3)) сравнительно несложно решается рядом известных детерминированных алгоритмов, таких как метод ветвей и границ, метод Балаша, так и достаточно эффективным методом, предложенным авторами данной работы [4].

В случае более сложной целевой функции (1) и временных ограничений (2) (нелинейность, дискретность и т.д.) целесообразно использовать биоинспирированные алгоритмы, такие как генетические, роевые, муравьиные и иммунные, в том числе используя разработанные авторами данной работы методы и алгоритмы [5-14].

В случае векторного критерия (1) или сетевой постановки исходной задачи авторами предложены методы и алгоритмы [15,16].

Статья написана при поддержке РФФИ в рамках выполнения грантов 16-01-00-391и 15-01-05-129.

Литература

1. Чернышев Ю.О., Сергеев А.С., Дубов Е.О. и др. Биоинспирированные алгоритмы решения задач криптоанализа классических и асимметрических криптосистем: монография/ Краснодар: КВВУ, 2015.-132 с.

2. Остроух Е.Н. Золотарев А.А., Демидов А.А., Солопова О.Г. Система интерактивного тестирования //Современные проблемы многоуровневого образования: материалы VI междунар. науч.- метод. симп. ДГТУ.- Ростов н/Д, 2011.- С. 235-238.

3. Остроух Е.Н., Остроух Т.А. Оптимальные подходы в подготовке учащихся к контролю знаний в форме тестирования // Актуальные проблемы педагогической диагностики и мониторинга системы образования: тр. межрегион. семинара. - Таганрог, 2003- С.18.

4. Остроух Е. Н., Чернышев Ю.О. Алгоритм решения одного класса задач целочисленного линейного программирования (ЦЛП) // Вы-

числительная техника и моделирование сложных систем в гражданской авиации.-1976. Вып.2.- С. 63-66.

5. Чернышев Ю.О., Басова А.В., Полуян. А.Ю. Решение задач транспортного типа генетическими алгоритмами. - Ростов н/Д: ЮФУ, 2008.-88с.

6. Chernyshev Yu.O. Intelligentalgorithmus für Datenzugriff- Optimierung auf der Basis eines Anpassungsautomaten /Yu.O. Chernyshev, N.N. Wenzow/ KYBERNETIKA. - 2010. - № 2, pp. 5-9.

7. Остроух Е.Н., Бычков А.А., Золотарев А.А. Оптимизация экологических затрат на молкомбинате //Современные наукоемкие технологии.-2011.-№4.- С. 45-47.

8. Остроух Е.Н., Солопова О.Г., Кулешова Е.Ю. Нахождение оптимальной стратегии функционирования многономенклатурного пищевого предприятия с использованием генетических алгоритмов и метода роя частиц //Международный научно-исследовательский журнал.-2014.-№ 5(24), ч.1.- С.13-16.

9. Чернышев Ю.О., Полуян А.Ю., Панасенко П.А., Паскевич Д.Ю. Бионический поиск решения задач транспортного типа на основе стратегии адаптации/ //Вестник ДГТУ, 2015, №2.- С. 63-69.

10. Остроух Е.Н., Золотарева Л.И., Бычков А.А. и др. Векторная оптимизация перерабатывающих процессов с учетом сырьевого дефицита/ //Фундаментальные исследования.-2011.-№12(часть1).- С. 224-227.

11. Dasgupta D. Information Processing in the Immune System/ D. Corne, M. Dorigo & F. Glover, McGraw Hill // New Ideas in Optimization.-London, 1999. - pp.161-165.

12. Венцов Н.Н., Долгов В.В., Подколзина Л.А. Об одном способе построения запросов к базе данных на основе аппарата нечеткой логики //Инженерный вестник Дона. - 2015.- №3.- URL: ivdon.ru/ru/magazine/archive/n3y2015/3172.

13. Valiant Leslie. Probably Approximately Correct: Nature's Algorithms for Learning and Prospering in a Complex World. New York: Basic Books, 2013. - 208 p.

14. Чернышев Ю.О., Венцов Н.Н., Панасенко П.А. Исследование вариантов адаптивного анализа решений оптимизационных задач на основе логик Райхенбаха и Лукасевича //Инженерный вестник Дона - 2015.- №2, ч.2.- URL: ivdon.ru/ru/magazine/archive/n2p2y2015/3045.

15. Остроух Е.Н., Солопова О.Г. Сетевая модель функционирования многономенклатурного пищевого предприятия //Междунар. научно-исследовательский журнал, 2013, № 7(14). Часть 1.- С.134.

16. Остроух Е.Н., Солопова О.Г. Математическая модель функционирования молкомбината в форме задачи о максимальном потоке с векторным критерием //Электронные ресурсы в непрерывном образовании (”ЭРНО-2010”):тр. Междунар. науч.-метод. симп., - г. Туапсе. - Ростов н/Д: Изд-во ЮФУ, 2010.- С. 9.

References

1. Chernyshev Yu.O., Sergeev A.S., Dubov E.O. i dr. Bioinspirirovannye algoritmy resheniya zadach kriptoanaliza klassicheskikh i asimmetricheskikh kriptosistem: monografiya [Bioinspired algorithms for solving problems of cryptanalysis of classic and asymmetric cryptosystems: monografiya].Yu.O. Chernyshev, Krasnodar: KVVU, 2015.132 p.

2. Ostroukh E.N. Zolotarev A. A., Demidov A.A., Solopova O.G. Sovremennye problemy mnogourovnevogo obrazovaniya: materialy VI mezhdunar. nauch. metod. simp. DGTU. Rostov n.D, 2011.pp. 235-238.

3. Ostroukh E.N., Ostroukh T.A.. Aktual'nye problemy pedagogicheskoy diagnostiki i monitoringa sistemy obrazovaniya: tr. mezhregion. seminara. - Taganrog, 2003. P.18.

4. Ostroukh E. N. , Chernyshev Yu.O. Vychislitel'naya tekhnika i modelirovanie slozhnykh sistem v grazhdanskoy aviatsii.1976. Vyp.2. pp. 63-66.

5. Chernyshev Yu.O., Basova A.V., Poluyan A.Yu. Reshenie zadach transportnogo tipa geneticheskimi algoritmami [Meeting the challenges of transport such as genetic algoritmami]. Rostov n.D: YuFU, 2008. 88p.

6. Chernyshev Yu.O. Yu.O. Chernyshev, N.N. Wenzow. KYBERNETIKA. 2010. № 2, pp. 5-9.

7. Ostroukh E.N., Bychkov A.A., Zolotarev A.A. Sovremennye naukoemkie tekhnologii. 2011. №4.pp. 45-47.

8. Ostroukh E.N., Solopova O.G., Kuleshova E.Yu. Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal. 2014. № 5(24), ch.1. pp. 13-16.

9. Chernyshev Yu.O. , Poluyan A.Yu., Panasenko P.A., Paskevich D.Yu.Vestnik DGTU, 2015, №2. pp. 63-69.

10. Ostroukh E.N., Zolotareva L.I., Bychkov A.A. i dr. Fundamental'nye issledovaniya.2011. №12 (chast'1).pp. 224-227.

11. Dasgupta D. D. Corne, M. Dorigo & F. Glover, McGraw Hill. New Ideas in Optimization. London, 1999. pp. 161-165.

12. Ventsov N.N., Dolgov V.V., Podkolzina L.A. Inženernyj vestnik Dona (Rus), 2015. №3. URL: ivdon.ru.ru.magazine.archive.n3y2015.3172.

13. Valiant Leslie. Probably Approximately Correct: Nature's Algorithms for Learning and Prospering in a Complex World. New York: Basic Books, 2013. 208 p.

14. Chernyshev Yu.O., Ventsov N.N., Panasenko P.A. Inženernyj vestnik Dona (Rus), 2015. №2, ch.2. URL: ivdon.ru.ru.magazine.archive.n2p2y2015.3045.

15. Ostroukh E.N., Solopova O.G. Setevaya model' funktsionirovaniya mnogonomenklaturnogo pishchevogo predpriyatiya. Mezhdunar. nauchno. issledovatel'skiy zhurnal,2013, № 7(14). Chast' 1. p.134.

16. Ostroukh E.N., Solopova O.G. Elektronnye resursy v nepreryvnom obrazovanii (”ERNO.2010”):tr. Mezhdunar. nauch.metod. simp., g. Tuapse. Rostov n.D: Izd.vo YuFU, 2010.P. 9.