ИНСТИТУТ ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ КН МОН РК

ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

TURAN UNIVERSITY

Lublin University of Technology

МАТЕРИАЛЫ

III МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ
«ИНФОРМАТИКА И ПРИКЛАДНАЯ МАТЕМАТИКА»
посвященная 80-летнему юбилею профессора Бияшева Р.Г.
и 70-летию профессора Айдарханова М.Б.

(ЧАСТЬ I)

26-29 сентября 2018 года

Алматы

4. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. — М: Связь, 1979. — 744 с.

5. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.

6. Ищукова Е. А., Кошуцкий Р. А., Бабенко Л. К. Разработка и реализация высокоскоростного шифрования с использованием алгоритма Кузнечик. // Auditorium: электронный научный журнал Курского государственного университета.2015. № 4 (08)

7. С. Гонсалес, Е. Коусело, В.Марков, А. Нечаев. Параметры рекурсивных МДР-кодов. Дискретная математика, т. 12, вып. 4. 2000.

8. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.:ил.

9. Олейников Р., Горбенко И. О новом украинском стандарте шифрования. // Журнал "Компьютерное обозрение", 2015г., http://ko.com.ua/o_novom_ukrainskom_standarte_shifrovaniya_110863.

10. Jorge Nakahara Jr, ElcioAbrah˜ao. A New Involutory MDS Matrix for the AES. // International Journal of Network Security, Vol.9, No.2, PP.109–116, Sept. 2009.

11. R.Elumalai, Dr.A.R.Reddy. Improving Diffusion Power of AES Rijndael with8x8 MDS Matrix. // International Journal of Scientific & Engineering Research Volume 2, Issue 3, March-2011.

ОБ ОДНОМ МЕТОДЕ ОБРАБОТКИ ЭКСПЕРТНОЙ ИНФОРМАЦИИ

Мазаков Т.Ж., Исимов Н.Т., Жолмагаметова Б.Р., Карымсакова Н.Т., Ыдырышбаева М.Б.

КазНУ имени аль-Фараби
Институт информационных и вычислительных технологий, КН МОН РК

Аннотация. *В данной статье проанализированы проблемы мониторинга и управления социально-эпидемиологической ситуации. Предложена новая математическая модель и алгоритм для обработки экспертной информации по оценке эпидобстановки с учетом эпидеомиологических, социальных и экономических показателей региона. Исследованы свойства математического алгоритма.*

Ключевые слова. *Эпидобстановка, функционал, градиентный метод.*

Введение. Одна из актуальных задач медицины состоит в своевременной профилактике различных эпидемических болезней с помощью медико-

биологических и социально-экономических мер. Своевременность и действенность медицинских мероприятий может быть обеспечена лишь при условии хорошо разработанной службы прогнозирования, которая должна предсказывать эпидобстановку в обследуемом районе в зависимости от состояния многочисленных абиотических, биотических, социальных и других факторов.

В работе [1] разработана математическая модель, учитывающая динамику и взаимосвязь абиотических и биотических факторов, характеризующих эпидобстановку в исследуемом очаге.

Основная часть

Ввиду необходимости комплексной оценки эпидемиологических, социальных и экономических показателей вводится понятие "эпидпотенциал", характеризующего эпидобстановку в районе. Обозначим его через Э. Эпидпотенциал аналогично вероятности может принимать значения от 0 до 1. Чем больше значение Э, тем больше вероятность начала эпидемии.

Пусть m – количество информационных параметров оценки социально-эпидемиологической ситуации; $x = (x_1, \dots, x_m)$ - вектор, компоненты которого характеризуют социально-эпидемиологическую ситуацию.

Определим эпидпотенциал:

$$Э = \prod_{k=1}^{m} x_k^{\alpha_k} \quad . \tag{1}$$

Формула (1) соответствует математической задаче многокритериальной оптимизации, где неизвестными являются коэффициенты α_k, определяющие влияние k –го критерия (информационного параметра) на общий результат.

Введем следующие обозначения:

K – количество экспертов;

N – количество анкет;

M=N*K – количество экспертных оценок

X_{ij} – значение i –го параметра в j –й анкеты, где $i = \overline{1,m}$, $j = \overline{1,N}$;

$Э_{ij}$ – оценка i –го эксперта в j –й анкеты, где $i = \overline{1,K}$, $j = \overline{1,N}$.

Предполагается, что

1) значения экспертной оценки удовлетворяют ограничениям $0 \le Э_{ij} \le 1$,

2) значения параметров в анкетах удовлетворяют ограничениям $1 \le X_{ij} \le 100$.

Прологарифмируем выражение (1):

$$ln Э = \sum_{k=1}^{m} \alpha_k x_k. \tag{2}$$

Коэффициенты α_k могут быть найдены из условия максимального совпадения знаний экспертов, т.е. минимума функционала

$$S = \sum_{j=1}^{N} \sum_{i=1}^{m} (\ln Э_{ij} - \alpha_i \sum_{k=1}^{N} X_{ik})^2. \quad (3)$$

Минимум функционала (3) определяется при следующих ограничениях

$$A = \left\{ 0 \le \alpha_i \le 1; \sum_{i=1}^{m} \alpha_i = 1 \right\}. \quad (4)$$

Легко показать, что А является выпуклым замкнутым множеством в пространстве R^m.

Обозначим через α_i^n n-е приближение для вычисления коэффициента α_i.

Построим итерационный процесс

$$\alpha_i^{n+1} = \Pi_A\left(\alpha_i^n - \gamma_n S'(\alpha_i^n)\right). \quad (5)$$

Здесь Π_A - оператор проектирования на множество А. Коэффициенты $\gamma_n \ge 0$, определяющие длину шага на n-м этапе, могут быть определены из условия $S(\alpha_i^n - \gamma_n S'(\alpha_i^n)) = \min_{\gamma \in R} S(\alpha_i^n - \gamma S'(\alpha_i^{k,n}))$ или в процессе дробления шага.

В качестве нулевого приближения выбирается $\alpha_i^0 = 1/m$.

Теорема. Пусть множество А выпукло и замкнуто. Тогда последовательность $\{\alpha_i^n\}$, определяемая по формуле (5) сходится к решению задачи минимизации функционала (3) на множестве (4).

Доказательство. Так как множество А является выпуклым и замкнутым, функционал (3) является выпуклым и дифференцируемым, то любая предельная точка последовательности $\{\alpha_i^n\}$ является точкой минимума [2].

Ввиду того, что эпидпотенциал – это показатель возможности заражения человека чумой в природном очаге в определенный момент времени. Нами предложен алгоритм вычисления эпидемиологического потенциала. В своей работе мы рассмотрели следующие природные очаги чумы в Казахстане: Урало-Эмбенский автономный очаг, Приаральско-Каракумский автономный очаг, Прибалхашский автономный очаг, Волго-Уральский автономный очаг, Мангышлакский автономный очаг, Зауральский автономный очаг. Основной расчет был проведен для Прибалхашского автономного очага. Использовались данные по числу Вольфа из соответствующей литературы, данные по температуре, осадкам и численности биотических факторов были модельными, приближенными к реальным.

Заключение

В статье рассмотрена математическая модель по обработке экспертной информации оценки эпидемиологической ситуации в регионе.

На основе метода проекции градиента решена задача выбора оптимальных коэффициентов для свертки многих критериев в один.

На основе теоретических результатов, опубликованных в работах [3-4], и данной статьи на СУБД VisualFoxPro 9 [5] построена экспертная система прогнозирования и управления эпидемиологической обстановкой в заданном районе. Экспертная система позволяет проводить мониторинг и прогнозирование эпедимиологических данных, а также на основе обработки анкетных данных осуществляет расчет эпидпотенциала.

Работа выполнена за счет средств грантового финансирования научных исследований на 2018-2020 годы по проекту AP05132044 «Разработка аппаратно-медицинского комплекса оценки психофизиологических параметров человека».

Литература

1. Тойкенов Г.Ч., Мазаков Т.Ж. Применение математических методов в эпидемиологии // Вестник КазГУ. Матем.,механ., информатика. N 4. – Алматы, КазГУ, 1996. с.184-189.

2. Сухарев А.Г., Тимохов А.В., Федоров В.В. Курс методов оптимизации. – М.: Наука, 1986. – 328 с.

3. Исимов Н.Т., Мазаков Т.Ж, Карымсакова Н.Т., Жолмагамбетова Б.Р., Зиятбекова Г.З. Оптимальное управление эпидобстановкой //Труды 14-й международ. азиатской школы-семинара «Проблемы оптимизации сложных систем», Кыргызская Республика, Иссык-Куль, 20-31 июля, 2018, с.250-258

4. Исимов Н.Т., Мазаков Т.Ж., Карымсакова Н.Т. Исследование модели прогнозирования и управления эпидобстановкой с применением нечеткого и интервального анализа //Научно-технический журнал «Вестник Алматинского университета энергетики и связи», спец.выпуск, 2018, с.147-155

5. Клепинин В.Б., Агафонова Т.П. Visual FoxPro 9. – Санкт-Петербург «БХВ-Петербург», 2007. – с.1216.

КУБИКИ, ПОЛУКУБИКИ, ЭЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ ПРИЛОЖЕНИЯ

Нурлыбаев А.Н., Магауин Б.А.

Алматинский университет энергетики и связи, Казахстан
e-mail: s.tynym@mail.ru

Аннотация. *Приводится краткий аналитический обзор плоских алгебраических кубических кривых, нахождения их корней и связанных с ними эллиптических кривых. Интерес к последним стимулировался с 1985 г. по двум*