ISSN 0869-8325

ТОМ 21
Выпуск 4

ОБОЗРЕНИЕ ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ МАТЕМАТИКИ

В выпуске:

Секция **«Прикладная дискретная математика»**

28.IX – 5.X • 2014

Пятнадцатый Всероссийский симпозиум
по прикладной и промышленной математике
Осенняя открытая сессия. Научные доклады. Часть I

Редакция журнала «ОПиПМ» • МОСКВА
2014

остальных автоматов получаются переопределением номера стратегии и компонент платежной матрицы.

00	... ...	... ...	... ... 0*f*
... ...	... ...	... ...	... ...
30	... ...	... ...	... ... 3*f*
40 ... **43**	44 ... **47** ... 4b	4*c* ...	**4f**
... ...	... ...	... ...	... ...
*b*0 ... *b*3	b4 ... ... bb	*bc* ...	*bf*
*c*0 ... **c3**	c4 ... **c7** ... cb	*cc* ...	**cf**
... ...	... ...	... ...	... ...
*f*0 ... *f*3	f4 ... ... fb	*fc* ...	*ff*

СПИСОК ЛИТЕРАТУРЫ

1. *Rabin M. O.* Probabilistic Automata. — Inform. Control, 1963, № 6, p. 230–245.
2. *Думачев В. Н., Пешкова Н. В., Калач А. В., Чудаков А. А.* Ситуационное моделирование прорыва противопаводковой дамбы во время аномального наводнения на дальнем востоке летом 2013 г. — Вестник Воронежского ин-та ГПС МЧС России, 2013, № 4(9), с. 35–39.
3. *Думачев В. Н., Пешкова Н. В., Калач А. В., Чудаков А. А.* Ситуационное моделирование работы Зейской ГЭС во время аномальных наводнений. — Вестник Воронежского ин-та ГПС МЧС России, 2014, № 2(11), с. 18–25.

Н. В. Евсеев, К. К. Рыбников, А. Г. Чернышова (Мытищи, МГУ леса). **Классические тренды технических и экономических процессов, основанные на методе наименьших квадратов, и перспективы их использования.**

История развития математических подходов к анализу экономических процессов вряд ли насчитывает более 100 лет. Математические модели в экономике можно разделить на два основных класса: аналитические модели и модели прогнозов. К первому классу можно отнести модели планирования, основанные на использовании методов математического программирования, а первой моделью второго класса, видимо, стала модель денежной эмиссии О. Ю. Шмидта, в 1922 году горячо обсуждаются как экономистами, так и математиками. (см., например [1]).

В дальнейшем основными моделями стали модели трендов временных рядов, где математической основной стал метод наименьших квадратов (МНК).

Реализация этого метода приводит к построению приближенной формулы:

$$f(x) \approx F(x),$$

где $f(x)$ — функция, заданная таблично $f(x_i) = y_i \quad (i = 0, 1, 2, \ldots, n)$, а $F(x) = \sum_{j=0}^{m} a_j x^i$, заключается в решении задачи выбора коэффициентов $a_0, a_1, \ldots, a_m$ таким образом, чтобы сумма $S(a_0, a_1, \ldots, a_m) = \sum_{i=0}^{n} (F(x_i) - y_i)^2$ квадратов отклонений значений функции от значений $F(x)$ в точках $x_0, x_1, \ldots, x_n$ была наименьшей.

Построение функции $F(x)$ является основой математического аппарата для определения трендов экономических процессов, по которым можно не только разрабатывать прогнозы, но и производить апостериорный анализ.

Примером первого направления может послужить прогноз индекса Nikkei 225 Токийской фондовой биржи по данным Мэрфи [2] за 1994–1998 гг. В соответствии с этими данными индекс Nikkei с апреля 1994 года по октябрь 1996 года колеблется между 375 и 395. Однако, с октября 1996 года по ноябрь 1997 года он падает с 415 до 285. Анализируя эти данные Мерфи утверждает, что построение тренда невозможно. (см. с. 41 [2]).

Однако, если взять данные только за два года (1996 и 1997) МНК приводит к построению простого квадратного тренда $F(x) = -7,5x^2 - 2,5x + 400$, где x — показатель временный шкалы.

Так для значений x, соответствующего началу 1998 года значение тренда равно 270. В действительности индекс Nikkei к началу 1998 года составил 278. Таким образом, если рассматривать значение 270 как прогноз, то его следует признать удовлетворительным.

Аналогичные прогнозы можно строить для данных Мэрфи для транспортного и промышленного индекса Dow Jones. Очевидной трудностью при определении фьючерсных прогнозов является необходимость правильно угадывать периоды, соответствующие волнам Элиота (см., например [3]). (Именно нисходящей волне Элиота соответствует рассмотренный выше период (1996–1997 гг.).)

Другим направлением в использовании трендов является апостериорный анализ.

В работах [4–6] при изучении зависимостей энергозатрат от объема производства на ряде цеховых подразделений предприятия «Воскресенские минеральные удобрения» был выделен линейный тренд. При изучении показателей значительно уклоняющихся от тренда, было выявлено, что они соответствуют отступлением от стандартного технологического режима (дополнительное плавление комовой серы, промывка цистерн, переработка кислоты повышенной концентрации). Обнаружение таких ситуаций может быть использовано в методах экологического контроля [4], [5].

СПИСОК ЛИТЕРАТУРЫ

1. *Рыбников К. К.* Математики Московского государственного университета леса. М.: ГОУ ВПО МГУЛ, 2009, 132 с.
2. *Мэрфи, Джон Дж.* Технический анализ финансовых рынков: полный справочник по методам и практике трейдинга: пер. с анг. М.: И. Д. Вильямс, 2013, 496 с.
3. *Арталь Л., Салес Ж.* Ипотека и уравнения. Математика в экономике. (Мир Математики. Т. 19.) М.: Де Агостини, 2014, 160 с.
4. *Рыбников М.К., Рыбников К. К.* Методы выявления изменений в стандартном режиме производства на химических предприятиях, производящих минеральные удобрения, как информация для экологического контроля. — В сб.: Труды международной конференции «Математические и физические методы в экологии и мониторинге природной среды», Королев–Москва, 2001, с. 238–240.

5. *Рыбников К. К.* О возможностях использования результатов анализа трендовых моделей объема энергозатрат в условиях растущего объема производства для экологического контроля. — Обозрение прикл. и промышл. матем., 2003, т. 10, в. 1, с. 213–214.
6. *Курзин П. А.*, *Курзина В. М.*, *Рыбников М.К.*, *Рыбников К. К.* Математические основы принятия управленческих решений: монография. М.: ГОУ ВПО МГУЛ, 2007, 150 с.

А. А. Елистратов, **Н. В. Никонов**, **А. О. Шумилов** (Москва, ТВП). **О паддинг-атаках на криптографические протоколы, использующие стандартные n-разрядные блочные режимы шифрования.**

Одной из первых работ, посвященных так называемым паддинг-атакам (от англ. padding-attack) на криптопротоколы TLS, IPsec и др. является работа С. Воденея [1], представленная на конференции Eurocrypt 2002. Описанная в работе [1] атака относится к классу активных атак с подобранными шифртекстами, которая позволяет без нахождения ключа найти блоки открытого текста $x_1, \ldots, x_N$ исходя из соответствующих перехваченных блоков шифртекста $y_1, \ldots, y_N$, полученных в режиме CBC ([2, 3]) и некоторой дополнительной информации. Основой данной атаки является знание того факта, что последний неполный блок непосредственно перед шифрованием в режиме CBC должен быть дополнен до полного блока известной последовательностью байтов — паддингом. Кроме того, для проведения атаки необходимо наличие «оракула», который некоторым способом сообщает об ошибке при расшифровании в случае получения неверного паддинга или другой информации, связанной с паддингом. Применительно к протоколу TLS таким оракулом может являться TLS Alert Protocol (протокол извещения, см.[4, 5]), а для IPsec — протокол ICMP (Internet Control Message Protocol, см. [6]).

В данных тезисах авторы обращают внимание на тот факт, что аналогичные атаки возможны в некоторых случаях и при использовании других режимов шифрования, в частности режимов гаммирования: CFB, OFB и CTR (см. [2, 7, 8, 9, 10]), которые не требуют дополнения последнего неполного блока до полного. Для TLS такая возможность может возникнуть в случае известных полей данных (например, для сокрытия истинной длины открытого текста) или при встраивании блочной шифрсистемы с режимами гаммирования именно как блочной шифрсистемы, а не поточной, что потребует присутствия однобайтового поля PL (Padding Length), содержащего 0. Для IPsec эта возможность обуславливается наличием однобайтовых полей PL и NH (Next Header). Данные поля (а, возможно и другие) по сути будут играть роль паддинга, что позволит находить не менее одного байта каждого блока открытого сообщения.

Пусть имеются зашифрованные блоки $y_1, y_2, \ldots, y_N$, полученные в одном из четырех упомянутых выше режимах шифрования из блоков открытого текста $x_1, x_2, \ldots, x_N$, уравнения в кратком виде для которых представлены в табл. (столбец 2).

Приведем общий алгоритм (не зависящий от вида паддинга и т. п.), основанный на содержимом табл., для определения последнего байта $x_j^{(b)}$ блока $x_j = x_j^{(1)}, x_j^{(2)}, \ldots, x_j^{(b)}$, b — размер в байтах блока шифрсистемы E_k (блочной системы шифрования с неизвестным ключом k) при условии известного паддинга. В обозначениях алгоритма $\Omega(Y)$ — результат проверки корректности паддинга у X (см. табл., столбец 4) после расшифрования сообщения (табл., столбец 3) исходя из того или иного паддинга (1 — паддинг корректен, 0 — нет).

1. Выбрать случайно $r = r^{(1)}, r^{(2)}, \ldots, r^{(b)}$;
2. Для всех возможных $r^{(b)}$ выполнить {если $\Omega(Y) = 1$, переход на 3};
3. Положить $x_j^{(b)} = (X^{(b)} \oplus r^{(b)})$, где $X^{(b)}$ — последний байт X.