

*В.М.КАРТАШОВ, д-р техн. наук, С.И.БАБКИН, канд. техн. наук, Е.Г.ТОЛСТЫХ*

## МЕТОДИЧЕСКИЕ ПОГРЕШНОСТИ ИЗМЕРЕНИЯ МЕТЕОВЕЛИЧИН ПРИ КОРРЕЛЯЦИОННОЙ ОБРАБОТКЕ СИГНАЛОВ СИСТЕМ РАДИОАКУСТИЧЕСКОГО ЗОНДИРОВАНИЯ

### Сообщение 2

#### Введение

В предыдущем сообщении [1] рассмотрено влияние ряда факторов на формирование методических погрешностей измерения метеорологических величин аппаратурой радиоакустического зондирования (РАЗ), в котором применяется корреляционная обработка принятых радиосигналов. В частности, показано, что при регистрации вертикальных температурных профилей с применением комплексной технологии обработки сигналов источником достаточно весомых методических погрешностей является отсутствие априорной информации о таких метеорологических величинах, как скорость ветра, количество водяного пара в воздухе, турбулентность атмосферы; существенным является также отсутствие информации о вертикальном распределении указанных параметров.

Данная работа посвящена оценке методических погрешностей измерения влажности воздуха, возникающих за счет априорной неопределенности высотного распределения других метеорологических величин, анализу их влияния при регистрации вертикальных профилей измеряемой метеорологической величины с использованием корреляционной обработки принятых сигналов систем радиоакустического зондирования.

#### Регистрация профилей влажности

##### 1. Анализ расчетной формулы

Известная формула для определения влажности воздуха методом двухчастотного РАЗ с использованием корреляционной обработки данных зондирования имеет вид [2]

$$e = P \cdot \exp \left\{ 0,385 \cdot \ln \left[ \frac{(C_\infty^2 - C_0^2)(f_2^2 - f_1^2)}{2C \cdot \Delta C} \right] - 7,947 \right\}, \quad (1)$$

где  $e$  – парциальное давление водяного пара, гПа;  $P$  – полное давление воздуха, гПа;  $C_0$  – скорость звука при очень малых частотах, м/с;  $C_\infty$  – скорость звука при очень больших частотах, м/с;  $f_1$  и  $f_2$  – частоты зондирующего звука, с<sup>-1</sup>;  $\Delta C$  – разность скоростей звука этих частот  $C_1$  и  $C_2$  соответственно, м/с; а  $C = \frac{C_1 + C_2}{2}$ , поскольку  $C_1 \approx C_2$  [3].

Вследствие отсутствия экспериментальных данных по измерению скоростей  $C_1$  и  $C_2$  при определении влажности воздуха двухчастотным РАЗ с корреляционной обработкой данных зондирования репрезентативность формулы (1) на практике не проверялась. Нами для оценки практической применимости указанной формулы выполнен численный эксперимент, основанный на использовании табличных данных для коэффициента молекулярного поглощения звука во влажном воздухе, приведенных в работе [4].

Авторами [5] предложено выражение, позволяющее рассчитать скорость звука  $C$  по известным параметрам зондирующей системы и найденному в эксперименте значению параметра Брэгга:

$$C = \frac{2\pi f_n}{\frac{4\pi f_e}{c} - q}, \quad (2)$$

где  $f_n$  – частота синусоидального заполнения акустического пакета;  $f_e$  – рабочая частота радиолокатора;  $c$  – скорость распространения радиоволн;  $q$  – параметр расстройки условия Брэгга.

Для численных расчетов нами использованы значения частот звука 80 и 7150 Гц, которые близки к значениям частот, используемых в известных системах РАЗ: низкочастотной (19 Гц) [6] и высокочастотной (6800 Гц) [7]. Для выбранных частот известны табличные значения коэффициентов молекулярного поглощения звука во влажном атмосферном воздухе [4]. В вычислительном эксперименте предполагалось равенство энергетических потенциалов каждого из радиоканалов. Для заданных метеорологических условий рассчитывалось ослабление принимаемой мощности в каждом канале за счет молекулярного поглощения [1, 4], определялись значения параметров  $q_1$  и  $q_2$ , после чего – значения  $C_1$  и  $C_2$ .

Наиболее неопределенным в уравнении (1) является теоретический множитель  $(C_\infty^2 - C_0^2)$ , описывающий эффекты дисперсии скорости звука во влажном воздухе. Для определения численного значения этого множителя используем приближенные формулы, приведенные в ряде работ. В частности, из работы [8] следует

$$C_\infty^2 / C_0^2 \approx 1 + \varepsilon \text{ при } \varepsilon = 0,2 \cdot 0,0032, \quad (3)$$

где  $\varepsilon$  – релаксационная сила.

Это означает, что изменение скорости звука во влажном воздухе вследствие колебательной релаксации не может быть выше 0,032 %. В то же время, в работе [9] указано, что при температуре 20°C разность скоростей звука в воздухе

$$C_\infty - C_0 = 0,12 \text{ м/с.} \quad (4)$$

Для количественной оценки значения множителя  $(C_\infty^2 - C_0^2)$  была решена система двух уравнений (3) и (4) с двумя неизвестными –  $C_\infty$  и  $C_0$ . В результате оказалось, что  $C_0 = 375 \text{ м/с}$ , а  $C_\infty = 375,12 \text{ м/с}$ . При таких значениях этих скоростей множитель  $(C_\infty^2 - C_0^2) = 90,0144 \text{ (м/с)}^2$ .

Для метеорологических условий с атмосферным давлением 1013,25 гПа, температурой 20 °C и относительной влажностью  $H = 40\%$  с использованием формулы (1) было рассчитано парциальное давление водяного пара, равное 24,9 гПа. Однако это значение не соответствует табличным данным метеорологических величин. Для согласования данных расчета и табличных данных в формулу (1) необходимо ввести корректирующий коэффициент  $k = 0,375$ , учитывающий приближения, введенные в работах [8, 9]. Тогда для заданных выше метеорологических условий парциальное давление водяного пара  $e = 9,35 \text{ гПа}$ , и это достаточно точно соответствует данным метеорологических таблиц.

Результатом проведенного анализа является рабочая формула, пригодная для расчетов влажности по данным двухчастотного радиоакустического зондирования атмосферы с корреляционной обработкой данных амплитудных измерений:

$$e = P \cdot \left\{ k \exp \left[ 0,385 \cdot \ln \frac{(C_\infty^2 - C_0^2)(f_2^2 - f_1^2)}{2C \cdot \Delta C} - 7,947 \right] \right\}, \quad (5)$$

где  $k = 0,375$  – корректирующий коэффициент.

Основываясь на результатах численного эксперимента, выполненного с учетом приближенного и нелинейного характера зависимостей, описывающих молекулярное поглоще-

ние звука в воздухе, которые представлены в работах [4, 8, 9] и использованы при выводе формулы (1), можно полагать, что доработанная формула (5) репрезентативна.

## 2. Влияние атмосферной турбулентности

При оценке возможностей метода РАЗ для измерения влажности атмосферного воздуха, различные исследователи в вопросе о влиянии турбулентности на погрешность таких измерений придерживались различных взглядов. В частности, авторы работы [7] предполагали, что одновременное (или череспериодное с последующим совмещением) измерение амплитуды принятых радиосигналов при двухчастотном РАЗ атмосферы позволяет исключать влияние турбулентности на погрешность измерения влажности на близких частотах 3400 и 6800 Гц [7]. Результаты экспериментальных исследований показали, что в условиях неподвижной атмосферы две последовательно зарегистрированные, а затем совмещенные во времени огибающие амплитуд действительно оказывались подобными по форме, но имели различные показатели экспоненты. Однако по мере возникновения и развития турбулентности степень корреляции между огибающими заметно снижалась, а результаты расчета влажности становились некорректными. Исследованиями было установлено, что теоретически неучтенная частотная зависимость коэффициента турбулентного рассеяния звука и поперечного масштаба когерентности фазового фронта звуковой волны при доплеровском двухчастотном способе амплитудных измерений влажности могли приводить к значению методической погрешности измерения в (20 – 40) % значений относительной влажности [10, 11].

Оценку влияния мелкомасштабной турбулентности на методическую погрешность измерения влажности воздуха рассматриваемым способом проведем, используя методику работы [1] с учетом особенности способа: для получения информации о количестве водяного пара в воздухе необходимо применять пару звуковых частот. Сделаем это для двухчастотной системы РАЗ [7], с помощью которой были получены экспериментальные результаты измерения влажности амплитудным способом. Такой подход позволит сравнить значения методических погрешностей измерения влажности при доплеровской и корреляционной обработках принятых сигналов.

Хорошо известно, что основными факторами, влияющими на среднюю принимаемую мощность приемником системы РАЗ в дециметровом диапазоне длин волн, являются частотный характер зависимости коэффициента турбулентного рассеяния звука и нарушение поперечной когерентности фазового фронта акустической волны [4, 10, 11]. Преобладающим фактором из двух указанных является деформация фазового фронта акустической волны [12]. Поэтому оценим влияние только эффекта нарушения поперечной когерентности фазового фронта акустической волны.

С этой целью проведем расчеты, используя выражения (3) – (8) из работы [1], для двух рабочих частот звукового излучателя указанной выше системы РАЗ (3400 и 6800 Гц) при следующих метеорологических условиях: полное атмосферное давление 1022,25 гПа, температура воздуха 293,15 К, относительная влажность воздуха 40 %. Результаты расчетов показали, что при выполнении измерений влажности воздуха на высотах 50 и 100 м, с помощью известной двухчастотной системы РАЗ [7] и применения корреляционной обработки амплитуды принятых радиосигналов, методическая погрешность измерений может достигать 100 % от значений относительной влажности, даже при термической турбулентности. Такой результат может оказаться естественным для использованных в расчетах значений технических параметров этой двухчастотной системы РАЗ с произвольно выбранными рабочими частотами и конструкцией антенных устройств радио- и звукового каналов.

Прежде всего, это малый разнос зондирующих частот (эффекты дисперсии скорости во влажном атмосферном воздухе при небольшом разnose звуковых частот проявляются слабо). В работе [3] показано, что в зависимости от количества водяного пара в атмосфере положение релаксационной частоты, а с ней и дисперсионной ступеньки, меняется на частотной оси. Поэтому для минимизации методической погрешности измерений влажности в заданных

метеоусловиях необходимо выбирать зондирующие звуковые частоты так, чтобы они располагались на верхней и нижней границах дисперсионной ступеньки.

Кроме того, конструкция антенных устройств данной системы не соответствует требованиям формирования необходимой области взаимодействия радио- и звукового пучков [4]. Поэтому при разработке двухчастотных систем РАЗ для экспериментальных исследований по дистанционной регистрации вертикальных профилей характеристик влажности с заданной методической погрешностью и с использованием корреляционной обработки принятых радиосигналов следует учитывать эти особенности рассматриваемого способа. Поиск пары оптимальных частот для зондирования с целью минимизации методической погрешности измерения влажности в условиях турбулентной атмосферы является предметом дальнейших исследований.

### 3. Влияние горизонтального ветра на погрешность измерений

Одним из метеорологических факторов, влияющих на погрешность измерения влажности воздуха рассматриваемым способом, является горизонтальный ветер. Вследствие влияния этого фактора происходит вынос горизонтальным ветром акустических пакетов двух частот из диаграмм направленности антенн радиоканалов и наблюдается “соскальзывание” обоих пятен рассеянных сигналов с апертуры приемных радиоантенн.

При измерении влажности воздуха на заданной высоте и отсутствии априорной информации о вертикальном распределении горизонтальной скорости ветра к значению разности скоростей распространения звуковых частот  $C_1$  и  $C_2$ , которое определяется количеством водяного пара в атмосфере, добавляется значение разности скоростей  $\Delta C_q$ , вызванное изменением параметра Брэгга за счет неопределенности влияния скорости ветра на каждый из двух зондирующих пакетов на высоте регистрации. Это явление может стать причиной возникновения методической погрешности измерения влажности при произвольном выборе технических параметров (в частности, параметров антенных устройств) двухчастотной зондирующей системы и использовании корреляционной обработки данных зондирования. Условия, при которых влияние данного фактора при измерении влажности воздуха двухчастотным РАЗ и использовании в качестве информационного параметра принятых радиосигналов их амплитуды исключается, а методическая погрешность минимизируется, подробно рассмотрены в работе [7]. Важнейшим из этих предпосылок является условие

$$\frac{\Theta_1}{\Theta_2} = \frac{\lambda_{e1}}{\lambda_{e2}}, \quad (6)$$

где  $\Theta$  – ширина диаграмм направленности антенн обоих радиоканалов,  $\lambda_e$  – рабочая длина волн этих каналов.

Другим необходимым условием выбора оптимального режима работы двухчастотной системы РАЗ является использование одинаковых значений количества длин волн в акустических пакетах обоих каналов  $N_1 = N_2$  (7). При выполнении этого условия обеспечивается равенство значений ширины главных лепестков зависимости мощности рассеяния Брэгга на обеих частотах:

$$p^2_1 = f_1\left(\frac{\lambda_{e1}}{\lambda_{a1}}\right) \quad \text{и} \quad p^2_2 = f_2\left(\frac{\lambda_{e2}}{\lambda_{a2}}\right). \quad (8)$$

### 4. Влияние вертикальных градиентов температуры воздуха и скорости ветра

Возможный вклад вертикальных градиентов температуры воздуха и скорости ветра в методическую погрешность регистрации вертикального профиля влажности воздуха оценим, опираясь на результаты работы [1]. Как показал анализ, существование вертикальных градиентов основных метеорологических величин приводит к изменению уровня мощности при-

нимаемого сигнала по сравнению с тем, который заложен для корреляционной обработки сигнала, что и приводит к появлению методической погрешности. Однако, если при создании двухчастотной системы РАЗ для дистанционной регистрации вертикальных профилей влажности воздуха с использованием корреляционной обработки принятых радиосигналов выполнены условия (6) и (8) и число волн в звуковых посылах обеих частот одинаково (условие (7)), то сужение (или расширение) диаграмм направленности обоих акустических излучателей под действием вертикального градиента температуры воздуха происходит синхронно и одинаково, а разворот их фазовых фронтов под действием вертикального градиента скорости ветра также оказывается равным. В таком случае дополнительной разности потерь мощности принимаемых радиосигналов в обоих каналах не наблюдается, и методической погрешности измерения влажности воздуха за счет существования вертикальных градиентов метеорологических величин не возникает.

## Выводы

1. В случае применения корреляционной обработки принятых радиосигналов в системе РАЗ атмосферы, предназначенной для измерения влажности воздуха, влияние турбулентности атмосферы на методическую погрешность оказывается более значительным, чем при доплеровской обработке.

2. При разработке двухчастотных систем РАЗ заданного метеорологического назначения необходимо обеспечивать разность частот зондирующих звуковых колебаний.

3. Для снижения значений методических погрешностей измерений влажности воздуха, возникающих за счет горизонтального ветра и рефракции звуковых волн в реальной атмосфере, необходимо применять корректные конструктивные решения при разработке антенных устройств и выбирать режимы работы систем зондирования, близкие к оптимальным.

**Список литературы.** 1. *Карташов, В.М., Бабкин, С.И., Толстых, Е.Г.* Методические погрешности измерения метеовеличин при корреляционной обработке сигналов систем радиоакустического зондирования. Сообщение 1 // Радиотехника. – 2015. – Вып.183. – С.18-23. 2. *Карташов, В.М., Бабкин, С.И., Куля, Д.Н.* К вопросу о возможности регистрации влажности воздуха при корреляционной обработке сигналов системы радиоакустического зондирования // Радиотехника. – 2013. – Вып.172. – С. 67-71. 3. *Ультразвук.* Маленькая энциклопедия; гл ред. И. П. Голямина. – М.: Сов. энциклопедия, 1979. – 400 с. 4. *Каллистратова, М.А., Кон, А.И.* Радиоакустическое зондирование атмосферы. – М.: Наука, 1985. – 195 с. 5. *Карташов, В.М., Волох, А.В., Радионова, В.В.* Тела неопределенности зондирующих сигналов систем радиоакустического зондирования атмосферы // Радиотехника. – 2007. – Вып. 150. – С. 94-99. 6. *Стратосферно-тропосферное радиоакустическое зондирование / В.А.Зиничев, В.О.Рапопорт, В.Ю.Трахтенгерц и др.* // Труды X Всесоюз. симп. по лазерн. и акустич. зондир. атмосферы. Ч.2. – Томск, 1989. – С. 74 -78. 7. *Радиоакустическое зондирование атмосферы / Прошкин Е.Г., Бабкин С.И., Г.В.Груша и др.* Разд.2 // Дистанционные методы и средства исследования процессов в атмосфере Земли; под ред. Кашеева Б.Л., Прошкина Е.Г., Лагутина М.Ф. – Харьков: Коллегиум, 2002. С.44-98. 8. *Harris, C. M.* Effect of Humidity on the Velocity of Sound // JASA, v.49, #3, 1971, pp 890-893. 9. *Физическая акустика;* под ред. У.Мезона // Свойства газов, жидкостей и растворов. Т. II, ч. А; пер. с англ. под ред. И Г Михайлова. – М.: Мир, 1968. – 487 с. 10. *Бабкин, С.И., Груша Г.В.* Влияние атмосферной турбулентности на точность определения влажности воздуха амплитудным радиоакустическим методом // Оптика атмосферы. – 1990. – Т.3, №10. – С.1064 – 1069. 11. *Бабкин, С.И.* К вопросу измерения влажности воздуха радиоакустическим зондированием // Сб. науч. трудов по материалам 4-й Междунар. конф. “Теория и техника передачи, приема и обработки информации. Новые информационные технологии”. 28-30 сентября 1998 г. Харьков-Туапсе, с. 96-97. 12. *Налбандян, О.Г.* // Известия АН СССР. Физика атмосферы и океана. – 1976. – 12, №8. – С. 877-880.

*Харьковский национальный  
университет радиоэлектроники*

*Поступила в редколлегию 28.03.2017*

## ОЦЕНКА ПАРАМЕТРОВ СПЕКТРОВ РАССЕЯННЫХ СИГНАЛОВ В РЛС ВЕРТИКАЛЬНОГО ЗОНДИРОВАНИЯ АТМОСФЕРЫ

### Введение

Радиолокационные методы исследования атмосферы позволяют в реальном времени контролировать тонкую пространственно-временную структуру метеорологических полей в атмосфере, существенно дополняя стандартные метеорологические измерения. Одним из перспективных методов дистанционного зондирования атмосферы является метод вертикального радиолокационного зондирования, который позволяет получать вертикальные профили метеорологических величин. Системы дистанционного зондирования атмосферы на основе радиолокационных станций вертикального зондирования (РЛС ВЗ) обеспечивают высокую оперативность, широкий пространственный охват и меньшую стоимость проведения измерений по сравнению с контактными системами измерения.

### Особенности спектров сигналов обрабатываемых в радиолокационных станциях вертикального зондирования

Для получения информации о динамике атмосферных движений методом вертикального зондирования используется явление отражения электромагнитных волн от турбулентных образований в ясном небе [1]. Временное положение рассеянного сигнала и сдвиг по частоте, обусловленный эффектом Доплера, позволяют получить информацию о высоте и скорости перемещения атмосферных неоднородностей. Анализ параметров рассеянных сигналов позволяет получать в реальном масштабе времени высотно-временное поле скорости ветра и интенсивности турбулентности.

Спектральная плотность мощности (СПМ) принятого сигнала в РЛС ВЗ содержит сигнальную составляющую, обусловленную рассеянием излученного зондирующего импульса от движущихся с преобладающим ветром турбулентных неоднородностей коэффициента преломления атмосферы, рис. 1 – позиция 1, а также компоненты, обусловленные земной помехой – позиция 2, и шумами приемного тракта – позиция 3.

Сигнал земной помехи (ЗП) формируется элементами земной поверхности на удалении, соответствующем высоте зондирования. Ширина спектра ЗП обычно существенно уже ширины спектра сигналов, рассеянных турбулентными неоднородностями. Уровень ЗП для малых дальностей зондирования значительно, иногда на 20 – 40 дБ, превосходит уровень полезного сигнала. При квадратурной схеме обработки сигналов ширина компонент спектра ЗП значительно меньше, чем для одноканальной схемы, вследствие устранения неоднозначности определения фазы принимаемого сигнала. Вследствие

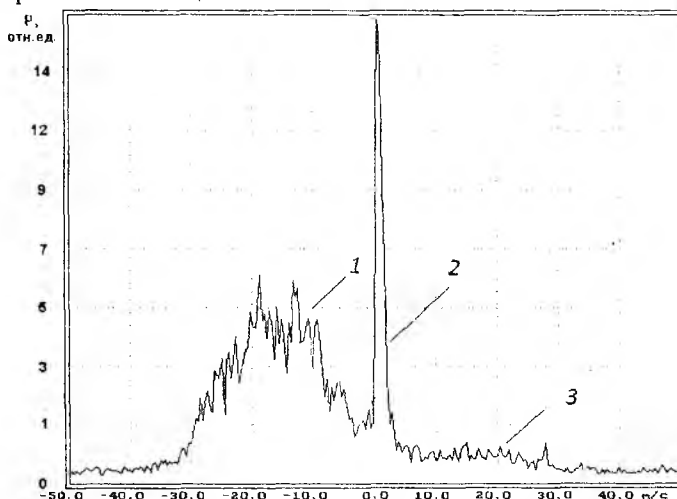


Рис. 1

ограниченной длины реализации для спектрального анализа спектр ЗП растекается на несколько частотных отсчетов. К такому же эффекту приводит и наличие медленно перемещающихся целей, отражения от которых воспринимаются по боковым лепесткам диаграммы направленности антенны. Наличие в спектральной плотности мощности рассеянного сигнала

шумов и помех усложняет определение параметров сигнальной части спектра, вызывая смещение оценок доплеровского сдвига в сторону меньших абсолютных значений. Отражение от местных предметов практически когерентно и медленно меняется во времени. Мощность, отраженная от наземных объектов, образующих земную помеху, обратно пропорциональна четвертой степени расстояния до них, в то время как мощность отраженных от атмосферных неоднородностей сигналов меняется обратно пропорционально квадрату расстояния вследствие увеличения импульсного объема с ростом дальности [1]. Поэтому на высотах, приближающихся к максимальным высотам зондирования, влияние ЗП снижается. Для нижних высотных слоев мощность ЗП значительно превышает мощность сигналов, рассеянных турбулентными неоднородностями.

### Модель сигнала на входе в радиолокационной станции вертикального зондирования

Сигнал на входе РЛС ВЗ формируется как отражение от совокупности элементарных «целей», сосредоточенных в пределах импульсного объема, ограниченного диаграммой направленности РЛС и пространственной протяженностью зондирующего импульса. Поскольку в импульсном объеме присутствует множество неоднородностей, то рассеянный сигнал представляет собой суперпозицию отдельных отражений от каждой неоднородности в отдельности. Так как случайные колебания скорости отдельных отражателей независимы, то с увеличением их числа закон распределения флуктуационной компоненты зарегистрированной РЛС ВЗ скорости ветра стремится к нормальному закону в силу центральной предельной теоремы. Утверждение о гауссовой СПМ рассеянного сигнала справедливо при времени накопления более нескольких секунд, что подтверждают экспериментальные результаты. Пример регистрации СПМ рассеянного сигнала, полученных с временем накопления сигнала 4 с, приведен на рис. 2, а, с временем накопления 200 с на рис. 2, б. Данные получены на РЛС ВЗ дециметрового диапазона ХНУРЭ [1].

Ширина спектра ЗП оценивается путем анализа характеристик выборок рассеянных сигналов с нижних высотных слоев. Проведенные исследования подтвердили соответствие гауссовой модели ЗП результатам измерений [2]. Параметры оценивались по выборкам, полученным в ходе зондирования атмосферы на РЛС ВЗ дециметрового диапазона [1]. Анализ выборок, полученных при диапазоне однозначного определения  $\pm 50$  м/с, показал, что спектр ЗП центрирован около нулевого значения скорости и имеет ширину  $\Delta\nu = 0.0158\nu_{\max}$ .

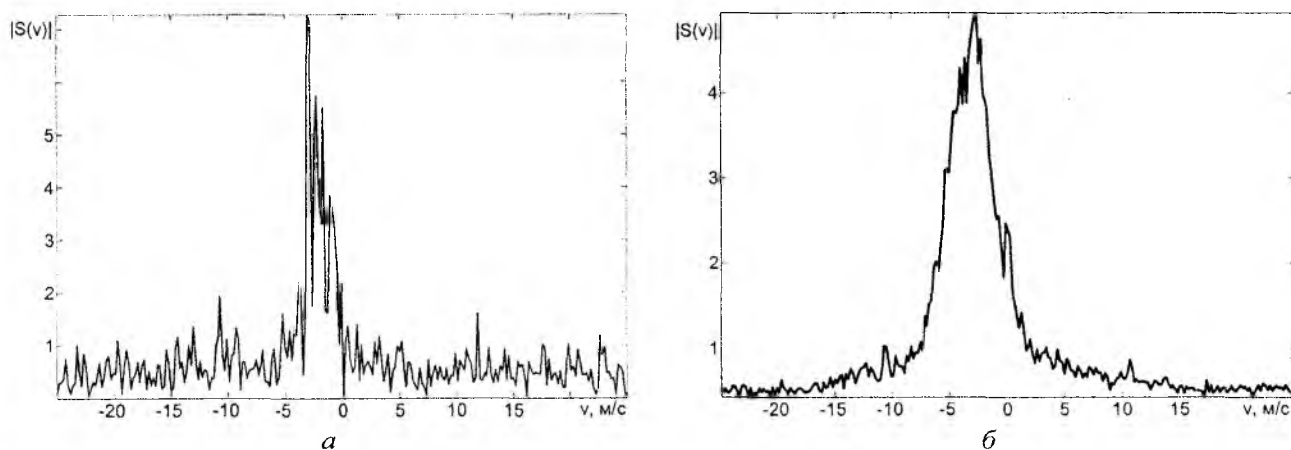


Рис. 2

При рассмотрении рассеянного сигнала на интервалах времени, превосходящих время существования неоднородностей в атмосфере, можно использовать упрощенную математическую модель рассеянного сигнала, исходя из осредненных параметров наблюдаемых выборок в натурном эксперименте. Амплитудный спектр модели сигнала рассеянного на турбулентных неоднородностях коэффициента преломления атмосферы формируется в виде функции Гаусса с заданными параметрами, а фазовый спектр представляет собой равномер-

но распределенный на интервале  $-\pi \dots \pi$  случайный процесс. СПМ ЗП задается в виде функции Гаусса с математическим ожиданием, равным нулю, и дисперсией, определенной на основе экспериментальных данных. Переход во временную область осуществляется путем обратного преобразования Фурье от комплексного спектра. Для формирования помехового компонента сигнала к реализации, полученной в результате обратного преобразования Фурье, добавляется белый гауссовый шум.

### Методы оценки параметров спектров сигналов рассеянных на атмосферных неоднородностях

Информативными параметрами сигнала в системах дистанционного зондирования атмосферы являются первые три момента спектра: мощность рассеянного сигнала, доплеровский сдвиг, спектральная ширина. Смещение оценок информативных параметров возможно вследствие воздействия ЗП, тепловых шумов, помех индустриального и естественного происхождения. В зависимости от вида функции стоимости ошибок измерения [3], параметризация может быть реализована методом максимумов, методом моментов или методом наименьших квадратов.

Наиболее простым в реализации методом параметризации спектров сигналов рассеянных на атмосферных неоднородностях является метод максимума. Он подразумевает оценку центральной частоты по положению максимального пика спектра, и оценку спектральной ширины по количеству отсчетов, превысивших порог. Этот метод имеет существенный недостаток – чувствительность к мощным узкополосным помехам, которые могут быть приняты за полезный сигнал, и привести к промахам в оценке доплеровского сдвига.

Метод моментов заключается в оценивании моментов спектра случайного процесса по выборке:

$$P' = \sum_{i=1}^N y_i, \quad f_0' = \frac{1}{P'} \sum_{i=1}^N i \cdot y_i, \quad \sigma' = \sqrt{\frac{1}{P'} \cdot \sum_{i=1}^N y_i \cdot (i - f_0')^2}.$$

Мощные узкополосные помехи, например ЗП, приводят к смещению оценок скорости ветра, однако этот эффект для метода моментов выражен значительно слабее по сравнению с методом максимума.

Параметрические методы основаны на подборе параметров модели, при котором достигается минимум меры расхождения модельных данных с реальными. Наиболее распространенным методом из этой категории является метод наименьших квадратов (МНК). В МНК осуществляется минимизация функции:

$$e(f_0, \Delta f) = \sum_{i=1}^N [y(i) - g(i, f_0, \Delta f)]^2, \quad (1)$$

где  $g$  – применяемая модель. В качестве модели для МНК применяется функция Гаусса. Функция Гаусса имеет два параметра, которые определяют положение ее центра и ширину, то есть решение оптимизационной задачи непосредственно дает искомые результаты. Целевая функция параметризации спектра рассеянного сигнала МНК (исходный спектр в виде функции Гаусса) представлена на рис. 3.

Для минимизации целевой функции могут быть использованы различные методы. Наиболее прост в реализации метод прямого перебора всех возможных значений параметров с последующим выбором тех значений, которые обеспечивают минимальную невязку модели с выборочным спектром. Более перспективными являются методы оптимизации, при этом используются прямые методы (метод Нелдера – Мида, метод покоординатного спуска) и косвенные методы (градиентные, в частности метод наискорейшего спуска и его модификации) [4].

Можно выделить разновидности мешающих факторов, приводящих к систематическим погрешностям при параметризации спектров рассеянных сигналов :

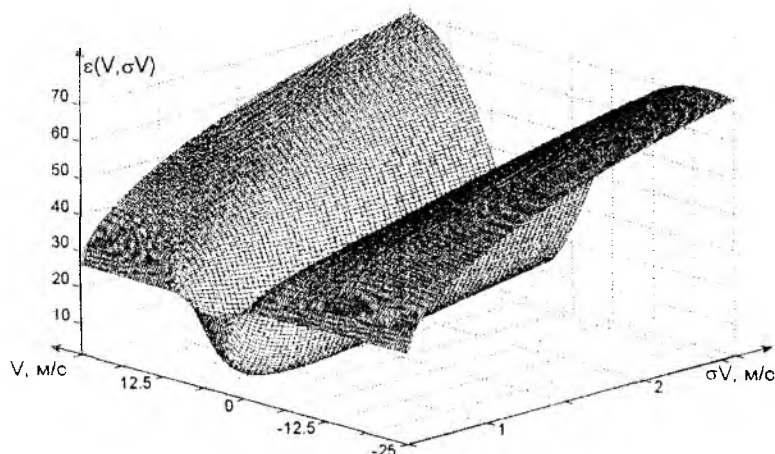


Рис. 3

- мешающие отражения от земной поверхности проявляются в виде интенсивной частотной составляющей на нулевой частоте и приводят к смещению оценки скорости ветра в сторону меньших по модулю значений;

- краевые эффекты при параметризации проявляются в виде смещения оценки скорости ветра в сторону меньших по модулю значений.

### Алгоритмические методы подавления земной помехи в спектре рассеянного сигнала

Параметризация спектра сигнала производится после удаления ЗП из спектра рассеянного сигнала. Основными алгоритмическими методами подавления ЗП являются:

- замена участка спектра, примыкающего к нулевой частоте реализацией шума;
- формирование массива шаблонов ЗП путем усреднения большого числа спектров рассеянных сигналов для разных высотных слоев и направлений зондирования;
- применение режекторных фильтров, настроенных на подавление сигналов нулевой частоты, метод эффективен в случае неперекрывающихся спектров ЗП и полезного сигнала (метод вейвлет-фильтрации, метод адаптивной режекции на основе авторегрессионной модели).

Для подавления земной помехи наиболее эффективным из рассмотренных методов оказался метод вейвлет-фильтрации [5]. Принцип действия вейвлет-фильтра основан на разложении сигнала в базисе вейвлет-функции с последующим обнулением коэффициентов разложения, соответствующих помеховым составляющим. На рис. 4 приведены: 1 – результаты вейвлет-разложения модели сигнала для случая модели сигнала без ЗП, 2 – для случая модели сигнала с ЗП. Коэффициенты разложения изображены в порядке возрастания уровня разложения. При наличии в анализируемом сигнале ЗП коэффициенты первого уровня разложения [6] имеют повышенную дисперсию. Из проведенного анализа свойств коэффициентов разложения видно, что коэффициенты разложения рассеянного сигнала уменьшаются значительно медленнее с увеличением уровня разложения. Это позволяет выработать критерий различения сигнала и ЗП по дисперсии коэффициентов разложения.

Для исследования эффективности работы алгоритмов подавления ЗП был применен метод имитационного моделирования, использовалась рассмотренная ранее модель со следующими параметрами: отношение сигнал/шум 20 дБ, спектральная ширина полезного сигнала 1,5 м/с, полный диапазон однозначного определения скорости  $\pm 25$  м/с. На рис.5 приведены результаты параметризации спектров рассеянных сигналов, соответствующих диапазону скоростей ветра  $\pm 25$  м/с, методом наименьших квадратов для случаев применения всех рассматриваемых фильтров подавления ЗП (1 – исходный профиль, 2 – без фильтрации, 3 – обнуление ЗП, 4 – адаптивный фильтр авторегрессионный фильтр, 5 – вейвлет-фильтр).

Наибольшую величину погрешностей можно наблюдать при отсутствия фильтрации ЗП, наименьшую – в случае применения вейвлет-фильтра. Анализ результатов моделирования показал преимущества применения вейвлет-фильтра для подавления земной помехи в РЛС

ВЗ, особенно в случае частотного перекрытия спектров рассеянного сигнала и земной помехи, в сравнении с методами, основанными на адаптивной фильтрации.

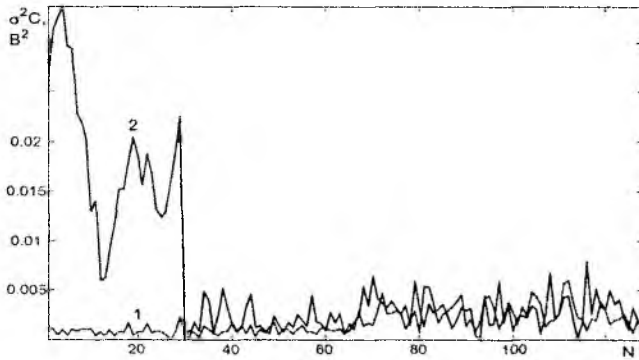


Рис. 4

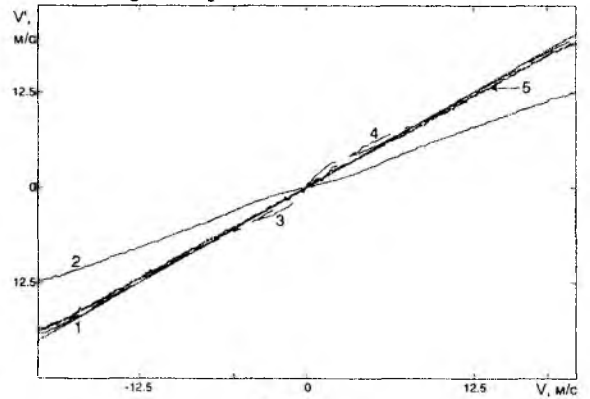


Рис. 5

### Краевые эффекты при параметризации спектров сигналов, рассеянных атмосферными неоднородностями

Параметризация спектров сигналов, рассеянных атмосферными неоднородностями, имеет особенность, заключающуюся в циклическом характере спектра сигнала, когда величина доплеровского смещения приближается к половине частоты дискретизации  $\pm f_{\text{диск}}/2$ . В этом случае спектральный максимум смещается к краю частотной оси и часть спектральных составляющих циклически переходит на частоты  $\mp f_{\text{диск}}/2$ . Диапазон однозначно определяемых скоростей РЛС определяется через диапазон однозначно определяемых доплеровских сдвигов, составляющий  $f_{\text{д}} = -1/T \dots 1/T$ , где  $T$  – период повторения зондирующих импульсов.

Повышение отношения сигнал/шум в РЛС ВЗ достигается методом когерентного накопления, при этом для уменьшения флуктуационных погрешностей применяются максимально возможная кратность накопления и наиболее узкий диапазон измеряемых скоростей ветра, что приводит к возрастанию систематических погрешностей, вызванных краевыми эффектами. Снижение погрешностей параметризации спектров возможно следующими путями:

- применением методов параметризации, нечувствительных к краевым эффектам;
- выбором кратности накопления, при которой краевые эффекты для максимальных значений измеряемых скоростей ветра проявляются несущественно.

В случае использования циклического спектра, метод моментов обеспечивает смещенные оценки центральной частоты.

Представим спектр в полярной системе координат, тогда координаты центра масс спектра записываются как [7]:

$$\bar{c} = E(\rho \cdot \cos \theta), \quad \bar{s} = E(\rho \cdot \sin \theta)$$

(здесь и далее  $E$  – оператор среднего значения). Полярные координаты центра масс определяются выражением

$$\bar{\theta} = \arctg(\bar{s}/\bar{c}), \quad \bar{\rho} = \sqrt{\bar{s}^2 + \bar{c}^2}$$

Математическое ожидание угловой координаты центра масс

$$\bar{\theta} = \arctg\left(\frac{E(\rho \cdot \sin \theta)}{E(\rho \cdot \cos \theta)}\right)$$

Метод наименьших квадратов подвержен краевым эффектам, поскольку в целевой функции (1) не учитывается явление подмены частот, вызванное прореживанием реализаций

во время когерентного накопления. Вследствие этого явления ось частот «защипывается» и возникает неоднозначность определения доплеровских сдвигов и, соответственно, скоростей ветра.

В связи с этим, модель спектра для параметризации удобно формировать в полярных координатах, в «намотанном» виде [7, 8]. Намотанное нормальное распределение определяется выражением

$$f(\theta, \sigma) = \frac{1}{\sqrt{2\pi}\sigma} \cdot \sum_{k=-\infty}^{\infty} \exp\left(-\frac{1}{2} \cdot \frac{(\theta + 2\pi k)^2}{\sigma^2}\right)$$

или в виде ряда Фурье:

$$f(\theta, \sigma) = \frac{1}{2\pi} \cdot \left(1 + 2 \sum_{p=1}^{\infty} (\exp(-\sigma^2 / 2))^{p^2} \cdot \cos(p\theta)\right).$$

Влияние краевых эффектов при параметризации спектров рассеянных сигналов исследовалось путем имитационного моделирования с использованием рассмотренной ранее модели. При моделировании рассеянный сигнал формировался в диапазоне скоростей  $\pm 25$  м/с. Среднеквадратичное отклонение (СКО) оценок вычислялось по формуле

$$\sigma_X = \sqrt{\frac{\sum_{i=1}^N (x_i' - x_i)^2}{N-1}}$$

где  $x_i'$  – оценка параметра  $X$ ;  $x_i$  – истинное значение параметра  $X$ ;  $N$  – объем выборки моделирования.

Исследовалась зависимость среднего смещения оценки скорости ветра от истинного значения скорости ветра для рассмотренных методов параметризации. Результаты моделирования представлены на рис. 6 для следующих параметров рассеянного сигнала: отношение сигнал/шум 10 дБ, спектральная ширина рассеянного сигнала 2.5 м/с.

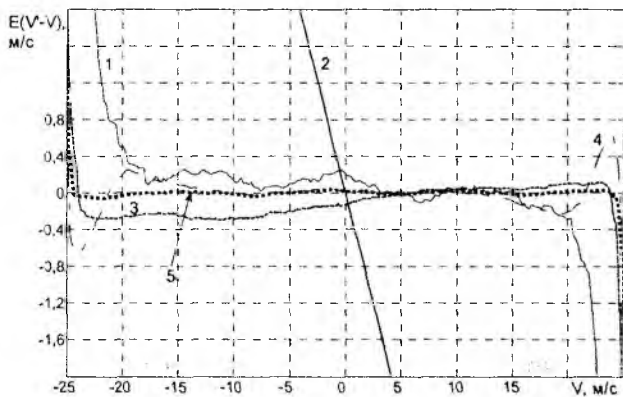


Рис. 6

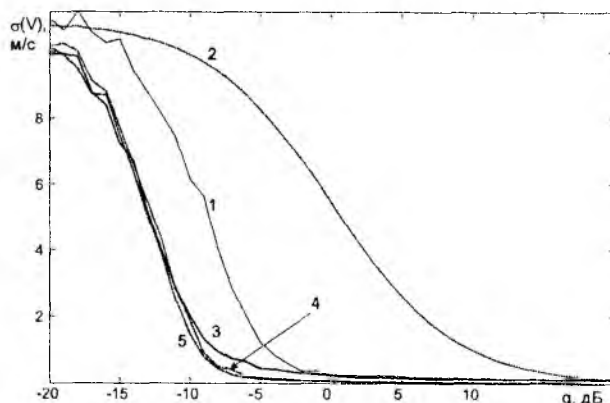


Рис. 7

Здесь приняты следующие обозначения: 1 – метод максимума, 2 – метод моментов, 3 – циклический метод моментов, 4 – МНК, 5 – циклический МНК. Также исследованы зависимости СКО оценки скорости от отношения с/ш при фиксированной спектральной ширине рассеянного сигнала, равной 2,5 м/с, результаты которого представлены на рис. 7, обозначения методов параметризации аналогичны обозначениям для рис. 6.

Результаты исследования зависимости скорости выполнения параметризации спектра от размера выборки представлены на рис. 8.

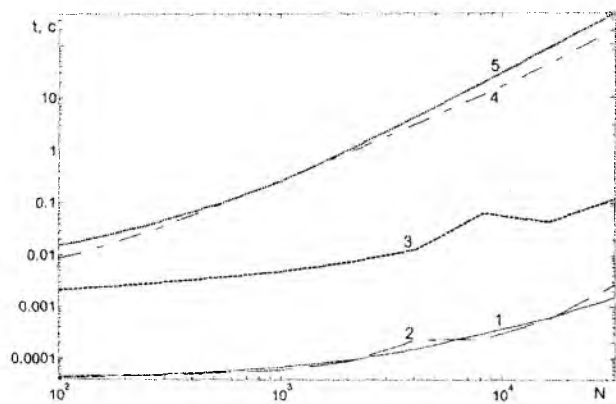


Рис. 8

точную ошибку параметризации.

Из рассмотренных методов параметризации наилучшие метрологические характеристики обеспечивает циклический метод наименьших квадратов. Циклический метод моментов уступает ему, однако имеет значительно более низкую вычислительную сложность, что позволяет применять его для предварительной оценки метеопараметров.

### Заключение

Рассмотрены методы оценки параметров спектра сигнала, рассеянного от турбулентных неоднородностей, получаемых с помощью РЛС ВЗ. На основе разработанной модели сигнала методом имитационного моделирования исследованы характеристики точности результатов оценки скорости ветра. В результате анализа определены доминирующие причины искажения оценок скорости ветра и промахов измерений. Применение методов параметризации, использующих представление спектров в полярных координатах, позволяет устранить краевые эффекты.

Предложены мероприятия по снижению влияния краевых эффектов при параметризации спектров и мешающих отражений от земной поверхности.

**Список литературы.** 1. *Дистанционные методы и средства исследования процессов в атмосфере Земли*; под ред. Б. Л. Кашеева, Е. Г. Прошкина, М. Ф. Лагутина. – Харьков: ХНУРЭ, 2002. – 425 с. 2. *Barrie Billingslay, J. Low-angle radar land clutter. Measurements and empirical models* / NY: William Andrew Publishing, 2002. – 719p. 3. *Тихонов, В.И., Харисов, В.Н.* Статистический анализ и синтез радиотехнических устройств и систем: учеб. пособие для вузов. – М.: Радио и связь, 2004. – 608 с. 4. *Бахвалов, Н.С.* Численные методы. – М.: Наука, 1975. – 630 с. 5. *Теория и практика вейвлет-преобразования* / В.И. Воробьев, В.Г. Грибунин. – СПб: ВУС, 1999. – 204с. 6. *Литвин-Попович, А.И.* Применение вейвлет-фильтрации для подавления земной помехи в РЛС вертикального зондирования атмосферы / А.И. Литвин-Попович, В.Н. Олейников // Прикладная радиоэлектроника. – 2008. – Т. 7, №1. – С.30-36. 7. *Мардиа, К.* Статистический анализ круговых наблюдений; пер. с англ. – М.: Наука, 1978. – 239 с. 8. *Литвин-Попович, А.И.* Параметризация спектров рассеянных сигналов в РЛС вертикального зондирования атмосферы / А.И. Литвин-Попович, В.Н. Олейников // Радиотехника. – 2008. – Вып. 152. – С. 49-52.

Харьковский национальный  
университет радиоэлектроники

Поступила в редакцию 18.04.2017

## **МОДЕЛЬ ВЫЯВЛЕНИЯ И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ СВЯЗИ НА ОСНОВЕ АППАРАТА МАРКОВСКИХ ПРОЦЕССОВ**

### **Постановка задачи**

В настоящее время значительный интерес представляют исследования беспроводных городских телекоммуникационных сетей, в которых имеется центральная станция, координирующая работу абонентских станций. Именно такая сетевая архитектура является основой технологии программных конфигурируемых сетей (SDN). Отличительными особенностями построения беспроводных городских телекоммуникационных сетей являются высокая сложность протокола подуровня управления доступом к среде, отвечающего, в частности, за организацию доступа абонентов к общему каналу связи, а также наличие большого числа неопределенных частей, в которых стандартизированы лишь некоторые механизмы сетевого взаимодействия. Эти особенности технологии SDN, а также ее новизна приводят к необходимости разработки методов повышения защиты информации при множественном радиодоступе абонентов.

Задача обеспечения безопасности становится особенно актуальной для телекоммуникационных сетей, где канал передачи данных часто разделяется между большим количеством пользователей. В беспроводных городских сетях появляется еще одна проблема – общедоступность канала связи.

Информационная безопасность является одной из составляющих гарантоспособности SDN [1 – 5]. Основную угрозу безопасности таких систем представляют уязвимости, прежде всего, программных компонентов. Поиск уязвимостей в программных компонентах является актуальной и ресурсоемкой задачей, которой занимаются крупные компании и исследовательские центры. Информацию об уязвимостях можно получить из общедоступных информационных источников, например Open Source Vulnerability Database ([www.osvdb.org](http://www.osvdb.org)), Common Vulnerabilities and Exposures ([www.cve.mitre.org](http://www.cve.mitre.org)), National Vulnerability Database ([www.nvd.nist.gov](http://www.nvd.nist.gov)) и других баз данных уязвимостей.

Однако, несмотря на общедоступность информации об уязвимостях программных продуктов, имеющихся данных недостаточно, чтобы количественно оценивать и сравнивать безопасность программных продуктов по одному обобщенному критерию, а также прогнозировать их защищенность от информационных вторжений в будущем. Одна из основных проблем выбора наиболее защищенной конфигурации SDN заключается в сложности количественной оценки уровня информационной безопасности, а также выбора адекватных показателей для оценки, позволяющих в комплексе учесть все факторы, влияющие на успешное проникновение в сеть и размер потенциального ущерба, который может быть нанесен при эксплуатации имеющихся угроз безопасности.

Цель статьи – исследование подходов к оценке и прогнозированию уровня информационной безопасности программных средств SDN на основе моделирования процессов выявления и устранения уязвимостей с использованием аппарата марковских процессов.

### **Основная часть**

Угрозами информационной безопасности являются отказы, нарушающие готовность сети, целостность или конфиденциальность информации. Причинами этих отказов являются уязвимости – специальный вид дефектов, которые активизируются вследствие

злонамеренных действий (хакерских атак, воздействия вирусов, вредоносных программ и др.).

Предварительный анализ процессов обнаружения и устранения уязвимостей показывает, что они могут быть описаны системой массового обслуживания с неограниченной длиной очереди. Параметры системы массового обслуживания могут быть получены и соотнесены с процессами и статистическими данными об обнаружении и устранении уязвимостей следующим образом [5]:

- число обслуживающих каналов  $n$  соответствует количеству организаций или групп разработчиков, которые занимаются устранением уязвимости конкретного программного продукта SDN. В простейшем варианте может быть рассмотрен только один обслуживающий орган;

- интенсивность поступления заявок  $\lambda$ , которая соответствует интенсивности обнаружения уязвимостей в рассматриваемом программном продукте SDN может быть получена на основе анализа базы данных уязвимостей CVE (первичной базы) как количество уязвимостей, опубликованных за рассматриваемый промежуток времени (неделя, месяц, год);

- интенсивность обслуживания заявок  $\mu$ , которая соответствует интенсивности устранения уязвимостей (выпуска обновлений, исправляющих уязвимости), может быть оценена с использованием информации из бюллетеней безопасности, публикуемых компаниями-производителями программного продукта SDN, а также баз уязвимостей NVD и OSVDB (вторичные базы);

- время обслуживания  $T_{обсл}$ , соответствующее параметру «количество дней риска» [2, 5], который используется при оценке информационной безопасности программного продукта SDN, определяется как усредненный период времени между появлением и устранением отдельных уязвимостей;

- вероятностью обслуживания поступившей заявки  $Q$  является вероятность устранения уязвимости, которая теоретически равна единице; на практике же встречаются ситуации, когда отдельные уязвимости отдельных программных компонентов так и не устраняются;

- вероятность отказа  $P_{отк}$  показывает вероятность того, что уязвимость не будет устранена;

- среднее число заявок в СМО  $z_{cp}$  показывает среднее количество уязвимостей, которые присутствуют в сети в данный момент времени, и для которых еще не выпущено программное обновление. Данный показатель является одним из наиболее важных, поскольку определяет количество потенциальных возможностей для атаки инфокоммуникационной сети:

- среднее число заявок в очереди  $r_{cp}$  определяет, сколько в среднем уязвимостей опубликовано и ожидает выпуска обновления для их устранения;

- среднее время пребывания заявки в очереди  $t_{оч, cp}$  показывает, сколько в среднем требуется времени для устранения уязвимости с момента ее обнаружения;

- среднее число занятых каналов  $k_{cp}$  говорит о том, сколько рабочих групп в среднем заняты устранением уязвимости.

Рассмотренную выше систему массового обслуживания можно представить в виде системы состояний, в которой каждому состоянию будет соответствовать определенное количество обнаруженных уязвимостей, присутствующих в системе, для которых еще отсутствует рекомендация или программное обновление для устранения. Такие уязвимости будем называть активными. Подобные процессы эффективно описываются марковскими цепями. Марковские цепи имеют сравнительно мало инженерных приложений, так как довольно редко на практике моменты возможных переходов системы из состояния в

состояние заранее известны и фиксированы. Гораздо чаще переходы из состояния в состояние могут происходить не в фиксированные моменты времени, а в случайные.

Будем считать, что переходы системы из состояния в состояние осуществляются под воздействием пуассоновских потоков событий (не обязательно стационарных).

Отсутствие последствия в пуассоновском потоке позволяет при фиксированном настоящем (состояние  $s_i$  системы в момент  $t$ ) не учитывать то, когда и как система оказалась в этом состоянии.

Пусть на графе состояний системы  $S$  существует стрелка, ведущая из состояния  $s_i$  в одно из соседних состояний  $s_j$  (рис.1).

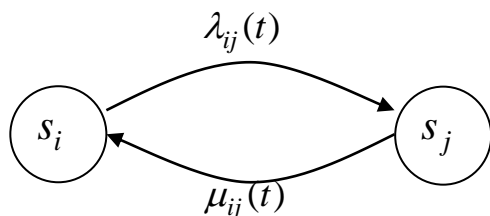


Рис.1. Переход из состояния  $s_i$  в одно из соседних состояний  $s_j$  под воздействием  $\lambda_{ij}(t)$  и  $\mu_{ij}(t)$

Будем считать, что переход системы из состояния  $s_i$  в состояние  $s_j$  осуществляется под воздействием пуассоновского потока событий с интенсивностью  $\lambda_{ij}(t)$ . Переход из  $s_i$  в  $s_j$  происходит в момент, когда наступает первое событие потока.

Рассмотрим на оси  $0t$  элементарный участок времени  $\Delta t$ , примыкающий к  $t$  (рис. 2) и найдем вероятность того, что за время  $\Delta t$  система перейдет из состояния  $s_i$  в состояние  $s_j$  в предположении, что система находилась в состоянии  $s_i$  в момент времени  $t$ .

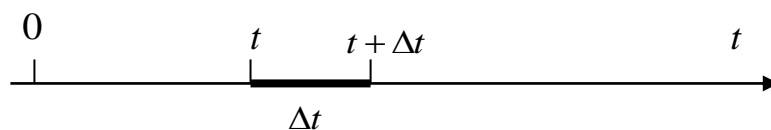


Рис. 2. Элементарный участок времени  $\Delta t$  на оси  $0t$

Эта вероятность  $p_i(t) = \lambda_{ij}(t)\Delta t$ , так как случайная величина равна числу событий потока, попадающих на элементарный участок  $\Delta t$ , имеет математическое ожидание  $m = \lambda_{ij}(t)\Delta t$  и с точностью до бесконечно малых высших порядков равна вероятности  $p_i$  попадания на элементарный участок одного события.

Если известны, все интенсивности пуассоновских потоков событий, переводящих систему из состояния в состояние, то можно составить систему дифференциальные уравнения для вероятностей состояния.

Пусть для любой пары состояний  $s_i, s_j$  известна интенсивность  $\lambda_{ij}(t)$  пуассоновского потока событий, переводящая систему из состояния  $s_i$  в любое другое состояние  $s_j (i \neq j)$ , будем полагать эту интенсивность равную нулю, если непосредственный переход из состояния  $s_i$  в состояние  $s_j$  невозможен.

Обозначим  $p_i(t)$  – вероятность того, что в момент времени  $t$  система находится в состоянии  $s_i (i = 1, 2, \dots, n)$ . Теперь придадим  $t$  приращение  $\Delta t$  и найдем вероятность  $p_i(t + \Delta t)$  того, что в момент  $t + \Delta t$  система будет находиться в состоянии  $s_i$ . Обозначим это событие  $A: A = \{S(t + \Delta t) = s_i\}$ .

Как это событие может произойти? Двумя способами: либо произойдет событие  $B$ , состоящее в том, что в момент  $t$  система уже была в состоянии  $s_i$ , и за время  $\Delta t$  не вышла из этого состояния; либо произойдет событие  $C$ , состоящее в том, что в момент  $t$  система была в одном из соседних  $s_j$ , из которых возможен переход в  $s_i$ , и за время  $\Delta t$  перешла из состояния  $s_j$  в  $s_i$ .

Очевидно,  $A = B + C$ . Найдем вероятности событий  $B$  и  $C$ . Согласно правилу умножения вероятностей вероятность события  $B$  равна вероятности  $p_i(t)$  того, что система в момент  $t$  была в состоянии  $s_i$ , умноженной на условную вероятность того, что за время  $\Delta t$  она не выйдет из этого состояния, т.е. в суммарном потоке событий, выводящих систему из состояния  $s_i$ , не появится ни одного события.

Так как суммарный поток событий, выводящий систему из состояния  $s_i$ , как и все его слагаемые, – пуассоновский с интенсивностью, равной сумме интенсивностей слагаемых потоков:  $\sum_{j=1}^n \lambda_{ij}(t), i \neq j$ , то условная вероятность того, что на участке  $\Delta t$  появится хотя бы

одно событие (приближенно)  $p_i(t) = \sum_{j=1}^n \lambda_{ij}(t)\Delta t, i \neq j$ , а условная вероятность противоположного события  $1 - \sum_{j=1}^n \lambda_{ij}(t)\Delta t$ .

Таким образом,

$$P(B) = p_i(t) \left[ 1 - \sum_{j=1}^n \lambda_{ij}(t)\Delta t \right]. \quad (1)$$

Найдем теперь вероятность события  $C$ . Представим его в виде суммы несовместных вариантов:

$$C = \sum_j C_j, \quad (2)$$

где суммирование распространяется на все состояния  $s_j$ , из которых возможен непосредственный переход в  $s_i$ . События  $C$ , в силу ординарности потоков, можно считать несовместными. По правилу сложения вероятностей

$$P(C) = \sum_j P(C_j). \quad (3)$$

По правилу умножения вероятностей  $P(C_j) = p_j(t)\mu_{ji}(t)\Delta t$ , откуда

$$P(C) = \sum_{j=1}^n p_j(t)\mu_{ji}(t)\Delta t \quad (i \neq j). \quad (4)$$

Следовательно,

$$P(A) = P(B) + P(C) = p_i(t) \left[ 1 - \sum_{j=1}^n \lambda_{ij}(t)\Delta t \right] + \sum_{j=1}^n p_j(t)\mu_{ji}(t)\Delta t$$

Таким образом,

$$p_i(t + \Delta t) = p_i(t) \left[ 1 - \sum_{j=1}^n \lambda_{ij}(t)\Delta t \right] + \sum_{j=1}^n p_j(t)\mu_{ji}(t)\Delta t. \quad (5)$$

Вычитая из (5)  $p_i(t)$ , получим приращение функции на участке  $t, t + \Delta t$ :

$$p_i(t + \Delta t) - p_i(t) = \sum_{j=1}^n p_j(t) \mu_{ji}(t) \Delta t - p_i(t) \sum_{j=1}^n \lambda_{ij}(t) \Delta t.$$

Деля приращение функции на приращение аргумента  $\Delta t$  и устремляя  $\Delta t \rightarrow 0$ , получим для вероятностей  $p_i(t)$  систему обыкновенных дифференциальных уравнений с переменными коэффициентами

$$\frac{dp_i(t)}{dt} = \sum_{j=1}^n p_j(t) \mu_{ji}(t) - p_i(t) \sum_{j=1}^n \lambda_{ij}(t). \quad (6)$$

Эти уравнения называются уравнениями Колмогорова. Первая сумма в правой части формулы (6) распространяется на те значения  $j$ , для которых возможен непосредственный переход из состояния  $s_j$  в  $s_i$ , а вторая – на те значения, для которых возможен непосредственный переход из состояния  $s_i$  в  $s_j$ .

Все потоки, переводящие систему  $S$  из одного состояния в другое, являются простейшими (стационарными пуассоновскими). Системы, в которых происходит такой процесс, называют простейшими системами. Для простейшей системы вероятности состояний определяются уравнениями Колмогорова с постоянными коэффициентами. Применим преобразование Лапласа к решению системы уравнений Колмогорова. Обозначим изображение вероятности состояния  $p_i(t)$  функцией  $\pi_i(x)$

$$p_i(t) \rightarrow \pi_i(x). \quad (7)$$

Тогда системе уравнений Колмогорова для вероятностей состояний будет соответствовать система уравнений для их изображений:

$$x\pi_i(x) = \sum_{j=1}^n \pi_j(x) \mu_{ji} - \pi_i(x) \sum_{j=1}^n \lambda_{ij} + p_i(0), i = 1, 2, \dots, n. \quad (8)$$

Откуда

$$\pi_i(x) = \frac{\sum_{j=1}^n \pi_j(x) \mu_{ji} + p_i(0)}{x + \lambda_i}, \quad (9)$$

где  $\lambda_i = \sum_{j=1}^n \lambda_{ij}$ .

Таким образом, вместо системы однородных дифференциальных уравнений с постоянными коэффициентами для вероятностей состояний получена система однородных алгебраических уравнений с постоянными коэффициентами для изображений вероятностей состояний.

Эту систему нужно решать с учетом нормировочного условия:

$$\sum_{i=1}^n p_i(t) = 1. \quad (10)$$

Следовательно, одно из уравнений можно заменить на

$$\sum_{i=1}^n \pi_i(x) = \frac{1}{x}, \quad (11)$$

которое является изображением нормировочного условия.

Зная интенсивности  $\lambda_{ij}$  и  $\mu_{ij}$  появления событий, порождаемых потоком, можно симитировать случайный интервал между двумя событиями в этом потоке:

$$\tau_{ij} = -\frac{1}{\lambda_{ij}} \ln(r), \quad \tau_{ji} = -\frac{1}{\mu_{ij}} \ln(r).$$

где  $\tau_{ij}$  – интервал времени между нахождением системы в  $i$ -м и  $j$ -м состоянии;  $r$  – равномерно распределенное от 0 до 1 случайное число, которое берется из генератора случайных чисел (ГСЧ).

Далее, очевидно, система из любого  $i$ -го состояния может перейти в одно из нескольких состояний  $j, j + 1, j + 2, \dots$ , связанных с ним переходами.

В  $j$ -е состояние она перейдет через  $\tau_{ij}$ ; в  $(j + 1)$ -е состояние она перейдет через  $\tau_{ij+1}$ ; в  $(j + 2)$ -е состояние она перейдет через  $\tau_{ij+2}$  и т. д.

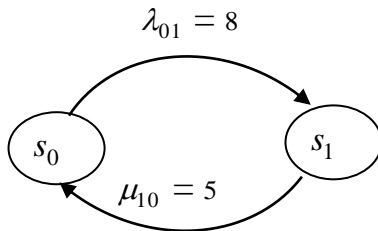


Рис. 3. Граф состояний

Ясно, что система может перейти из  $i$ -го состояния только в одно из этих состояний, причем в то, переход в которое наступит раньше.

Поэтому из последовательности времен:  $\tau_{ij}, \tau_{ij+1}, \tau_{ij+2}$  и т.д. надо выбрать минимальное и определить индекс  $j$ , указывающий, в какое именно состояние произойдет переход.

Рассмотрим пример. Пусть поступают заявки на обнаружения уязвимостей.

Обозначим состояния (рис.3):  $s_0$  – нет

заявки,  $s_1$  – поступила заявка. Зададим интенсивности потоков:

$\lambda_{01} = 8$  заявок в минуту;  $\mu_{10} = 5$  обработанных заявок в минуту.

Будем считать, что система в начальный момент находилась в состоянии  $s_0$ .

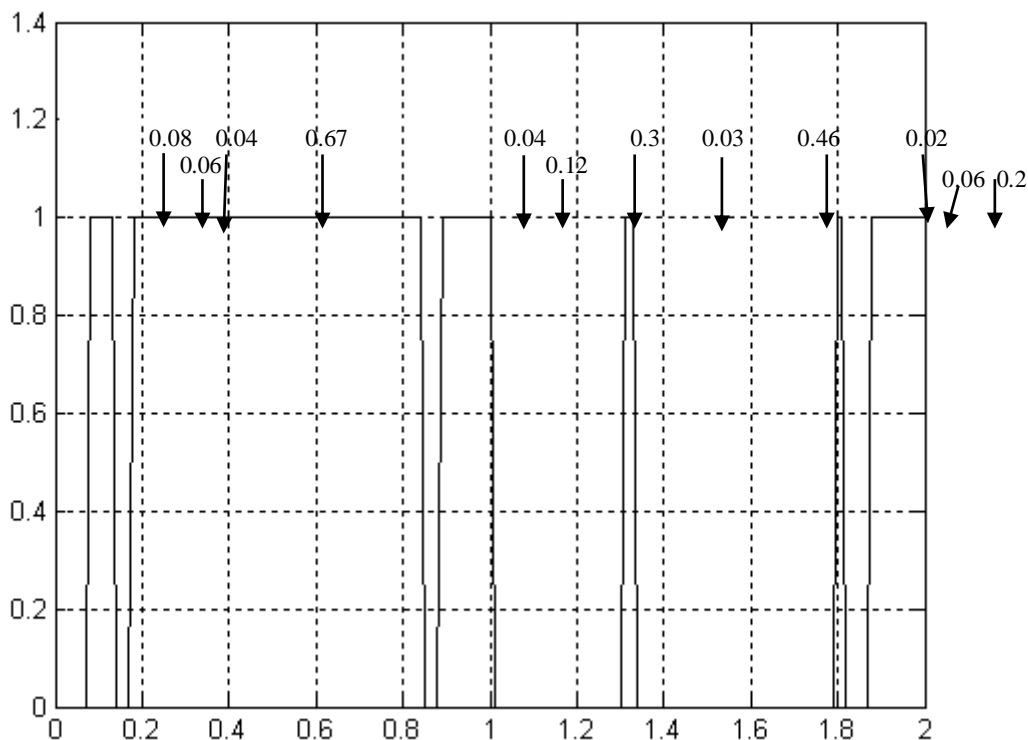


Рис. 4. Временная диаграмма поступления заявок на обнаружение уязвимостей

С помощью имитационного моделирования получена временная диаграмма поступления заявок на обнаружение уязвимостей (рис. 4). Таким образом, зная интенсивности потоков,

можно в реальном масштабе времени моделировать процессы поступления заявок на обнаружение уязвимостей.

### **Заключение**

Информационная безопасность является одной из составляющих гарантоспособности SDN. Основную угрозу безопасности таких систем представляют уязвимости, прежде всего, программных компонентов. Поиск уязвимостей в программных компонентах является актуальной и ресурсоемкой задачей, которой в последнее время занимаются крупные компании и исследовательские центры.

Анализ процессов обнаружения и устранения уязвимостей показывает, что они могут быть описаны системой массового обслуживания с неограниченной длиной очереди. Разработана модель выявления и устранения уязвимостей в программно-конфигурируемых сетях связи на основе аппарата марковских процессов. С помощью данной модели, зная интенсивности потоков, можно в реальном масштабе времени моделировать процессы поступления заявок на обнаружение уязвимостей.

**Список литературы:** 1. *Avizienis, A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J. C. Lapri, B. Randel // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11–33.* 2. *Щеглов, А. Ю. Безопасность современных ОС «в цифрах» [Электронный ресурс] / А. Ю. Щеглов. – Режим доступа: [http://blogs.csoonline.com/days\\_of\\_risk\\_in\\_2006](http://blogs.csoonline.com/days_of_risk_in_2006) (2006).* 3. *15th Annual CSI/FBI Computer Crime and Security Survey. Executive Summary. – CSI, FBI, 2010. – 17 p.* 4. *Vulnerability Disclosure Framework: Final Report and Recommendations by the Council. – Washington : NIAC, 2004. – 52 p.* 5. *Белобородов, А. Ю. Применение аппарата теории массового обслуживания для исследования процессов выявления и устранения уязвимостей программных средств / А. Ю. Белобородов, А. В. Горбенко, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – ISSN 1814-4225. – Харків.- 2014. – С.65-69*

*Харьковский национальный  
университет радиоэлектроники*

*Поступила в редколлегию 11.03.2017*

## О ПРОБЛЕМЕ АСТЕРОИДНО-КОМЕТНОЙ ОПАСНОСТИ

## Введение

Связующим звеном между зарегистрированными метеорными телами и их родительскими телами являются метеорные потоки. Еще 10 лет тому назад подавляющее число исследователей малых тел Солнечной системы исходили из того, что родительскими телами метеороидов и, следовательно, метеорных явлений в атмосфере Земли являются исключительно кометы. Своего рода прорыв произошел, когда с высокой вероятностью было установлено, что родительским телом самого известного ежегодного метеорного потока Геминиды является потенциально опасный астероид из группы Аполлона 3200 Phaethon.

К настоящему времени известны тысячи метеорных потоков и ассоциаций (МПА) и лишь для небольшой части из них найдены родительские тела. Например, на рис. 1 приведены результаты идентификации 5160 МПА каталога ХНУРЭ [1] согласно критерию Саутуорта - Хокинса [2] по базе NASA ([https://ssd.jpl.nasa.gov/sbdb\\_query.cgi](https://ssd.jpl.nasa.gov/sbdb_query.cgi)) из 16205 (на апрель 2017 г.) потенциально опасных для Земли астероидов и комет (объектов NEOs). Идентифицировано 835 МПА или 16 % каталога. Причем, как видно из графиков, для наклонения менее 30 градусов идентифицировано 56 % МПА. В то же время для наклонений более 70 градусов не идентифицировано ни одного МПА, что можно объяснить практическим отсутствием объектов NEOs с подобными орбитами в каталоге NASA.

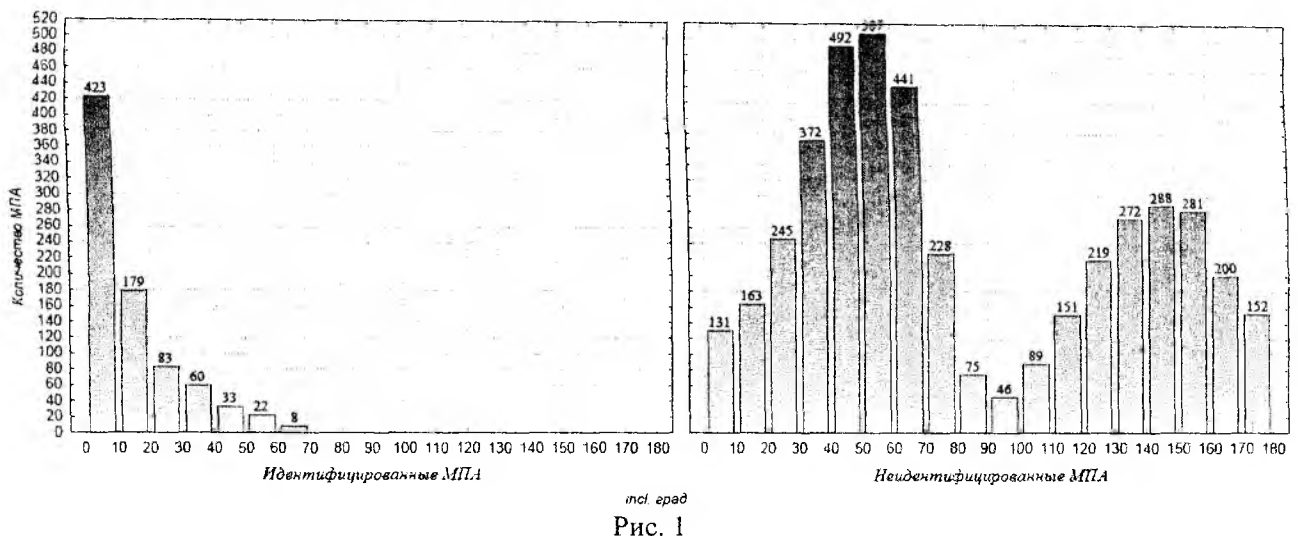


Рис. 1

Таким образом, если предположить, что у большинства метеорных потоков существуют источники, поддерживающие популяцию метеороидов на уровне, позволяющем выявить их на фоне спорадических метеороидов, то, следовательно, в каталогах орбит метеорных потоков содержится ценная информация о потенциально опасных для Земли астероидах и кометах, которые пока не обнаружены другими средствами наблюдений.

### 1. Анализ условий пересечения орбит объектов NEOs с орбитой Земли

Априорная вероятность сближения орбит космического тела (КТ) и Земли может быть рассчитана по выражению [3]

$$v_1 = 5.4189 \cdot 10^{-5} \sqrt{\frac{3.14 + 1 - a^{-2} - 2\sqrt{a(1 - e \cos^2)} \cos(i \text{incl})}{3 - a^{-2} - 2\sqrt{a(1 - e \cos^2)} \cos(i \text{incl})}} \times \left( \frac{a^2(1 - e \cos^2)}{2a - 1 - a^2(1 - e \cos^2)} - \frac{1}{\sin^2(i \text{incl})} \right), \quad (1)$$

где  $i \text{incl}$ ,  $a$  и  $e \cos$  – наклонение, большая полуось и эксцентриситет орбиты КТ соответственно.

На рис. 2 приведены категоризированные диаграммы вероятности  $v_1$  (чем больше размер символа «о», тем больше вероятность  $v_1$ ) в функции элементов орбит метеорных потоков каталога ХНУРЭ – наклонения, эксцентриситета и перигелийного расстояния (в анализе участвовало 4682 потока, для которых выражение под квадратным корнем в (1) больше нуля). Аналогичные зависимости для объектов NEOs приведены на рис. 3.

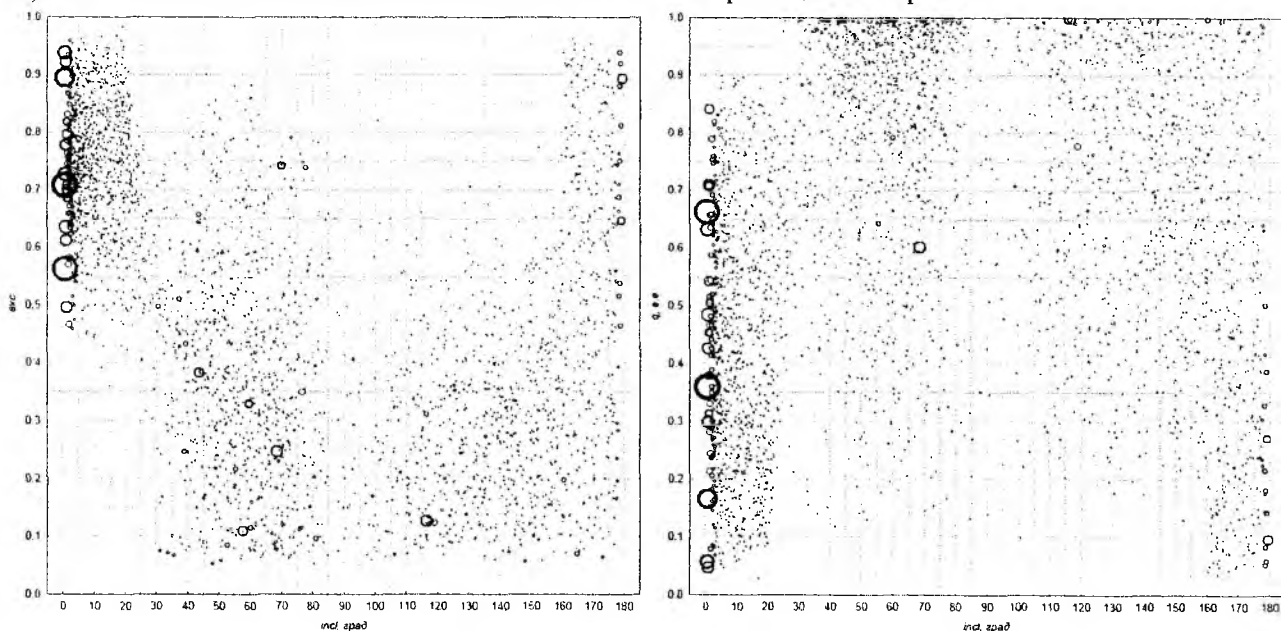


Рис. 2

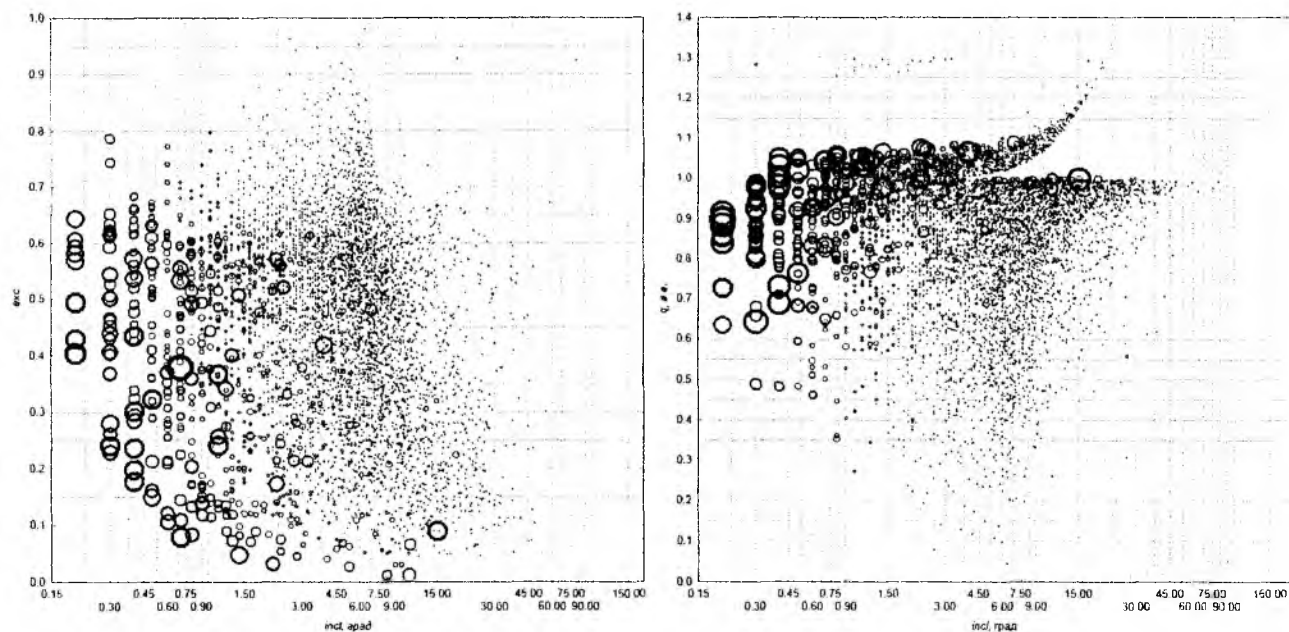


Рис. 3

Наибольшую априорную вероятность сближения орбит имеют потоки (и их потенциальные родительские тела NEOs), орбиты которых расположены в четырех кластерах: 1) наклонения в диапазоне  $incl < 10^\circ$ , эксцентриситеты  $exc > 0.5$  и перигелийные расстояния  $q < 0.7$  а.е.; 2) наклонения в диапазоне  $40^\circ < incl < 70^\circ$ , эксцентриситеты  $exc < 0.4$  и перигелийные расстояния  $q \approx 1$  а.е.; 3) наклонения в диапазоне  $110^\circ < incl < 140^\circ$ , эксцентриситеты  $exc < 0.4$  и перигелийные расстояния  $q \approx 1$  а.е.; 4) наклонения в диапазоне  $incl > 170^\circ$ , эксцентриситеты  $exc > 0.5$  и перигелийные расстояния  $q < 0.5$  а.е.

Как видно из графиков на рис. 3, наибольшую априорную вероятность сближения орбит имеют объекты NEOs с наклонениями орбит  $incl < 10^\circ$ , эксцентриситетами в интервале  $0.1 < exc < 0.7$  и перигелийными расстояниями  $q > 0.6$  а.е. Ретроградные орбиты ( $incl > 90^\circ$ ) практически отсутствуют.

Для выявления природы гипотетических тел метеорных потоков был использован критерий Кресака  $Pe$  [4] разделения на орбиты кометные и астероидного типа:

$$Pe = a^{1.5} exc = \begin{cases} > 2.5 & \text{для орбит кометного типа,} \\ < 2.5 & \text{для орбит астероидного типа.} \end{cases} \quad (2)$$

На рис. 4 приведена диаграмма вероятность  $v_1$  – критерий Кресака  $Pe$  орбит МПА каталога ХНУРЭ. Как видно из рис. 4, большинство (4682, или 89.85 %) метеорных потоков имеет астероидное происхождение.

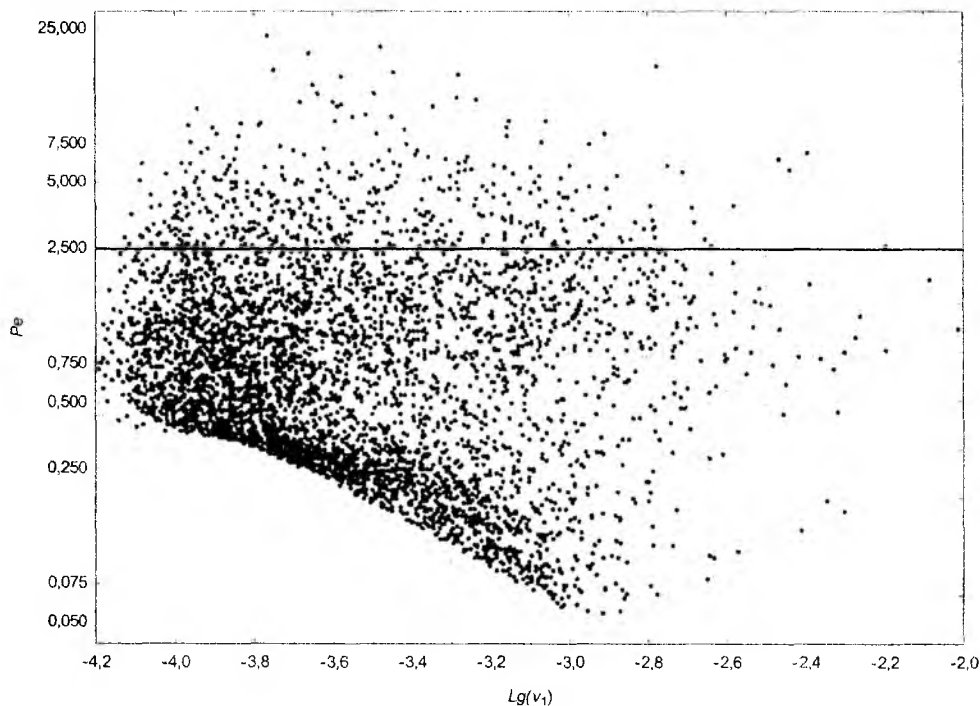


Рис. 4

Таким образом, для большинства опасных потоков родительскими телами можно считать астероиды групп Apollos, Amors и Atens.

## 2. Анализ условий столкновения объектов NEOs с орбитой Земли

Вероятность прохождения орбиты КТ через область захвата Земли можно рассчитать по формуле [3]:

$$v_2 = \frac{1064 \cdot 10^{-2}}{4a^{3/2}} \sqrt{\frac{3a - 1 - 2a\sqrt{a(1 - exc^2)} \cos(incl)}{q + Q - 1 - q \cdot Q}} \quad (3)$$

Функция (3) при перигелийном расстоянии орбиты КТ [ $q = a(1 - exc)$ ]  $\rightarrow 1$  и афелийном расстоянии орбиты КТ [ $Q = a(1 + exc)$ ]  $\rightarrow 1$  имеет особенности, поэтому ею можно пользоваться только в случаях, когда выражение  $q + Q - 1 - q \cdot Q \neq 0$ . В противном случае вероятность  $v_2 \rightarrow \infty$ . Из анализа рис. 5, где приведена кумулятивная гистограмма метеорных потоков по параметру  $q + Q - 1 - q \cdot Q$ , следует, что в диапазон  $q + Q - 1 - q \cdot Q < 0.01$  попадают 487 или 10.4 % потоков. В работе [5] отмечено, при выводе формулы для вероятности  $v_2$  не учитывались вековые возмущения эксцентриситетов и наклонений орбит КТ.

Чтобы учесть изменения данных элементов орбиты, можно использовать, как показано в

[6], квазистационарные параметры орбиты КТ Моисеева  $C1 = (1 - ex^2) \cos^2(incl) = const$  и Лидова  $C2 = ex^2(0.4 - \sin^2(incl) \sin^2(\omega)) = const$  ( $\omega$  – аргумент перигелия орбиты КТ).

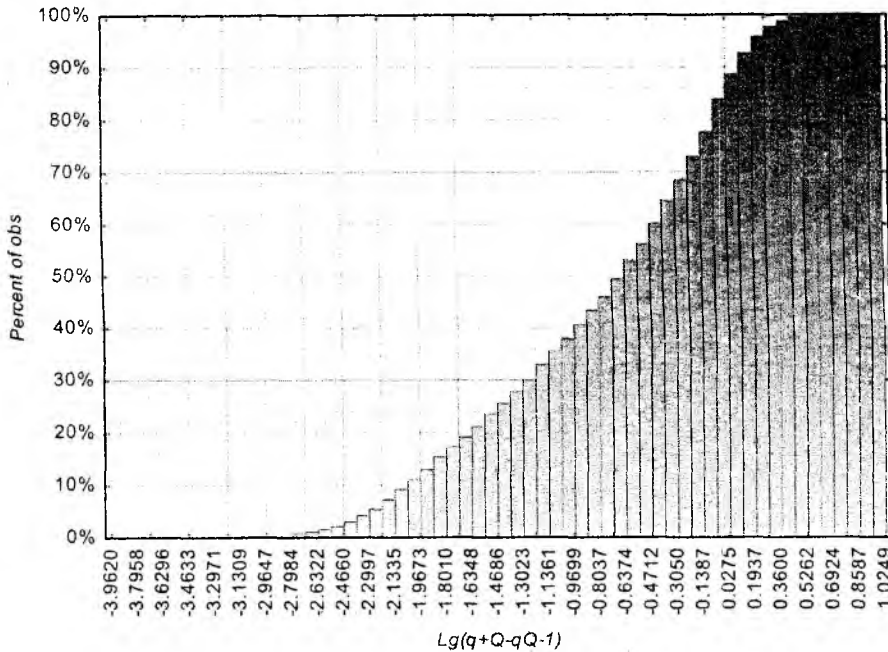


Рис. 5

Согласно [6] алгоритм расчета вероятности столкновения космического тела с Землей следующий:

1) дискриминант уравнения

$$p^2 - p \left[ C1 \cdot a - \frac{0.6}{a} + 2 \right] + 0.4 - C1 \cdot (1 - 2a) - C2 = 0 \quad (4)$$

меньше нуля, следовательно, орбиты тела и Земли никогда не пересекаются, и вероятность их встречи равна нулю;

2) дискриминант уравнения (4) больше нуля, но только один корень  $p_x$  удовлетворяет условию

$$p_x < a \left( 1 - 2.5e^2(0.4 - \sin^2(i) \sin^2(\omega)) \right), \quad (5)$$

тогда вероятность столкновения КТ с Землей определяется по формуле

$$v_0 = \frac{1811 \cdot 10^{-7} (3 - a^{-2} - 2\sqrt{a(1-ex^2)} \cos(incl) - 0.141)}{\pi a^{3/2} \sin(incl_x) \sqrt{(3 - a^{-2} - 2\sqrt{a(1-ex^2)} \cos(incl)) (2 - a^{-2} - p_x)}}, \quad (6)$$

где

$$incl_x = \arccos \left( \sqrt{\frac{a(1-ex^2)}{p_x}} \cos(incl) \right); \quad (7)$$

3) дискриминант уравнения (4) больше нуля и оба корня  $p_1$  и  $p_2$  удовлетворяют условию (5), тогда вероятность столкновения КТ с Землей определяется по формуле

$$v_0 = \frac{1811 \cdot 10^{-7} (3 - a^{-2} - 2\sqrt{a(1-ex^2)} \cos(incl) - 0.141)}{\pi a^{3/2} \sqrt{(3 - a^{-2} - 2\sqrt{a(1-ex^2)} \cos(incl))}} \times \left( \frac{(2 - \frac{1}{a} - p_1)^{-0.5}}{\sin(incl_1)} + \frac{(2 - \frac{1}{a} - p_2)^{-0.5}}{\sin(incl_2)} \right), \quad (8)$$

где наклонения  $incl_1$  и  $incl_2$  рассчитываются по (7) путем постановки  $p_1$  и  $p_2$  соответственно.

На рис. 6 приведены категоризированные диаграммы вероятности  $v_0$  (чем больше размер символа «о», тем больше вероятность  $v_0$ ) в функции элементов орбит метеорных потоков каталога ХНУРЭ – наклонения, эксцентриситета и перигелийного расстояния.

Как видно из графиков на рис. 6, наибольшую вероятность встречи космического тела с

Землей имеют потоки (и их потенциальные родительские тела NEOs), орбиты которых имеют наклоны  $i_{rel} > 170^\circ$ .

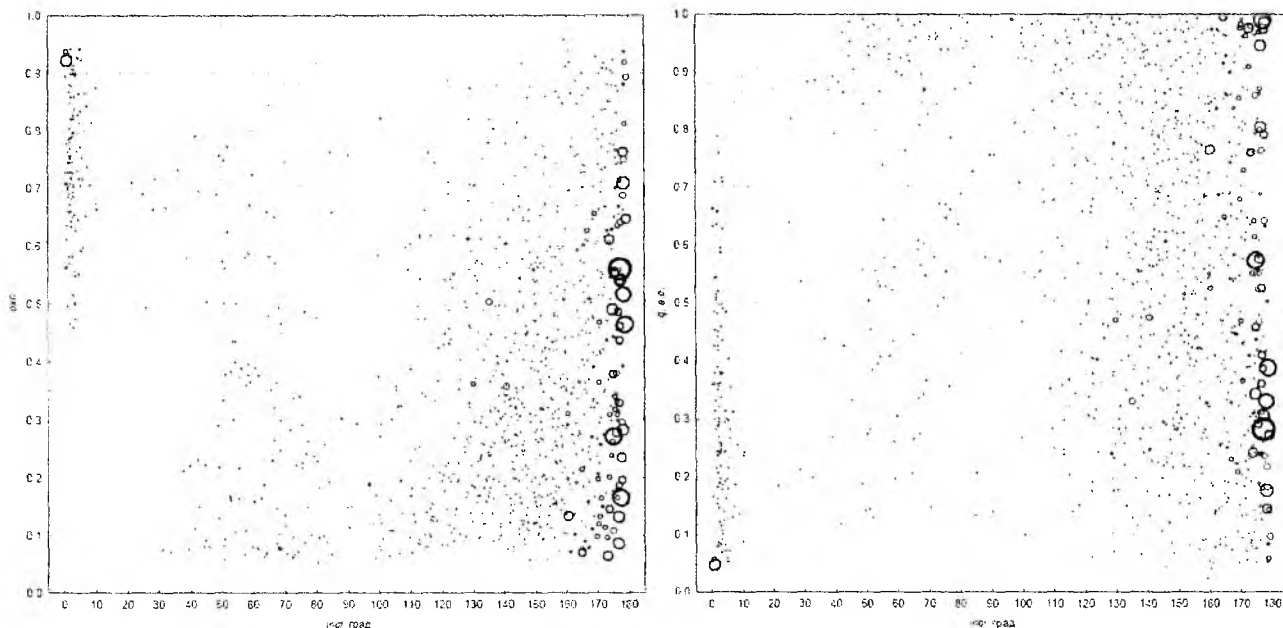


Рис. 6

На рис. 7 дана диаграмма вероятность  $v_0$  – критерий Кресака  $P_e$ . Наибольшую вероятность встречи космического тела с Землей имеют потоки астероидного происхождения.

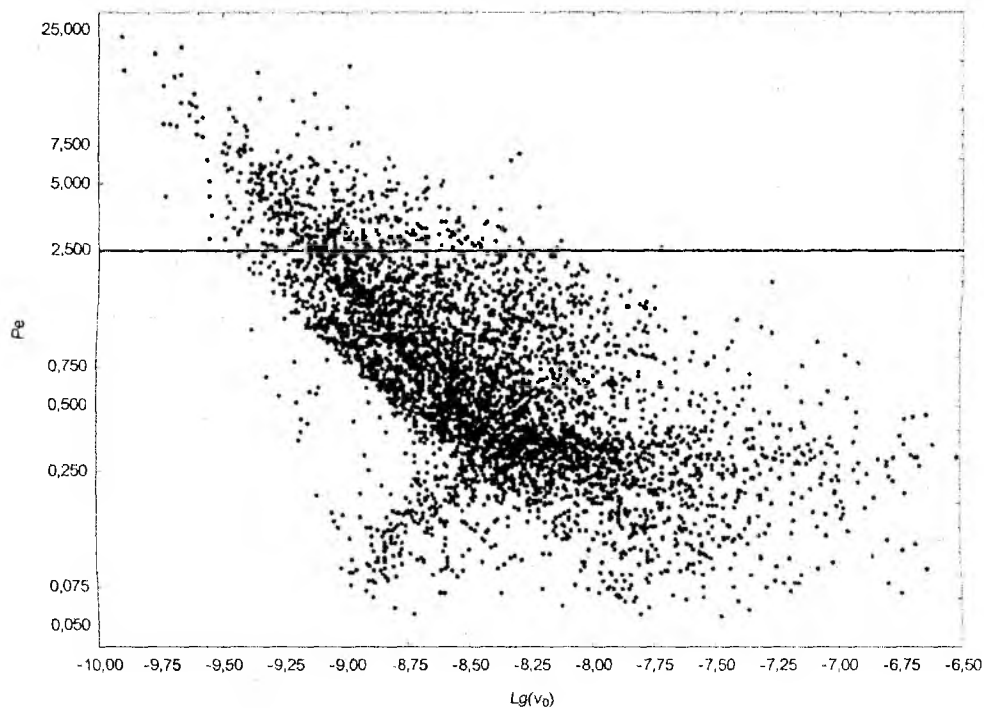


Рис. 7

Следует напомнить, что (6) и (8) дают оценку вероятности столкновения  $v_0 = v_1 v_2$ . Для родительских тел метеорных потоков в предположении, что они имеют орбиты, совпадающие со средними орбитами соответствующих потоков, вероятность  $v_1$  близка к 1. Тогда вероятность столкновения  $v'_2 = v_0/v_1$  резко возрастает.

На рис. 8 приведены категоризированные диаграммы вероятности  $v'_2$  (чем больше раз-

мер символа «○», тем больше вероятность  $v'_2$ ) в функции элементов орбит метеорных потоков каталога ХНУРЭ – наклонения, эксцентриситета и перигелийного расстояния.

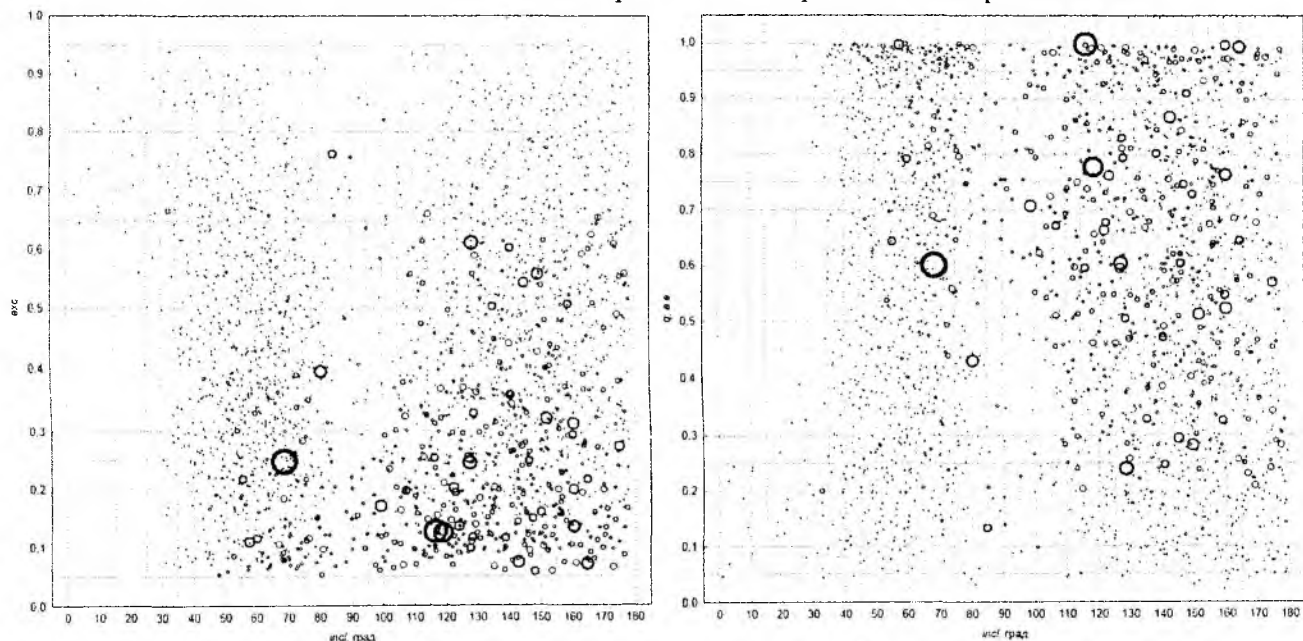
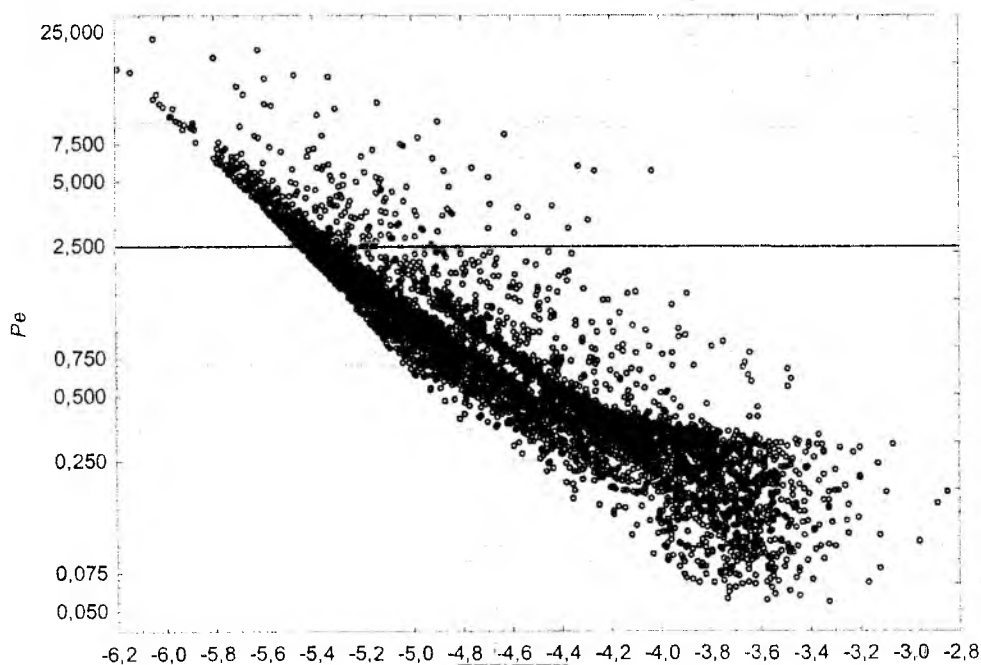


Рис. 8

Как видно из графиков на рис. 8, наибольшую вероятность столкновения гипотетических родительских тел метеорных потоков, при условии, что эти потоки проявляли себя в атмосфере Земли, имеют потоки, орбиты которых имеют наклоны  $incl > 90^\circ$ , эксцентриситеты  $exs < 0.3$  и перигелийные расстояния  $q > 0.5$  а.е.

На рис. 9 приведена диаграмма вероятность  $v'_2$  – критерий Кресака  $Pe$ . Как видно из графика на рис. 9, наибольшую вероятность  $v'_2$  имеют потоки астероидного происхождения.



## Выводы

1. Из 200 наиболее «опасных» метеорных потоков по оценкам вероятности  $v'_2$  большинство потоков, во-первых, имеют ретроградные орбиты (для 177 потоков или 88.5 % выполняется условие  $incl > 90^\circ$ ), причем максимальная вероятность  $v'_2$  соответствует наклонениям  $incl \approx 60^\circ$  и  $120^\circ$ ; во-вторых, пересекают орбиту Земли либо в афелии (для 157 потоков или 78.5 % выполняется условие  $1 < Q < 1.05$  а.е.), либо в перигелии (для 34 потоков или 17 % выполняется условие  $0.95 < q < 1$  а.е.).

2. Значения эксцентриситетов анализируемых потоков расположены в диапазоне  $0.05 < exc < 0.76$ , причем для 178 потоков или 89 % выполняется условие  $exc < 0.5$ ; значения большей полуоси расположены в диапазоне  $0.57 < a < 1.54$  а.е., причем для 162 потоков или 81 % выполняется условие  $a < 1$  а.е., что говорит в пользу их астероидного происхождения, а именно астероидов группы Atens – околоземных астероидов, чьи орбиты пересекают земную орбиту с внутренней стороны: афелийные расстояния орбит больше перигелийного расстояния Земли  $Q > 0.983$  а.е. и большая полуось меньше земной  $a < 1$  а.е.

Всего на данный момент (апрель 2017 г.) известно 1176 астероидов группы Atens. Столь малая популяция объясняется, во-первых, тем, что наблюдение визуальными методами NEOs Atens возможно только в ночное время суток, когда они оказываются от Солнца дальше, чем Земля (причем, чем меньше афелийные расстояния орбит астероидов, тем сложнее их обнаружить, поскольку появляются они над горизонтом лишь незадолго перед рассветом или сразу после захода Солнца и легко теряются в его лучах на фоне еще светлого неба); во-вторых, астероиды группы Atens имеют малые размеры (у наиболее крупного всего 3,4 км), следовательно, и обнаружить их ночью на фоне темного неба также сложнее.

3. Вероятность хотя бы одного столкновения Земли с родительскими телами анализируемых потоков в год составляет 0.074 или, в среднем, 74 столкновения за 1000 лет. Вероятность хотя бы одного столкновения Земли с родительскими телами потоков из каталога ХНУРЭ в год составляет 0.304 или, в среднем, 304 столкновения за 1000 лет.

4. Для решения задачи прогнозирования астероидно-кометной опасности, во-первых, требуется целенаправленный поиск астероидов группы Atens (особенно с ретроградными орбитами); во-вторых, требуются исследования в области теории квантования пространства орбит метеорных тел в Солнечной системе с целью подтверждения гипотезы группирования генетически не связанных метеорных тел на общей стабильной орбите, т.е. гипотезы формирования метеорного потока без родительского тела из спорадического фона.

**Список литературы:** 1. Волощук, Ю.И. Метеорные потоки и ассоциации, выявленные по результатам многолетних радиолокационных наблюдений метеоров в Харькове : монография / Ю.И. Волощук, Д.Ю. Горелов. – Харьков : Изд-во НТМТ, 2011. – 382 с. 8. 2. Southworth R.D., Hawkins G.S. Statistics of Meteor Streams // *Smithson. Contribs. Astrophys.* -1963. – №7. – P. 261-285. 3. Öpik E. Collision probabilities with the planet and the distribution of interplanetary matter // *Proc. Roy. Irish. Acad.* – 1951. – N 12. – P. 165-169. 4. Kresak, L. Relation of Meteor Orbits to the Orbits of Comets and Asteroids // *Smithson. Contribs. Astrophys.* – 1967. – V. 11. – P. 9–34. 5. Крамер, Е.Н., Шеатака, И.С. Вероятность выпадения на поверхность планет межпланетных тел типа Аполлона – Амура // *Астрон. вестн.* – 1987. – Т. 21, №3. – С. 225-232. 6. Горелов, Д.Ю. Вероятность столкновения гипотетических родительских тел метеорных потоков с Землей / Д.Ю. Горелов, Н.В. Плащенко // *Радиотехника.* – 2009. – Вып. № 157. – С. 30-36.

Харьковский национальный  
университет радиозлектроники

Поступила в редколлегию 04.04.2017

## РАСПРЕДЕЛЕНИЕ ПЛОТНОСТИ ПОТОКА ФОТОНОВ В ДИФРАКЦИОННОЙ КАРТИНЕ ОТ ОДНОЙ И ДВУХ ПАРАЛЛЕЛЬНЫХ ЩЕЛЕЙ

### Введение

В работах [1, 2] отмечалось, что парадокс, заключающийся в различии интерференционных картин при прохождении света через одну и две узкие щели (см. рис.1, 2) снимается предположением о том, что частицы (фотоны или электроны), проходя через щель, взаимодействуют с веществом и приобретают, рассеиваясь на электронах, дискретные значения импульса. При дифракции на двух щелях максимумы в интерференционной картине наблюдаются в тех местах, куда, при рассеянии, попадают частицы, а минимумы соответствуют точкам, куда частицы не попадают. В случае дифракции на одной щели получается плавная кривая распределения интенсивности. Это объясняется тем, что спектр электронов, находящихся в полубесконечных плоскостях, является непрерывным, следовательно, и угол дифракции рассеянных частиц принимает непрерывные значения.

Авторы [1, 2], основываясь на законах сохранения импульса и энергии, получили количественное соотношение, определяющее положение максимумов на дифракционной картине:

$$a \frac{\sin \varphi}{1 + \cos \varphi} = m \frac{\lambda}{2}. \quad (1)$$

Полученное соотношение (1), в случае малых углов дифракции, совпадает с известным из волновой оптики [3] выражением

$$a \sin \varphi = m\lambda, \quad (2)$$

где  $m = 0, \pm 1, \pm 2, \dots$ ,  $a$  – ширина металлической ленты, разделяющей щели;  $\lambda$  – длина волны фотонов (или электронов), падающих на экран с двумя щелями,  $\varphi$  – угол дифракции.

### Распределение интенсивности фотонов при дифракции на одной щели

При определении математического выражения для распределения интенсивности в дифракционной картине ограничимся получением соотношения, справедливого при тех же предположениях, что и в работах [1, 2], а именно:

- 1) фотон, проходя через щель, взаимодействует с электроном;
- 2) столкновение фотона с электроном происходит по закону абсолютно-упругого удара;
- 3) щель – узкая.

Будем считать также, что ось X декартовой системы координат совмещена с плоскостью экрана и направлена перпендикулярно щели. Фотон движется перпендикулярно экрану вдоль оси Y.

В известном опыте Л.М. Бибермана и др. [4] доказано, что дифракционная картина при дифракции потока частиц получается такой же, как и при длительной экспозиции, когда каждый электрон проходит через щель индивидуально. Время пролета электрона в упоминаемом опыте было равным  $7 \cdot 10^{-9}$  с, а интервал времени (скважность) между

пролетом двух очередных электронов составлял  $3 \cdot 10^{-5}$  с. Таким образом, опыт показывает, что в данном случае имеет место только явление дифракции.

При таком представлении возникает вопрос, как же это стало возможно, когда без учета взаимодействия частицы с веществом экрана в волновой оптике получается правильное, совпадающее с экспериментом выражение для определения интенсивности света в дифракционной картине? Сравним с ситуацией, которая наблюдается в более длинноволновой области при изучении явления дифракции электромагнитных волн на решетке из идеально проводящих лент. Для получения дифракционной картины, отраженной от решетки и прошедшей волны, решается краевая задача с постановкой конкретных граничных условий, учитывающих электродинамические свойства структуры.

Следует отметить, что работ, посвященных дифракции электромагнитных волн достаточно много. Среди них уместно отметить работу [5], положившую начало строгому решению задач о дифракции электромагнитных волн на периодических структурах. В данной работе задача о дифракции плоской волны на решетке, образованной периодической последовательностью бесконечно тонких идеально проводящих лент была сведена к решению краевой задачи Римана – Гильберта.

В случае дифракции монохроматического пучка фотонов на одной щели амплитуда вероятностей попадания частиц в какую-либо точку экрана с координатой  $x$  (см. рис. 1) может быть представлена пси-функцией (или амплитудой):

$$\psi_1 = c_1 \frac{e^{\mp i\vec{k}\vec{r}}}{\sqrt{r}}, \quad (3)$$

где  $|\vec{k}| = \frac{2\pi}{\lambda}$  – волновой вектор плоской волны де-Бройля, поставленной в соответствие фотону, имеющий две составляющие  $\vec{k} = \vec{i}k_x + \vec{j}k_y$ ; где  $k_x$  – составляющая, приобретенная фотоном вследствие упругого столкновения с электроном, находящимся в состоянии свободного движения в полуплоскостях, лежащих по обе стороны от щели 1 и 2 (см. рис. 1), а  $k_y$  – равно волновому числу фотона. Верхний знак в выражении (3) соответствует электрону, движущемуся в полуплоскости (2), нижний – в полуплоскости (1).

Как известно [6], спектр импульсов электронов в полупространстве является непрерывным. Следовательно, кривая распределения вероятностей части фотонов будет описываться плавной кривой:

$$|\psi_1|^2 = \frac{|c_1|^2}{|\vec{r}|}. \quad (4)$$

При  $r = y, (x = 0)$ ,  $|\psi_1|^2$  достигает максимума и плавно спадает при положительных и отрицательных значениях  $x$ .

### **Распределение потока фотонов при дифракции света на двух щелях**

Пусть на бесконечно тонкий металлический экран с двумя бесконечно протяженными в направлении лент щелями падает монохроматический пучок фотонов (см. рис. 2).

Будем считать, что квантовомеханической моделью ленты является бесконечно глубокая потенциальная яма. Электроны, совершающие свободное движение в яме, будут иметь дискретные значения импульсов [6].

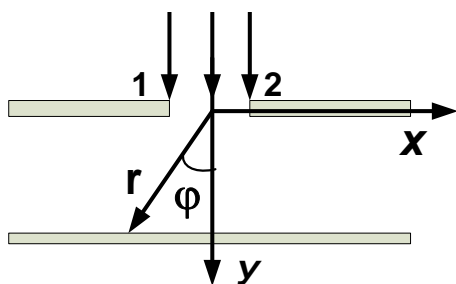


Рис. 1. Дифракция света на щели

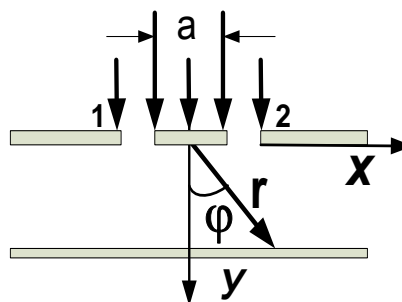


Рис. 2. Дифракция света на двух щелях

Займемся определением вероятности попадания фотона в произвольную точку экрана наблюдения с координатой  $x$ . В данном случае у фотона имеется четыре возможности: 1) фотон проходит через щель 1 и взаимодействует с электроном из ленты или же с электроном из бесконечной полуплоскости; 2) фотон проходит через щель 2 и реализуется один из вариантов первого пункта. Если положить плотность потока частиц равным единице, то пси-функцию  $\psi$  (амплитуду вероятности) падающего фотона можно представить в виде волны де-Бройля:

$$\psi = e^{iky} = e^{i\frac{p_\phi}{\hbar}y}, \quad (5)$$

где  $p_\phi = k\hbar = \frac{2\pi}{\lambda}\hbar$  – импульс фотона,  $\lambda$  – длина волны де-Бройля, которую мы сопоставляем с фотоном. Проходя через щель, фотон испытывает упругое столкновение с электроном, совершающим свободное движение в потенциальной яме. Амплитуду электрона (опускаем «вероятности» для краткости) представляем в виде суммы двух бегущих в противоположных направлениях волн:

$$\psi = c \begin{pmatrix} e^{i\frac{p_e}{\hbar}x} & -e^{-i\frac{p_e}{\hbar}x} \end{pmatrix}. \quad (6)$$

При произведении операций с амплитудами будем следовать правилам, сформулированным в работе [7]. Учитывая, что взаимодействие частиц соответствует произведению амплитуд, а также то, что для двух зависимых событий конечное состояние которых одинаково, амплитуда вероятности события, соответствующего случаю, когда фотон попадает в некоторую точку экрана, определяется суммой амплитуд, получаем:

$$\psi_{1z} = \psi_1 + \psi_2 = \frac{c}{\sqrt{r}} e^{i\frac{p_f}{\hbar}y} \left( e^{i\frac{p_e}{\hbar}\left(x-\frac{a}{2}\right)} + e^{i\frac{p_e}{\hbar}\left(x+\frac{a}{2}\right)} \right). \quad (7)$$

Здесь первое слагаемое соответствует фотону, прошедшему через щель 1, второе – фотону, прошедшему через щель 2. Соответствующее выражение для вероятности попадания фотона в точку экрана, вследствие взаимодействия фотона с электроном, двигающимся в пластине, разделяющей две щели, будет иметь вид

$$P = \frac{|c|^2}{|r|} \left( 1 + \cos 2\frac{p_e}{\hbar}a \right). \quad (8)$$

Согласно [6], значения импульса  $P_e$ , которые может иметь электрон в бесконечно глубокой потенциальной яме, определяются из выражения

$$p_e = \frac{\pi n}{a} \hbar,$$

где  $n = \pm 1, \pm 2, \dots$

Таким образом, для вероятности  $P$  получаем выражение

$$P = \frac{|c|^2}{|r|^2} (1 + \cos 2\pi n). \quad (9)$$

Полная вероятность попадания частицы в точку с координатой  $x$  должна определяться суммой выражений (4) и (9). Однако анализ графиков распределения интенсивности пучка электронов, полученных в работе [8] при дифракции электронов на решетке металлических лент, позволяет заключить, что «фон», создаваемый слагаемым (4), незначителен. Поэтому, с учетом пренебрежения этим фоном, можно считать, что картина дифракции будет описываться выражением (9). Из анализа соотношения (9) видно, что центральный максимум (когда  $n = 0$ ) будет равен  $\frac{4|c|^2}{r^2}$ . Боковые максимумы будут симметрично расположены относительно центрального, а их интенсивность будет убывать с увеличением расстояния как  $\frac{1}{|r|}$ .

### Выводы

В работе использован квантово-механический подход к решению задачи о дифракции фотонов на одной и двух щелях. Главной его особенностью является то, что явление дифракции объясняется упругим взаимодействием фотонов с электронами, обладающими дискретными значениями импульсов, что и обуславливает вид дифракционной картины, в случае, когда открыты обе щели. Полученный результат находится в согласии с выводами, вытекающими из эксперимента Л.М. Бибермана, Н.Г. Сушкина, В.А. Фабриканта, в котором дифракционная картина была получена для пучка частиц такой малой интенсивности, что временной интервал между прохождением каждого отдельного электрона от источника до фотопластинки был намного больше времени пролета.

**Список литературы:** 1. Безуглый, А.В. Дифракция фотонов на системе параллельных щелей // Радиотехника. – 2006. – Вып. 147. – С. 65-68. 2. Безуглый, Є.А., Безуглий А.В., Петченко О.М. Дифракція електронів на ґратці нескінченно тонких металевих стрічок // Вісник Харк. нац. ун-ту імені В.Н. Каразіна. Серія «Фізика». – 2012. – Вип. 17, № 1020. – С. 74-77. 3. Борн, М., Вольф, Э. Основы оптики. – М.: Наука, 1973. – С. 371. 4. Биберман, Л.М., Сушкин, Н.Г., Фабрикант, В.А. Дифракция одиночных поочередно летящих электронов // ДАН СССР. – 1949. – Т. 66, № 2. – С. 185. 5. Аграпович, З.С., Марченко, В.А., Шестопалов, В.П. Дифракция электромагнитных волн на плоских металлических решетках. – 1962. – Т. 32, № 4. – С. 381-394. 6. Ландау, Л.Д., Лифшиц, Е.М. Теоретическая физика. – М., 1963. – Т. 3. – С. 63, 87-89. 7. Фейнман, Р., Лейтон, Р., Сэндс, М. Фейнмановские лекции по физике. – 1966. – Т. 8. – С. 11-23. 8. Jonsson, C. Electroneninterferenzen an mehreren kunstlich hergestellten Feinspalten // Zs. Phys. – 1961. – P. 454-474.

Харьковский национальный университет  
городского хозяйства имени А.Н. Бекетова

Поступила в редколлегию 25.03.2017

## ОПРЕДЕЛЕНИЕ ЗАВИСИМОСТИ ХАРАКТЕРИСТИК ФОТОННОЙ ЗАПРЕЩЕННОЙ ЗОНЫ ОТ ПОКАЗАТЕЛЯ ПРЕЛОМЛЕНИЯ МАТЕРИАЛА

### Введение

Для моделирования распространения электромагнитных волн через фотонный кристалл рассмотрено распространение поперечной составляющей излучения (ТЕ-волны). Рассматриваемая структура фотонного кристалла представляет собой треугольную периодическую структуру, состоящую из стержней, окруженных воздухом (рис. 1). Диаметр стержней выбран  $d=125$  нм, расстояние между центрами стержней –  $\Lambda=380$  нм. Таким образом, соотношение  $d/\Lambda=0,33$ . Моделирование распространения ТЕ-волн ( $E_z$ ) проводилось в пределах видимой и инфракрасной области спектра в диапазоне длин волн от 0,2 до 2 мкм, был проведен расчет для 300 значений длин волн. Для моделирования распространения электромагнитных волн через рассматриваемую структуру мы возбуждали плоскую волну  $E_z$ , которая распространяется вдоль оси ОХ, и производили расчет плотности потока мощности излучения, исходящего через правую границу с использованием метода конечных элементов. Поскольку структура фотонного кристалла, изображенная на рис. 1, не имеет физических границ, мы использовали граничное условие рассеяния на всех границах структуры.

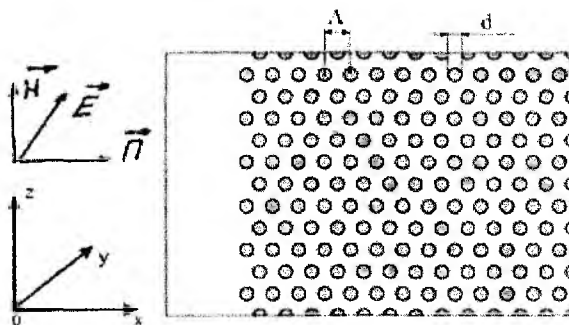


Рис. 1. Геометрическая структура рассматриваемого фотонного кристалла

Амплитуда возбуждаемой плоской волны  $E_z=1$  В/м. Плотность потока мощности излучения рассчитывалась для всех 300 длин волн в пределах рассматриваемого диапазона.

В качестве материалов, применяемых для изготовления фотонных кристаллов, в оптическом диапазоне выбраны следующие материалы: GaAs, политетрафторэтилен (фторопласт-4, Teflon FEP), полиимиды (Kapton HN, Kapton E), кварц. Коэффициент преломления представленных материалов практически не изменяется в рассматриваемом диапазоне длин волн. В таблице представлены значения показателей преломления выбранных материалов в ближнем инфракрасном диапазоне:

	Фторопласт-4	Kapton® HN	Kapton® E	Кварц	GaAs
$n$	1,36	1,7	1,9	1,46	3,4

На рис. 2 показана зависимость коэффициента преломления от длины волны ЭМ излучения для некоторых видов политетрафторэтилена и полиимидов. Как видно из представленных зависимостей, тефлон имеет нормальную дисперсию, поскольку коэффициент преломления увеличивается с уменьшением длины волны излучения. Нормальная дисперсия отмечается длиной волны света, приближающейся к краю фундаментального поглощения [2].

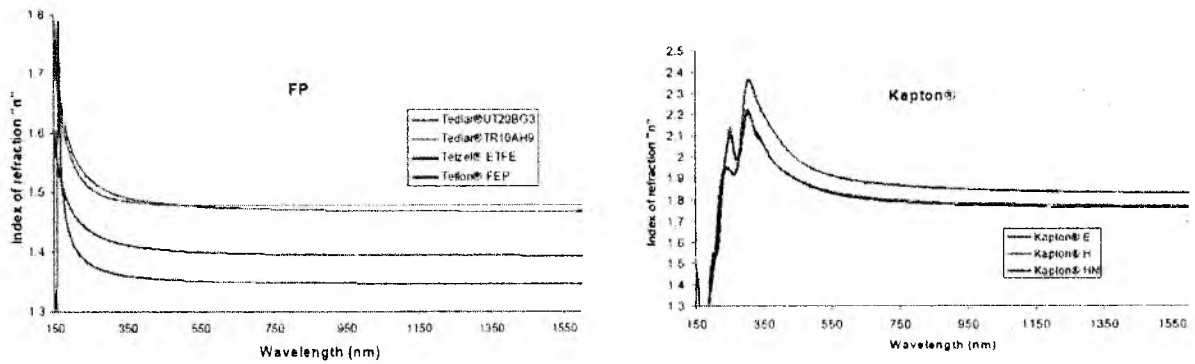


Рис. 2. Зависимость коэффициента преломления от длины волны ЭМ излучения для Teflon FEP и Kapton HN [1]

Также отметим, что показатель преломления у полиимидов значительно выше показателя преломления других видов полимеров. На рис. 2 представлена как нормальная дисперсия (показатель преломления увеличивается с уменьшением длины волны), так и аномальная, которая наблюдается при длине волны ниже края фундаментального поглощения. При этом наблюдается уменьшение значения показателя преломления с уменьшением длины волны. Учитывая представленные особенности, не будем проводить моделирование распространения излучения на длинах волн менее 500 нм.

На рис. 3 представлена зависимость нормированного значения плотности потока мощности, проходящего через исследуемую структуру (рис. 1), от длины волны излучения. Полученные результаты показывают, что рассматриваемая структура обладает свойствами фотонного кристалла и обладает ярко выраженной запрещенной зоной.

Как видно из рис. 3, в видимой области при длине волны порядка 640 нм оптическое излучение практически не проходит через данную структуру.

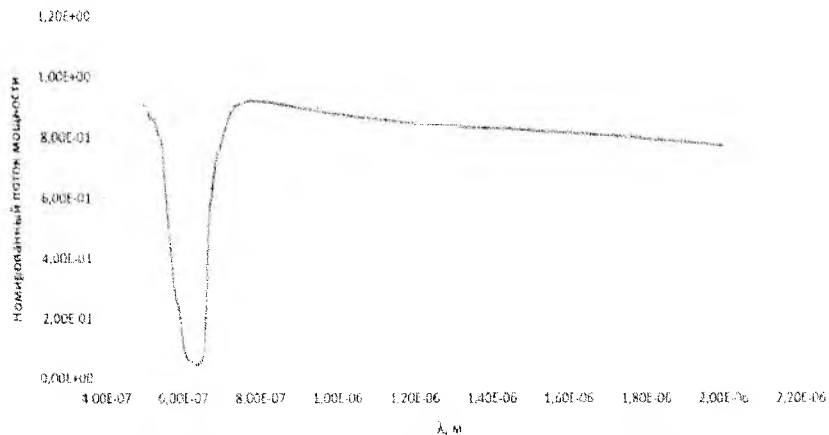
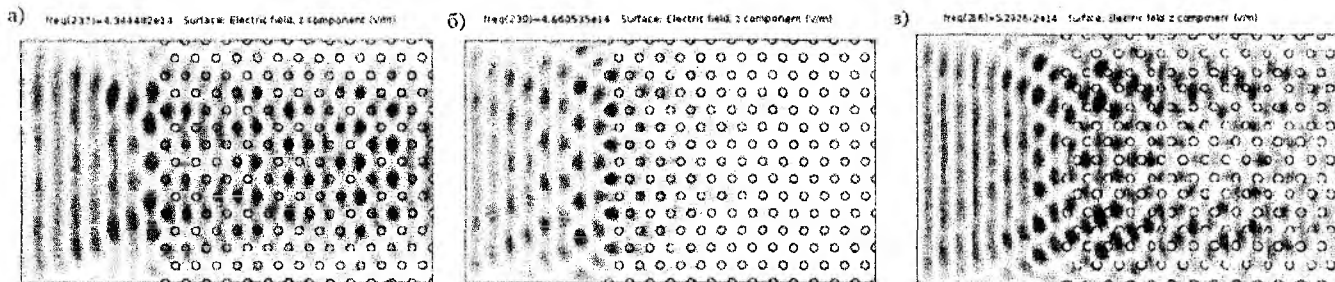


Рис. 3. Зависимость нормированного потока мощности излучения от длины волны

Представленный фотонный кристалл обладает узкой запрещенной зоной, ширина которой составляет около 50 нм.

Наличие части проходящего излучения может свидетельствовать о том, что данный фотонный кристалл может недостаточно хорошо отражать падающую волну и может иметь значительную глубину проникновения излучения. Для проверки этой гипотезы приведем результаты распределения  $E_z$  в фотонном кристалле. На рис. 4 представлено распределение  $E_z$  волн в фотонном кристалле при длинах волн выше ФЗЗ, в пределах ФЗЗ и ниже ФЗЗ.



Результаты при длинах волн: *a* – выше ФЗЗ,  $\lambda=676$  нм; *b* – в пределах ФЗЗ,  $\lambda=644$  нм; *c* – ниже ФЗЗ,  $\lambda=567$  нм

Рис. 4. Распределение поля  $E_z$  через фотонный кристалл

Представленные результаты распространения ТЕ-волн через фотонный кристалл, как и предполагалось, показывают, что при длинах волн ниже и выше ФЗЗ ТЕ-волны распространяются в фотонном кристалле (рис.4, *a*, *c*), а в пределах ФЗЗ входящее оптическое излучение отражается от исследуемого фотонного кристалла. Таким образом, как видно на рис. 4, *b*, ТЕ-волны проникают в фотонный кристалл и постепенно затухают.

На рис. 5 представлено распределение амплитуды ТЕ-волны (проходящей через центральную часть ФК) от глубины проникновения в фотонном кристалле при длине волны  $\lambda=644$  нм, которая входит в ФЗЗ. Как видно, на рис. 5 амплитуда ТЕ-волны затухает по экспоненциальному закону.

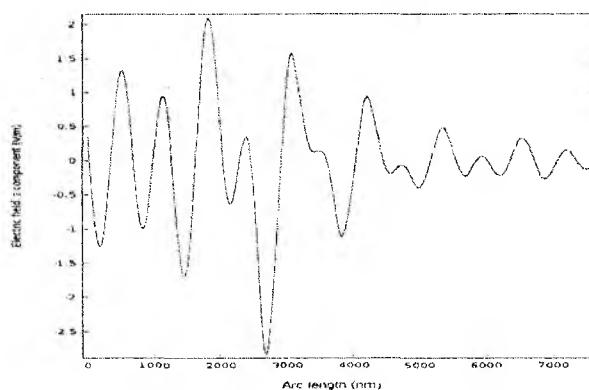


Рис. 5. Распределение амплитуды  $E_z$  в ФК от глубины проникновения в пределах ФЗЗ

Таким образом, фотонная запрещенная зона исследуемого фотонного кристалла, представленная на рис. 3, не достигает нулевого порога в связи с тем, что фотонный кристалл имеет конечные размеры. Исходя из этого для улучшения характеристик ФЗЗ можно увеличить размеры фотонного кристалла, уменьшив таким образом исходящее излучение.

### Моделирование распространения ТЕ-волн через GaAs фотонный кристалл

Для моделирования использовался образец с такими же геометрическими характеристиками, как и представленный на рис. 1 ( $d=125$  нм,  $\Lambda=380$  нм). В качестве материала выбран GaAs, поскольку этот полупроводниковый материал обладает наибольшим показателем преломления из материалов (см. таблицу,  $n=3,4$ ). Результаты моделирования распространения ТЕ-волн через рассматриваемый фотонный кристалл представлены на рис. 6. Также на рисунке представлена зависимость для образца с идентичной структурой, представленной на рис. 4. Как видно из рисунка, фотонный кристалл, изготовленный из GaAs, обладает намного более широкой запрещенной зоной, которая к тому же смещена в область более длинных волн.

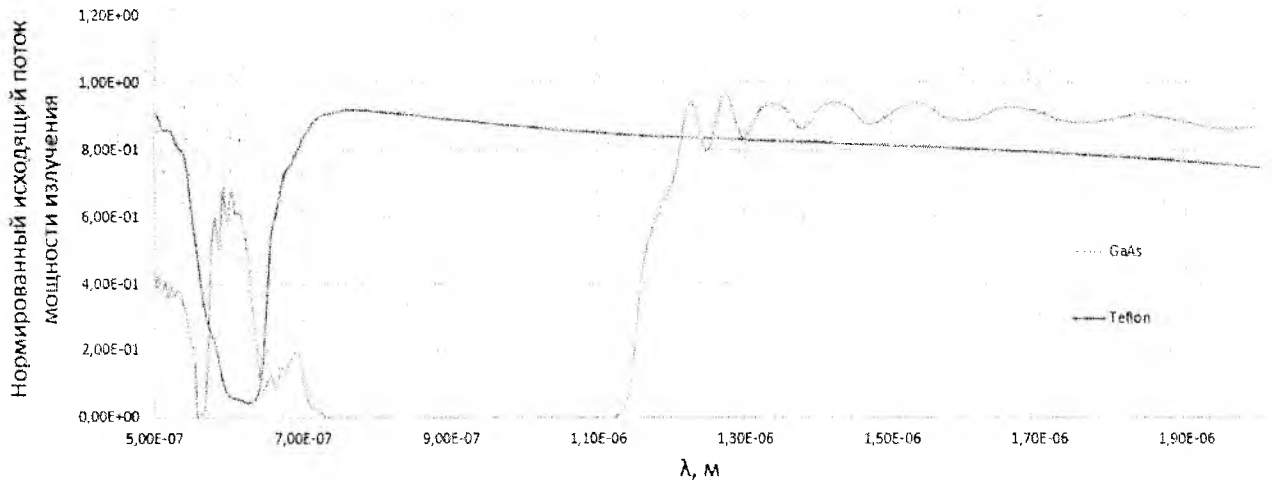


Рис. 6. Зависимость нормированного исходящего потока мощности излучения от длины волны в фотонном кристалле, состоящем из стержней GaAs

На рис. 7 представлено распространение TE-волн через данный фотонный кристалл. Полученные результаты показывают, что образец, изготовленный из тефлона, имеет ширину запрещенной зоны  $\Delta\lambda \approx 30$  нм, а изготовленный из GaAs – 370 нм. Кроме того, из рис. 7 очевидно, что образец, изготовленный из арсенида галлия, имеет значительно меньшую глубину проникновения излучения и намного более эффективно отражает падающую волну, чем образец, изготовленный из тефлона (см. рис. 4, б).

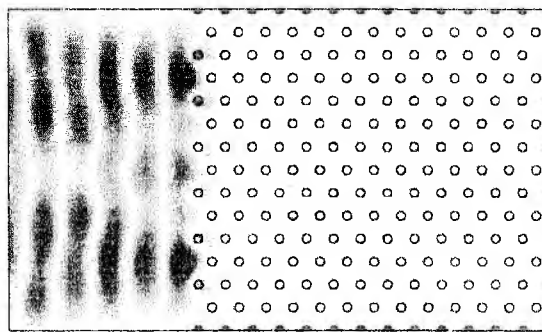


Рис. 7. Распределение TE-поля через фотонный кристалл при  $\lambda=900$  нм (в области ФЗЗ)

### Определение зависимости характеристик ФЗЗ от показателя преломления материала

Как известно, в оптике и фотонике наиболее широкое применение нашли устройства и линии передачи, работающие в инфракрасном диапазоне при длинах волн в области 1,5 мкм. Очевидно, что эта область инфракрасного спектра является наиболее перспективной для новых устройств и интегральной оптики. Поэтому целесообразно дальнейшее рассмотрение фотонных кристаллов, запрещенные зоны которых будут располагаться в этой области спектра.

Ранее мы определили, какими соотношениями  $d/\Lambda$  должен обладать фотонный кристалл, чтобы его ФЗЗ имела наилучшие характеристики. Учитывая, что показатель преломления материалов, представленных в таблице, практически не изменяется в рассматриваемой области длин волн, можно сделать предположение, что при сохранении соотношения  $d/\Lambda$  в рассматриваемом фотонном кристалле можно сместить расположение ФЗЗ в область более длинных волн увеличивая диаметр стержней и шаг.

Для определения зависимости характеристик ФЗЗ от показателя преломления создана структура, соответствующая структуре, представленной на рис. 1, с  $d=395$  нм,  $\Lambda=750$  нм. В полученном образце соотношение  $d/\Lambda=0,53$ . Такое же соотношение  $d/\Lambda$  имел образец из тефлона с  $d=200$ , центр запрещенной зоны которого (как видно из рисунка) располагался на длине волны около 660 нм. Таким образом, мы увеличили шаг между стержнями практически в два раза. Учитывая, что показатель преломления тефлона практически не изменится при переходе в ближнюю инфракрасную область, можно предположить, что центральная часть фотонной запрещенной зоны нового образца будет находиться на длине волны  $\lambda=1,33$  мкм. На рис. 8 можно наблюдать ФЗЗ двух структур, изготовленных из тефлона с  $\Lambda=380$  и  $\Lambda=750$ . Для упрощения вычислений рассчитывали плотность потока мощности излучения нового образца в диапазоне длин волн 0,8 – 2 мкм.

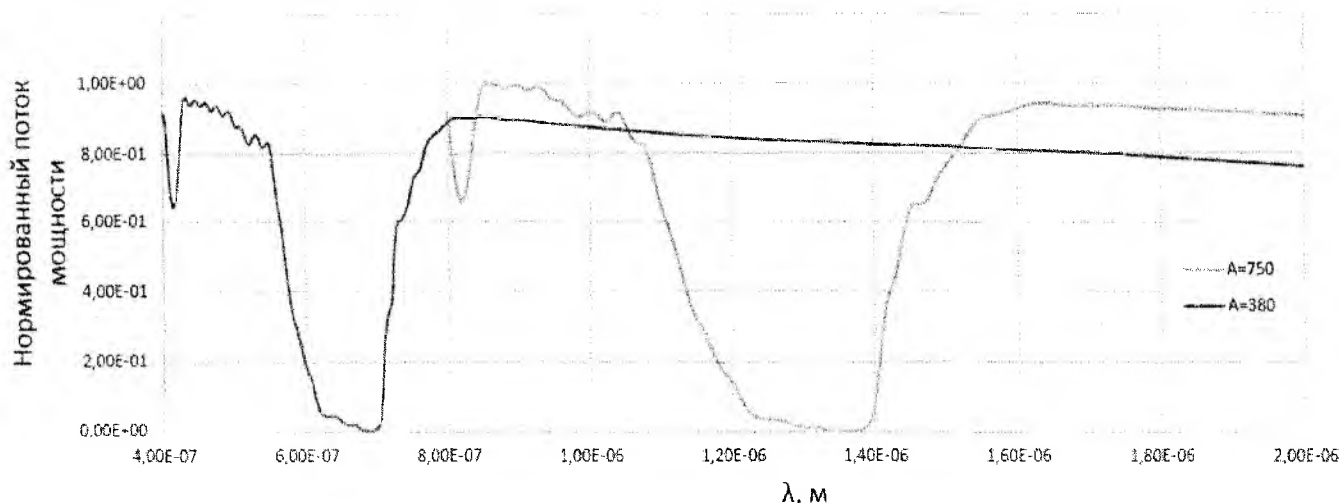


Рис. 8. Расположение ФЗЗ образцов с  $\Lambda=380$  и  $\Lambda=750$

Как видно из рис. 8, ФЗЗ исследуемого образца располагается точно в пределах  $\lambda=1,3 - 1,36$  мкм, как и ожидалось. Кроме того, при увеличении диаметра стержней и расстояния между их центрами в два раза мы наблюдаем увеличение ширины запрещенной зоны также в два раза. Полученные результаты свидетельствуют о том, что при сохранении соотношения  $d/\Lambda$  можно смещать ФЗЗ в область коротких или длинных волн при сохранении характеристик самой ФЗЗ.

Исходя из результатов, представленных выше, можно сделать вывод, что при сохранении соотношений  $d/\Lambda$  и  $\Lambda/\lambda$  возможно точно прогнозировать частоты, на которых будет располагаться ФЗЗ рассматриваемой структуры. Следовательно, возможно и обратное – задавая частоту, на которой необходимо расположение ФЗЗ, можно определить геометрические характеристики фотонного кристалла (диаметр и расстояние между центрами стержней фотонного кристалла).

Важно отметить, что данные преобразования будут выполняться только в том случае, если показатель преломления не изменяется (или изменяется в пределах нескольких процентов) в пределах рассматриваемого диапазона, как в случае использования тефлона.

На рис. 9 представлены зависимости нормированного потока мощности излучения исследуемого образца, изготовленного из различных материалов (см. таблицу).

Поскольку образец из GaAs обладает самой широкой запрещенной зоной, мы провели исследование распространения ТЕ-волн на диапазоне длин волн 0,8 – 2,65 мкм. На рис. 10 представлены результаты моделирования для образца из GaAs и тефлона.

## Выводы

Результаты, представленные на рис. 9 и 10, показывают, что при увеличении показателя преломления используемого материала ФЗЗ смещается в область длинных волн, при этом увеличивается ширина ФЗЗ, а также уменьшается глубина проникновения ТЕ-волн в фотонный кристалл. Эти особенности особенно проявляются в случае использования GaAs, показатель преломления которого более чем в 1,5 – 2 раза больше остальных материалов ( $n=3,4$ ).

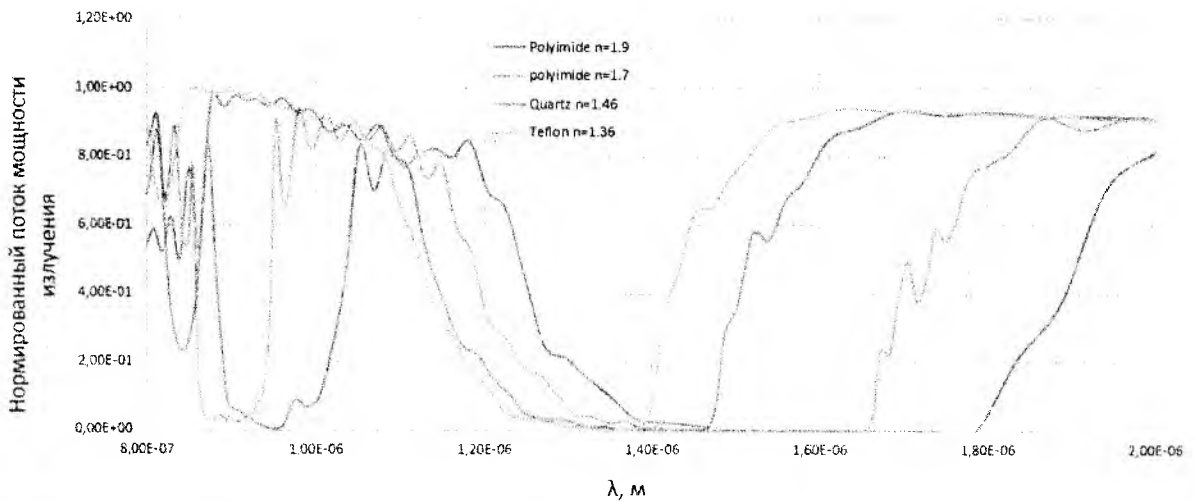


Рис. 9. Зависимости нормированного потока мощности излучения от длины волны для материалов, представленных в таблице

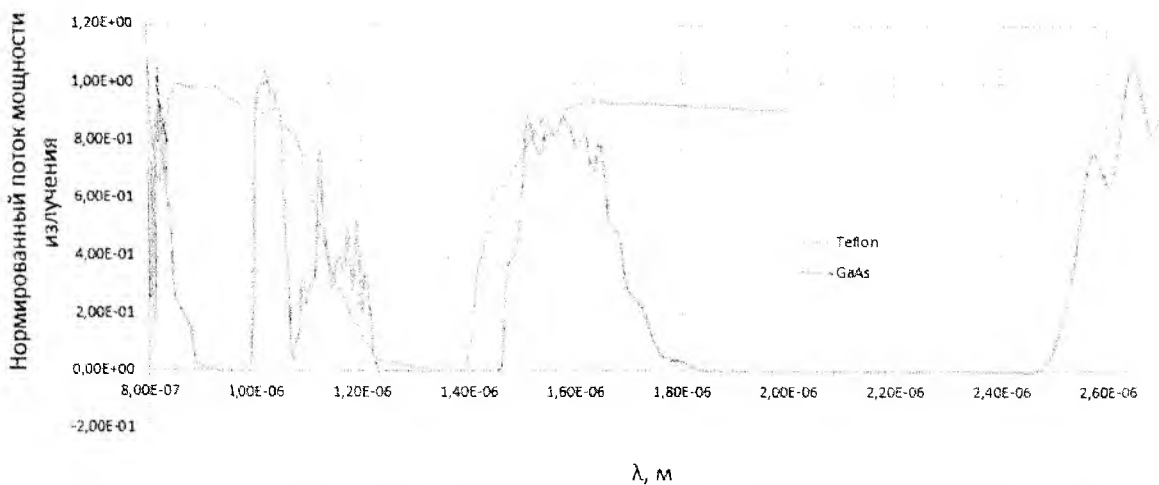


Рис. 10. Зависимости нормированного потока мощности излучения от длины волны для образцов из тефлона и GaAs

Отметим также, что исследуемые образцы, изготовленные из полиимидов, имеют еще одну ФЗЗ в области более коротких волн (900 – 950 нм), как видно из рис. 10. В образце, изготовленном из GaAs (рис. 10) кроме основной ФЗЗ наблюдаются еще две более узкие запрещенные зоны в области длин волн  $\lambda=1,25 - 1,45$  мкм и  $\lambda=0,9 - 1$  мкм.

Представленные выше результаты также показывают, что фотонный кристалл, изготовленный из арсенида галлия, обладает наилучшими характеристиками среди рассмотренных материалов, а именно: самой широкой запрещенной зоной (см. рис. 10), а также наименьшей глубиной проникновения излучения в фотонный кристалл.

**Список литературы:** 1. French, H. Optical properties of materials for concentrator photovoltaic systems / H. French, M. Rodríguez-parada, K. Yang, A. Derryberry, F. Lemon, J. Brown, R. Haeger, Samuels, C. Romano, E. Richardson // Journal of Microlithography, microfabrication and Microsystems. – 2009. – 2(3). – P.36-49. 2. French, H. Imaging of 32-nm 1:1 lines and spaces using 193-nm immersion interference lithography with second-generation immersion fluids to achieve a numerical aperture of 1.5 and a k1 of 0.25 [Текст] / H. French, Sewell, K. Yang, S. Peng, D. Mccafferty, W. Qiu, C. Wheland, F. Lemon, I. Markova, K. Crawford // Journal of Microlithography, microfabrication and Microsystems, topical issue on hyper-na imaging. – 2005. – 4(3). 3. Filipenko, A. I. Investigation of the 2-D Photonic Crystal Filter / A. I. Filipenko, A. N. Donskov // International Conference on Advanced Optoelectronics and Lasers (CAOL 2013). – 2013. – P. 58-59.

Харьковский национальный  
университет радиоэлектроники

Поступила в редколлегию 02.04.2017

## МНОГОКОМПОНЕНТНЫЕ ПОЛУПРОВОДНИКОВЫЕ СТРУКТУРЫ В КОНСТРУКЦИЯХ СОЛНЕЧНЫХ ЭЛЕМЕНТОВ

### Введение

В связи с увеличением потребления энергии во всем мире запасы ископаемого топлива быстро истощаются, в то время как процессы их естественного пополнения требуют неизмеримо более длительного времени. Поэтому сейчас все более пристальное внимание уделяется солнечной энергии – экологически чистому и практически неистощимому энергетическому ресурсу человечества.

В статье рассматриваются солнечные батареи – наиболее перспективный поставщик солнечной энергии, поскольку они преобразуют солнечный свет непосредственно в электричество с высоким коэффициентом преобразования, создают почти постоянную мощность при низких эксплуатационных расходах и практически не загрязняют окружающую среду. В то же время один из основных недостатков солнечных элементов – экономическая невыгодность использования их в больших масштабах. Данный недостаток связан с несовершенством конструкции этих приборов. Одним из путей его преодоления является применение многокомпонентных полупроводниковых систем.

Цель статьи – анализ перспектив использования неоднородных полупроводниковых структур в устройствах преобразования солнечной энергии промышленного и бытового назначения.

### Теоретические сведения

Одной из общепринятых является следующая классификация преобразователей солнечной энергии:

1. Фотоэлектрические преобразователи (солнечные элементы, СЭ) – полупроводниковые устройства, прямо преобразующие солнечную энергию в электричество.
2. Гелиоэлектростанции (ГЕЭС) – солнечные установки, использующие энергию высококонцентрированного солнечного излучения для приведения в действие тепловых и других машин (паровой, газотурбинной, термоэлектрической и т.п.).
3. Солнечные коллекторы (СК) – солнечные нагревательные низкотемпературные установки.
4. Органические батареи – устройства преобразующие солнечные лучи в электричество с помощью генетически модифицированных клеток, напечатанных на тонком пластике с проводником.

Кремниевые солнечные элементы с *p-n* переходом служат эталонными приборами для всех солнечных батарей. На рис. 1 схематически представлен типичный солнечный элемент, который состоит из мелкого *p-n* перехода, созданного у поверхности лицевого омического полоскового контакта, тылового омического сплошного контакта и просветляющего покрытия на лицевой поверхности. Идеализированная схема замещения солнечного элемента представлена на рис. 2.

Параллельно переходу введен источник постоянного тока  $I_L$ , описывающий возбуждение неравновесных носителей солнечным излучением, при этом  $I_L$  – ток насыщения диода;  $R_L$  – нагрузочное сопротивление. Данная цепь построена из предположения, что солнечный элемент имеет идеальную вольтамперную характеристику, определяемую выражением

$$I = I_s \cdot \left( e^{q \cdot V / k \cdot T} - 1 \right) - I_L. \quad (1)$$

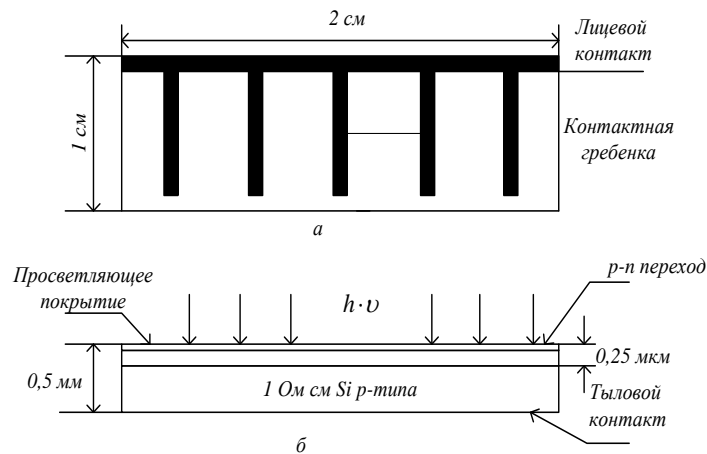


Рис. 1. Схематическое изображение кремниевого солнечного элемента с  $p-n$  переходом ( $a$  – вид сверху,  $b$  – вид сбоку)

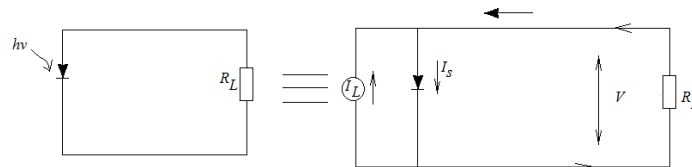


Рис. 2. Идеализированная эквивалентная схема солнечного элемента

В формуле (1):

$$J_S = \frac{I_S}{A} = q \cdot N_e \cdot N_v \cdot \left( \frac{1}{N_A} \cdot \sqrt{\frac{D_n}{\tau_n}} + \frac{1}{N_D} \cdot \sqrt{\frac{D_p}{\tau_p}} \right) \cdot e^{\frac{-E_g}{k \cdot T}}, \quad (2)$$

где  $A$  – площадь прибора. Типовые значения входящих в (1) и (2) величин:  $I_L=100$  мА,  $I_S=1$  мА,  $A=4$  см<sup>2</sup>,  $T=300$  К.

График ВАХ, определяемый выражением (1), представлен на рис. 3,  $a$ . Поскольку ВАХ проходит через четвертый квадрант, то это означает, что прибор служит источником энергии. Чаще всего ВАХ изображают, как показано на рис. 3,  $b$ .

Для реальных солнечных элементов в эквивалентную схему включается последовательное сопротивление, обусловленное омическим падением напряжения на лицевом контакте, и шунтирующее параллельное сопротивление, обусловленное токами утечки [1].

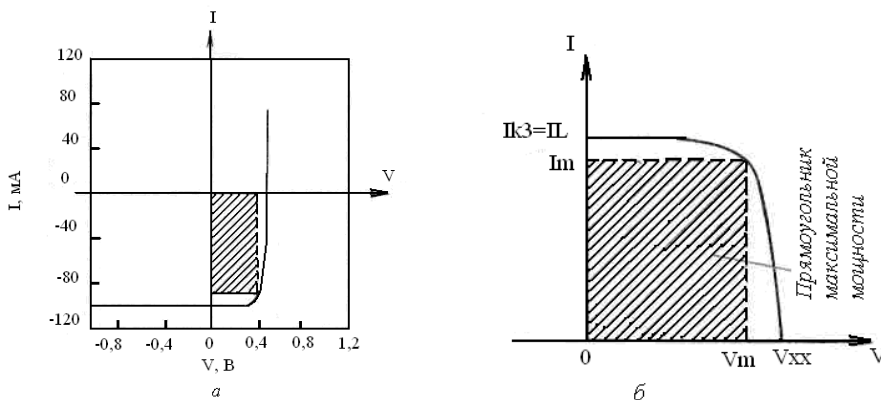


Рис. 3. Вольтамперная характеристика освещенного солнечного элемента

Для эффективной работы солнечных элементов необходимо соблюдение ряда условий:

- оптический коэффициент поглощения активного слоя полупроводника должен быть достаточно большим, чтобы обеспечить поглощение существенной части энергии солнечного света в пределах толщины слоя;
- генерируемые при освещении электроны и дырки должны эффективно собираться на контактных электродах с обеих сторон активного слоя;
- солнечный элемент должен обладать значительной высотой барьера в полупроводниковом переходе;
- полное сопротивление, включенное последовательно с солнечным элементом (исключая сопротивление нагрузки), должно быть малым для того, чтобы уменьшить потери мощности на выделение тепла в процессе работы;
- структура тонкой пленки должна быть однородной по всей активной области солнечного элемента, чтобы исключить закорачивание и влияние шунтирующих сопротивлений на характеристики элемента.

Основное внимание в производстве структур, удовлетворяющих данным требованиям, уделяется таким материалам, как сплавы на основе аморфного кремния ( $\alpha$ -Si:H), арсенид галлия и поликристаллические полупроводники [2]. Один из наиболее перспективных материалов для создания высокоэффективных солнечных батарей – арсенид галлия. Это объясняется такими его особенностями, как:

- почти идеальная для однопереходных солнечных элементов ширина запрещенной зоны 1,43 эВ;
- повышенная способность к поглощению солнечного излучения;
- высокая радиационная стойкость и высокая эффективность;
- характеристики сплавов GaAs с алюминием, мышьяком, фосфором или индием дополняют характеристики GaAs, что расширяет возможности при проектировании СЭ.

Главное достоинство арсенида галлия и сплавов на его основе – широкий диапазон возможностей для дизайна СЭ. Фотоэлемент на основе GaAs может состоять из нескольких слоев различного состава, что позволяет разработчику с большой точностью управлять генерацией носителей заряда. Для удешевления производства предлагается формировать СЭ на более дешевых подложках; выращивать слои GaAs на удаляемых подложках или подложках многократного использования [2].

### Основные конструкции солнечных элементов

*Солнечные элементы с барьерами вблизи тыловой поверхности (БТП)* имеют большее выходное напряжение, чем обычные элементы. Лицевая поверхность изготавливается обычным способом, но вблизи тыловой поверхности перед металлическим омическим контактом создается сильнолегированный полупроводниковый слой. На (рис. 4, а) представлена конструкция текстурированного элемента, лицевая поверхность которого покрыта пирамидами, которые создаются с помощью анизотропного травления поверхности. Даная конструкция позволяет свету, падающему на боковую поверхность одной из пирамид, отражаться на другую пирамиду, что приводит к уменьшению оптических потерь. Если же нанести дополнительное просветляющее покрытие, то потери на отражение снизятся на несколько процентов.

*Солнечные элементы с использованием анизотропного травления поверхности.* Этот элемент состоит из ряда отдельных  $p^+ - p - n^+$  диодов, которые соединены последовательно (рис. 5). Трапецидальная форма отдельных диодов получается за счет анизотропного травления поверхности.

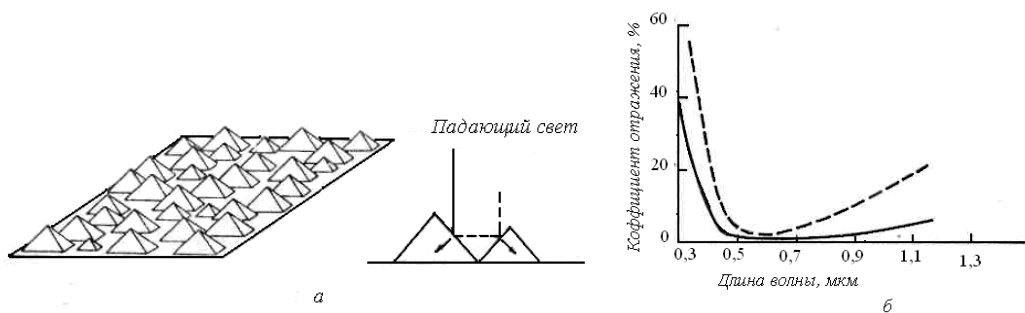


Рис. 4. *а* – текстурированный элемент с пирамидальной поверхностью, *б* – зависимость от длины волны коэффициента отражения солнечного элемента с плоской поверхностью и просветляющим покрытием (штриховая линия) и текстурированного солнечного элемента с просветляющим покрытием (сплошная кривая)

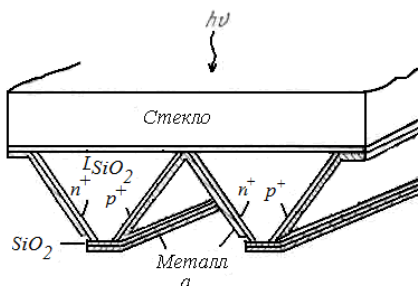


Рис. 5. Многопереходной солнечный элемент на V-канавках

Также существуют солнечные элементы со спаренными переходами, в которых сочетаются концепции элемента с БТП и текстурированного элемента. В этой конструкции нет тени от металла и облегчаются проблемы межсоединений благодаря тому, что  $p^+$  и  $n^+$  контакты создаются на тыловой поверхности. Прибор работает как биполярный транзистор с изолированным  $n^+$  эмиттером на лицевой поверхности (рис.6, б). Электроны, генерируемые светом в эмиттере или в базе, собираются  $n^+$  коллектором, подобно тому, как это имеет место в транзисторе.

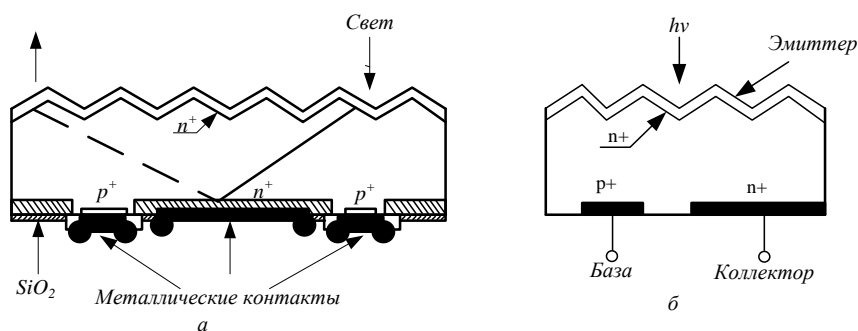


Рис. 6. Поперечное сечение солнечного элемента со спаренными переходами

В солнечных элементах с вертикальными переходами поверхность переходов и металлические поверхности расположены перпендикулярно поверхности элемента (рис. 7).

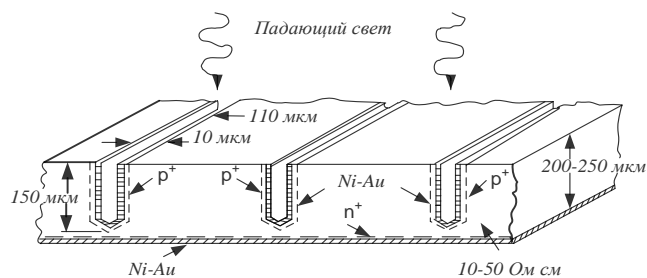


Рис. 7. Солнечный элемент со спаренными переходами

Диффузионные и металлические контакты расположены в глубоко вытравленных канавках, перпендикулярных поверхности и созданных благодаря анизотропному травлению поверхности. Расстояние между канавками 140 мкм, что равно диффузионной длине неосновных носителей. В этом случае диффузия с лицевой поверхности не проводится, а доля

затемненной поверхности благодаря небольшой ширине канавок (10 мкм) не превышает 7%. Ток протекает непосредственно через диффузионные  $p^+$ -области и металлический слой, расположенный на стенках канавок, и вводится через контактные полосы, лежащие на боковой поверхности элемента. Эти полосы соединяют все элементы параллельно. Практически все из выше названных конструкций используются в условиях высокой интенсивности излучения [1]. Солнечные элементы с гетеропереходами имеют ряд преимуществ:

- спектральный отклик увеличивается в коротковолновом диапазоне при условии, что энергия достаточно велика и фотоны с высокой энергией поглощаются в обедненном слое второго полупроводника;
- последовательное сопротивление понижается при условии, что первый полупроводник можно сильно легировать, не ухудшая при этом условия прохождения света через него;
- высокая радиационная стойкость, если первый слой полупроводника достаточно толстый и полупроводник имеет широкую запрещенную зону.

Одним из примеров солнечного элемента с гетеропереходом можно назвать гетеропереход проводящее стекло – полупроводник.

На рис. 8 представлена диаграмма энергетических зон освещенного солнечного элемента с барьером Шоттки.

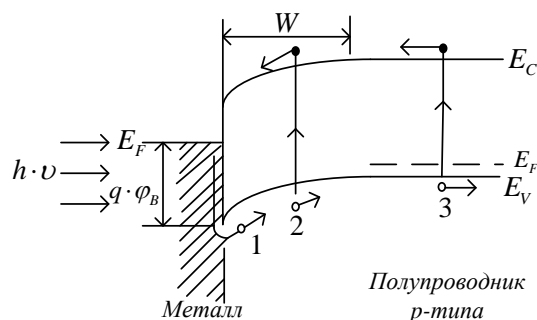


Рис. 8. Диаграмма энергетических зон освещенного солнечного элемента с барьером Шоттки

Слой металла достаточно тонкий, чтобы основная доля света достигала полупроводника. Выделяют три компонента фототока. Один из компонентов обусловлен поглощением в металле фотонов с энергией  $h \cdot \nu \rightarrow q \cdot \phi_s$  ( $q \cdot \phi_s$  – высота барьера), что вызывает возбуждение дырок через барьер в полупроводник (этот компонент обозначен 1 на (рис. 8)). Второй компонент – это падающий на полупроводник коротковолновый свет, который поглощается в основном в обедненном слое (обозначен цифрой 2). Третий компонент – длинноволновый свет, который поглощается в нейтральном объеме и создает электронно-дырочные пары,

затем электроны диффундируют к краю обедненного слоя, где происходит их коллектирование (фототок 3).

Солнечные элементы на барьерах Шоттки имеют свои преимущества:

- изготавливаются такие элементы при низких температурах, так как не требуется диффузия;
- данная технология применяется при создании поликристаллических и тонкопленочных солнечных элементов;
- высокая радиационная стойкость, поскольку вблизи их поверхности существует сильное электрическое поле;
- большой выходной ток и спектральный отклик, что объясняется непосредственным примыканием обедненного слоя к поверхности полупроводника, вследствие чего ослабляется негативное влияние малых времен жизни и высокой скорости поверхностной рекомбинации.

В солнечных элементах на МДП-структурах между металлом и полупроводниковой подложкой создается тонкий изолирующий слой. Преимущество таких элементов связано с тем, что в них имеется сильное электрическое поле вблизи поверхности полупроводника, которое направлено так, что помогает коллектированию носителей, создаваемых коротковолновым светом; кроме того, в активной области таких элементов нет кристаллических дефектов, возникающих при диффузии примесей и присущих солнечным элементам с диффузионными  $p-n$  переходами.

На рис. 9 представлена структура, в которой используется гребенка в виде МДП-структуры с толстым металлом.

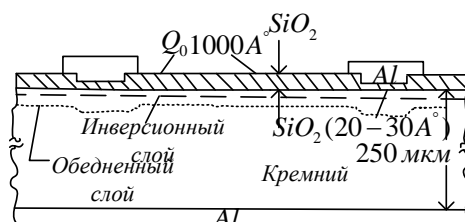


Рис. 9. Поперечное сечение солнечного элемента с гребенчатой МДП-структурой

Между отдельными полосками полупроводник покрыт прозрачным диэлектрическим слоем, который служит и прозрачным диэлектрическим слоем и просветляющим покрытием. Поскольку при создании таких структур не надо проводить диффузию, а выращивание окисла возможно и при низких температурах, предполагается, что именно такие структуры, изготавливаемые на поликристаллических и аморфных подложках, окажутся экономически наиболее выгодными источниками энергии.

В тонкопленочных солнечных элементах активными полупроводниковыми слоями являются поликристаллические или неупорядоченные пленки, которые наносятся или выращиваются на электрически активных или пассивных подложках. Тонкие пленки наносятся с помощью газовой эпитаксии, плазменного распыления и осаждения. Если толщина слоя полупроводника превышает обратный коэффициент поглощения, большая часть света будет поглощаться в полупроводнике; если диффузионная длина превышает толщину пленки, большая часть генерируемых светом носителей может быть коллектирована. К основному достоинству стоит отнести низкую стоимость, поскольку технология их изготовления дешевая и используются сравнительно дешевые материалы. К недостаткам относится низкий КПД (частично обусловлен влиянием границ зерен и частично низким качеством полупроводникового материала, выращиваемого на различных подложках) и постепенная деградация характеристик, что связано с химическими реакциями, протекающими между полупроводником и окружающей атмосферой [1].

### Перспективные технологии изготовления солнечных элементов

Особые надежды возлагаются на аморфные гетероструктуры, на основе которых возможна реализация фотоэлектрических устройств, в частности элементов солнечной

энергетики. Неоспоримыми преимуществами аморфных полупроводников являются простота их получения и более дешевая технология в совокупности с более широкой материальной базой и большими площадями нанесения. Особое место среди аморфных материалов занимает аморфный гидрогенизированный кремний и его соединения, прежде всего благодаря более широкому применению его в полупроводниковой оптоэлектронике и солнечной энергетике. Аморфный кремний по ряду параметров превосходит монокристаллический и является наиболее перспективным для солнечной энергетике. Основное достоинство данного материала – оптическое поглощение аморфного кремния в 20 раз выше, чем кристаллического. Поэтому для существенного поглощения видимого света достаточно пленки a-Si:H толщиной 0,5 – 1,0 мкм вместо дорогостоящих кремниевых 300-мкм подложек. Кроме того, благодаря существующим технологиям получения тонких пленок аморфного кремния большой площади не требуется операции резки, шлифовки и полировки, необходимых для солнечных элементов на основе монокристаллического кремния. По сравнению с поликристаллическими кремниевыми элементами изделия на основе a-Si:H производят при более низких температурах (300° С): можно использовать дешевые стеклянные подложки, что сократит расход кремния в 20 раз [4, 5].

Для оптимизации структуры фотопреобразователей необходимо создание строгой модели, которая адекватно учитывает основные особенности электрофизических процессов в сложных многослойных гетероструктурах на основе сплавов неупорядоченного и кристаллического кремния. Выходными данными для такой модели должны служить экспериментально определенные параметры слоев. Кроме того, модель должна позволять решать обратные задания с целью экстракции электрофизических параметров элементов структуры фотопреобразователя из его экспериментальных характеристик.

### **Выводы**

Таким образом, современная технология фотоэлектрического преобразования световой энергии (фотовольтаика) характеризуется стремительным изменением соотношения объемов производимой энергии в пользу батарей на основе некристаллических тонкопленочных фотопреобразователей, а также фотопреобразователей на основе гетеропереходу a-Si/c-Si. На данный момент рекордное значение эффективности тонкопленочных фотопреобразователей порядка 15,2 %, а гетероструктурных a-Si/c-Si – 21 %.

Дальнейшее развитие гелиоэнергетики связано со снижением удельного ватта электроэнергии. Существуют следующие возможности для такого удешевления:

- повышение эффективности преобразования энергии за счет оптимизации конструкции, оптических и кинетических свойств материала контактных и активных слоев (в том числе расширение спектрального диапазона, снижения оптических потерь в контактных слоях, повышение эффективности сбора неравновесных носителей заряда);
- повышение стабильности электрофизических свойств активных слоев;
- совершенствование технологии изготовления батарей, которое должно быть связано в основном со снижением времени формирования структуры преобразователей за счет снижения количества технологических операций.

**Список литературы:** 1. *Зи, С.* Физика полупроводниковых приборов. – М. : Мир, 1984. – 449с.  
2. *Мейтин, М.* Фотовольтаика: материалы, технологии, перспективы // *Электроника – НТ.* – 2000. – № 3. – С.13-23. 3. *Наумов, А.В.* Еще раз о развитии солнечной энергетике и рынке кремниевого сырья в 2007 – 2010 гг. // *Технология и конструирование в электронной аппаратуре.* – 2007. – № 4. – С. 8-12.  
4. *Глиберман, А.Я., Зайцева, А.К.* Кремниевые солнечные батареи. – М. ; Л. : Госэнергоиздат, 1961.  
5. *Luque, A., Hegedus, S.* Handbook of Photovoltaic Science and Engineering, 2003.

## THE APPLICATION OF MULTILATERATION TECHNOLOGY IN AIR TRAFFIC CONTROL

### 1. Introduction

The main task of the air traffic control system (ATCS) is to ensure that the air traffic safe and in order and increase the flight time and space utilization of flight routes and airports by managing and controlling the entire process of aircrafts from take-off to landing. The control area of both military and civil aviation aircraft activities can be divided into 3 parts: area control (flight routes), approach control (terminal area) and airport control (airport scene).

Until now, air traffic control two coordinate radar systems are the main technique of military civil aviation surveillance aircraft, whose surveillance range is 250 nautical miles (approximately 450km). However, airport control has to use the way of visual inspection to monitor aircrafts which are taking off, landing or moving in the airport duo to the lack of modern radio means for effective surveillance. It may cause that the pressure on air traffic controllers will be enormous when the aircraft flow is large. Therefore, the world civil aviation industry has began seeking new technological solutions science 10 years ago, such as laying high precision sensors around the airport to report the current location and route of each aircraft. At present, some experimental passive surveillance systems have been tested in several important airports in Europe and the United States. The best performance of them is to allow taking-off with less than 70m of visibility.

Considering the advantage of the multilateration, this paper introduces the multilateration into the ATC application to satisfy the mission requirements of ATC. And the key problems in engineering implementation have been analyzed and solved.

### 2. Multilateration Technology

Multilateration uses multiple receivers to receive the signal of the target radiation source simultaneously. Because the receiver can not confirm the emission time of the emitter, the method of measuring the time difference of signals arriving at different receivers is adopted. The distance difference is calculated according to the time difference, and the target position is obtained by geometry method. The working principle as shown in Figure 1.

The distance between the radiation source P and the reconnaissance station A and B is  $R_A$  and  $R_B$ , respectively. The time from which the electromagnetic wave emitted from the target P arrives at the A and B stations is  $T_A$  ( $T_A = R_A/c$ ) and  $T_B$  ( $T_B = R_B/c$ ). If the measured time difference is  $T_{AB} = T_B - T_A = (R_B - R_A)/c$ , then we can confirm the point P on the hyperbola which focuses on A and B. The distance from one point of the hyperbola to the A station and the B station is equal to  $R_B - R_A$ . Similarly, if measure the time difference between the electromagnetic wave of the target emitted at the C station and the A station is  $T_{AC} = T_C - T_A = (R_C - R_A)/c$ , we can determine another hyperbola. And the intersection point of the two hyperbolas is the estimated value of the P location of the emitter. By using the arrival azimuth information of the radio wave to remove another false mirror point which is symmetrical to the baseline.

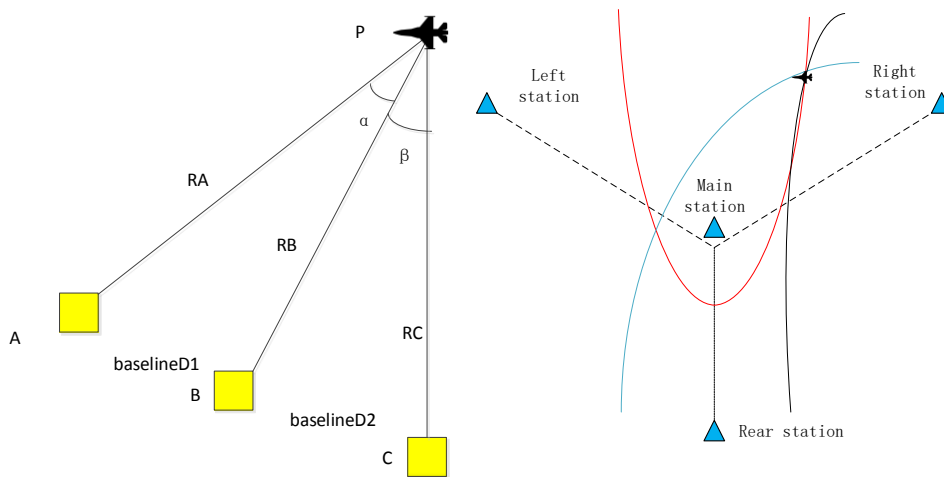


Figure 1. TDOA location principle (Hyperbola fix)

The three station TDOA location will be the position on the positioning plane, and this location can be approximately considered the horizontal position when the target distance is far away. In order to obtain the high value, the 4 station TDOA location should be adopted. The measurement equations are

$$\begin{cases} \sqrt{(x-x_1)^2 + (y-y_1)^2 + (z-z_1)^2} - \sqrt{x^2 + y^2 + z^2} = c \times \delta t_1 \\ \sqrt{(x-x_2)^2 + (y-y_2)^2 + (z-z_2)^2} - \sqrt{x^2 + y^2 + z^2} = c \times \delta t_2 \\ \sqrt{(x-x_3)^2 + (y-y_3)^2 + (z-z_3)^2} - \sqrt{x^2 + y^2 + z^2} = c \times \delta t_3 \end{cases}$$

By solving the equations, the three-dimensional position solution of the target can be obtained.

### 3. The features of multilateration technology used in air traffic control surveillance system

Multilateration technology is a new ATC surveillance technology. The position of an aircraft or other moving target is determined by multipoint passive sensor receive mode. Because the system is completely compatible with the SSR radar and ADS-B downlink data transmission link, it can receive and decode the SSR code and S model plane address, which has the target identification capability and high-precision positioning capabilities. The biggest feature of this technology is that it fully utilizes the onboard standard transponder, and does not need to install other airborne navigation equipment to complete the positioning monitoring. It is compatible with ADS-B technology, with high data update rate (1 times per second, two radars at least 4 seconds 1 times), and has lower system cost (compared with the existing SSR radar system, its investment cost is less than 1/3). It has high positioning accuracy, wide area positioning accuracy within 50 meters in the air, the ground positioning accuracy within 10 meters, with the ability to target identification. The interference to other systems is small, and the receiving station antenna is a simple omnidirectional antenna without rotating mechanism, which is characterized by small size, flexible site configuration, and good adaptability of system monitoring coverage. Therefore, this technology has a good application prospect in the air traffic surveillance field.

## 4. Key Technologies

### 4.1. The design scheme of the system

System design uses at least 4 low-cost sensors. According to the system characteristics, the system design can be divided into signal forwarding based centralized and time synchronization based distributed schemes, as shown in Figure 2 and 3.

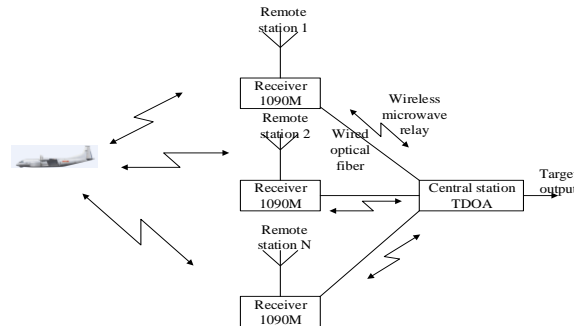


Figure 2. Signal forwarding based centralized schemes

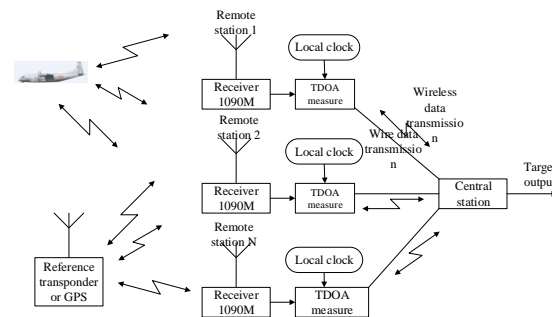


Figure 3. Time synchronization based distributed schemes

According to the system characteristics of the signal forwarding system:

- 1) Communication between auxiliary station and central station;
- 2) The center station measures the time difference between the main and secondary stations, and extracts the symbols to complete the identification function;
- 3) The system design is simple and the cost is low;
- 4) The time difference measurement needs many pulses, and the measurement accuracy is potentially high.

Shortcomings:

- 1) The relative relation between auxiliary station and central station is fixed and the interchangeability is poor;
- 2) The influence of modulation and demodulation on the rising edge of each station should be strictly controlled.

The characteristics of the time synchronization systems:

- 1) Each station can measure arrival time precisely;
- 2) Auxiliary stations are interchangeable;
- 3) Data transmission between station and station is flexible through data exchange, without distance differences. Point to multipoint transmission can be used;

Shortcomings:

- 1) The number of targets in instantaneous processing is limited by the data rate;

2) The time difference accuracy depends on the time synchronization accuracy.

#### 4.2. Error analysis of distribution station and location

According to the distribution of terrain and buildings in a domestic airport, the detection area is divided, and the location of IFF receiving and processing subsystem is planned, as shown in figure 4.

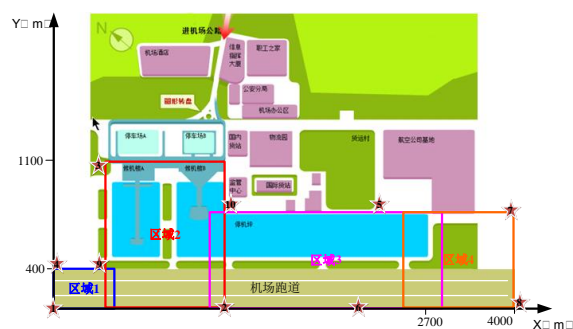


Figure 4 Detection area division

According to the above classification and site distribution, multi point positioning algorithm is applied, according to the  $N(0, 30)$  of the Gauss distribution simulation random timing error, repeated operation 30 times, with the mean positioning error as the final positioning error, the simulation results are shown in figure 5.

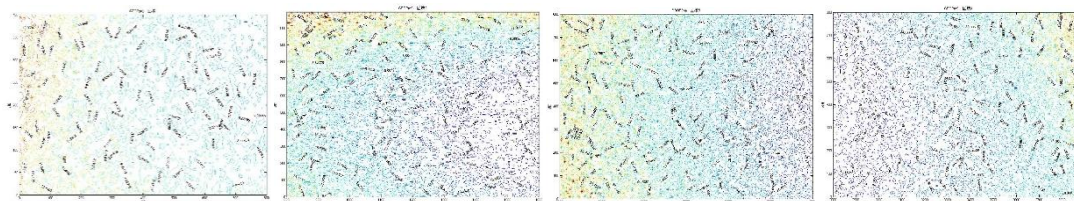


Figure 5 System simulation results

The simulation results are as follows:

Zone 1: positioning error <12 m.

Zone 2: positioning error <15 m.

Zone 3: positioning error <27 m.

Zone 4: positioning error <30 m.

#### 4.3. Anti-multipath interference method

Multipath propagation is due to various objects around the radiation source and receiver, including buildings, vehicles, pedestrians, trees and even the reflection of radio wave refraction and diffraction caused by energy disperse in space, and through multiple paths to the plurality of correlation signals into the receiver. The multipath interference caused by buildings, vehicles and ground surfaces in airport scenes is especially serious. According to the actual measurements of multipath interference at the airport, there are four main features that can be used:

- 1) Because the path difference caused by the pulse along the stray pulse, will not damage the pulse, due to the IFF response signal pulse interval is smaller, the conventional 1.45us, pulse width 0.45us, S encoding mode interval 1us, pulse width 0.5us. Therefore, the trailing edge of the front pulse has not reached the bottom, and the front edge of the latter pulse has been dashed;

- 2) The spurious pulse amplitude generated by multipath is not stronger than the main signal, and the signal amplitude will be less than 500mv (the following floating threshold is below the signal top 300mV, which can satisfy the suppression of multipath and obtain better quality TTL pulse);
- 3) The pulse width of multipath is not fixed pulse width, the pulse width is generally small, and the interval is rather chaotic;

For 1 symbol strings, the effects of multipath on each pulse are approximately the same, including amplitude, width, etc.

According to the characteristics of multipath interference signal, we can consider the following processing methods:

- 1) Considering the floating threshold mode and pulse width discrimination: floating threshold can ensure the accuracy of measurement of pulse width and multipath inhibited. When unable to suppress multipath trigger pulses, the pulse width of the judgment can restrain some spurious pulse. Waveform and channel anti multi path effect diagram shown in Figure 6, 7;

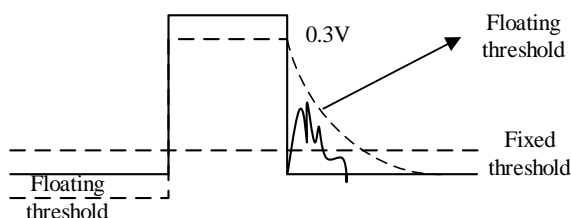


Figure 6. The waveform sketch

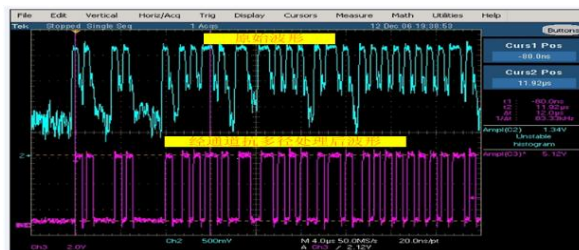


Figure 7. The actual effect of channel anti multipath interference

- 2) The channel gain is controlled according to the amplitude characteristic of the signal amplitude and multipath, so as to suppress the spurious pulse produced by multipath as much as possible;
- 3) When there is a low amplitude pulse followed the strong pulse, the influence brought by floating threshold may lead to pulse loss, so the floating threshold discharge delay time should be adjusted according to the actual situation of signal to find a balance point;

#### 4.4. High precision time difference extraction method

According to the analysis of the station and its positioning error, the time difference measurement accuracy must be better than the 10ns index in order to meet the requirements of the positioning accuracy of the air traffic surveillance system.

- 1) The influence on error of TDOA measurement accuracy

For the measurement of the pulse rising edge arrival time, we have implemented a low speed clock phase shift method. The so-called phase refers to two channels signals with the same

frequency, in one of which is a reference signal, the other channel signals moves forward or backward relative to the reference signal to form a phase difference. Digital phase delay method is usually used to delay to determine the length of the phase difference between the two digital signals. As shown in Figure 8:

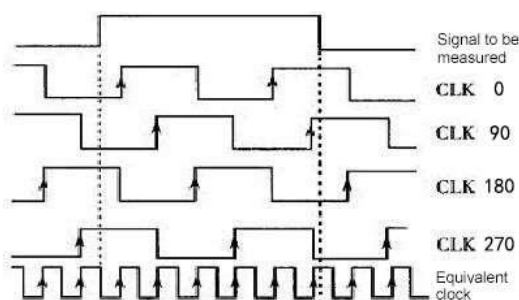


Figure 8. Measurement principle based on digital phase-shifting technology

As we can see, this method is equivalent to the fourfold frequency multiplication of the original actual count of the clock frequency, the clock frequency of  $4f$  the measured signal counting measurement, so as to improve the measurement accuracy to the original 4 times. At the same time, the method ensures the maximum working frequency of the circuit is  $f$ , the clock frequency is increased to avoid a series of problems brought.

## 2) Influence of rising edge stability on error

According to a regional surveillance area is  $10 * 10\text{km}$ , we simulate the minimum and maximum power of each point of the plane after reaching the sensor response signal path loss, the simulation results are shown in Figure 9, one of the biggest power difference is 32dB.

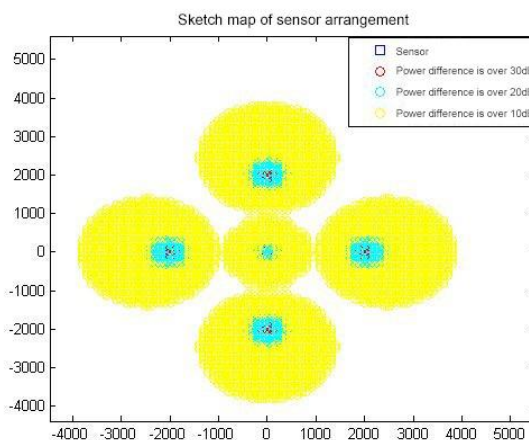


Figure 9. The power difference distribution of the sensor deployment

To verify the influence of the signal power and the rising edge of the video pulse on the stability of the comparison shaping pulse (TTL level), the following tests are carried out.

On the oscilloscope, the pulse modulated by the pulse source is synchronized, test the delay between a wide pulse and a modulating pulse; test the change in the delay time  $\Delta t$  of the rising edge of the video pulse at different power levels. The test block diagram is shown in figure 10:

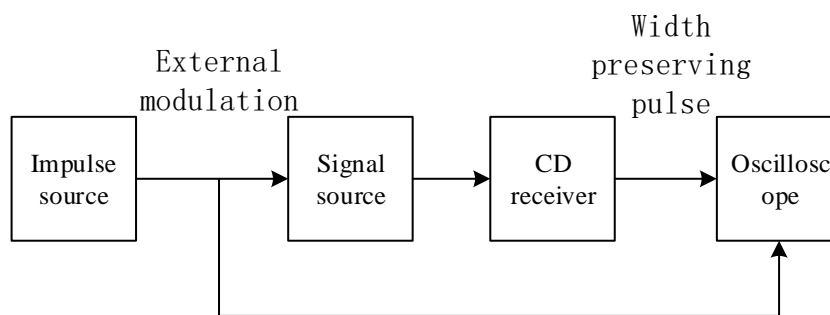


Figure 10. The test block diagram

Test method 1:

Input signal power: -40dBm to 0dBm, 10dB step

By filtering (reducing video bandwidth), the logarithmic video rise time is 100ns to 160ns.

Test results are as follows

Signal power (dBm)	-40	-30	-20	-10	0
Time delay $\Delta t$ (ns)	156	177	183	185	166

Test method two:

Input signal power: -40dBm to 0dBm, 10dB step

Remove filter capacitor, logarithmic video rise time is 60ns ~ 120ns

Test results are as follows

Signal power (dBm)	-40	-30	-20	-10	0
Time delay $\Delta t$ (ns)	162	158	154	152	146

According to the above test results, rising edge stability in 40dB dynamic range in the narrowband filter case, the error is 29ns. In the broadband detection, the error is 16ns. Therefore, SDLVA is considered in the design of broadband detection, if the pulse arrival time is not corrected according to the amplitude information, only the rising edge of the stability degree is an error on the TDOA error indicators have exceeded the system, the location error cannot meet the requirements of the system.

## 5. System test status

At the end of 2012, the system realized monitoring and positioning of the aircraft takeoff and landing, docking, taxiing on the aircrafts ground and bridges parked nearby targets in a domestic airport, the test results are shown in Figure 11.

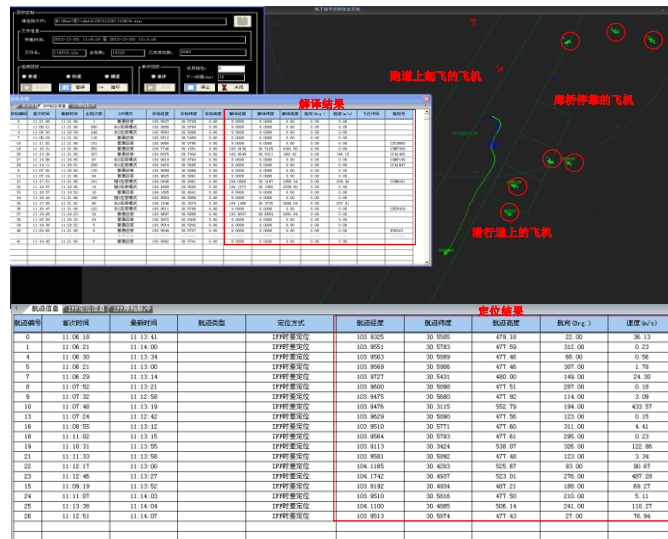


Figure 11. System scene monitoring

It can be seen from the test result that the system can recognize the multi-mode response signals of civil aviation, including conventional A/C mode response signal, long and short S mode response signal and so on. The system uses multilateration technology to give the target latitude and longitude, heading, speed and other information. At the same time, the system also has a certain capacity for identification of civil aviation targets. It can be compatible with the ADS-B downlink data link, and can receive and interpret the S mode response signal.

## 6. Performance comparison between system and ADS-B device monitoring

In order to detect the monitoring and positioning ability of the system, the real-time monitoring comparison between the system and the ADS-B device is carried out in the test process, as shown in figure 12.

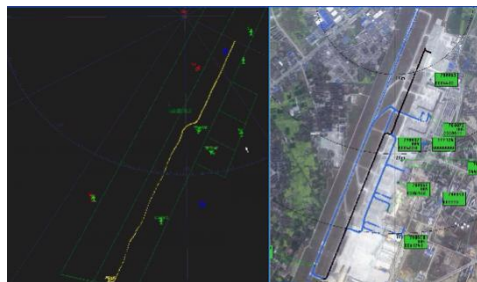


Figure 12. Performance comparison between system and ADS-B monitoring

By comparison, we can see that:

1. The aircraft on the taxiway of the airport, the system has a better ability to target monitoring. Through positioning accuracy analysis, the relative positioning error is less than 1%R, the normal direction which plus or minus 60 degrees in the alignment of the main station is equivalent to ADSB. The distance error is within the range of 20 meters, as the angle increases closer to the baseline position, the error is greater.

The following is the result that the system and the ADSB device take the GPS positioning timestamp as the baseline, and compare the anchor point data at the same time, as shown in figure 13.

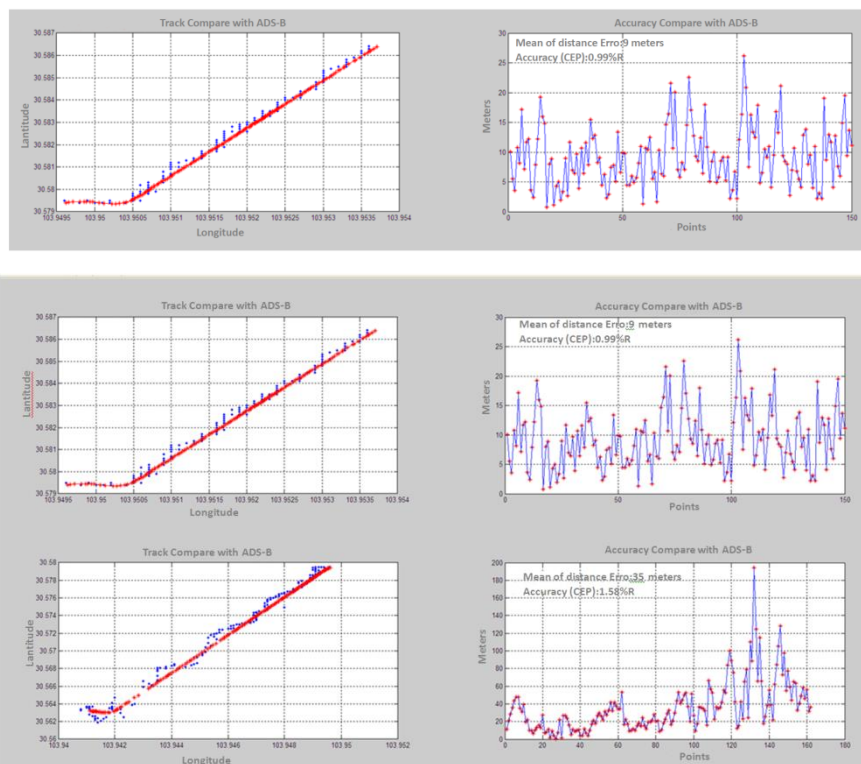


Figure 13. Target accuracy comparison

2. The aircraft taxiing or taking off at the airport ramp and runway, when responding in A/C mode, the system can achieve target tracking and detection, while the ADS-B device can not give the target effective location, as shown in figure 14.

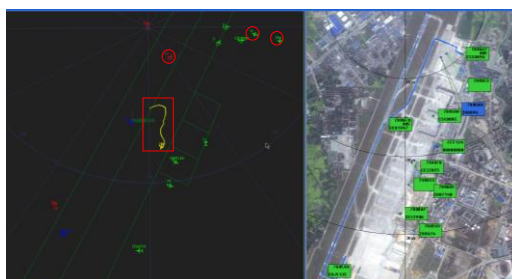


Figure 14. The system only receives the target of answering the A/C mode signal

3. For bridges parked aircraft, when no signal shielding, system can achieve effective positioning. But for the depths of bridges parked aircraft, the signal is blocked by ground object and can not meet the requirement of multi station TDOA location condition, the system can not give the target location, as shown in figure 15.

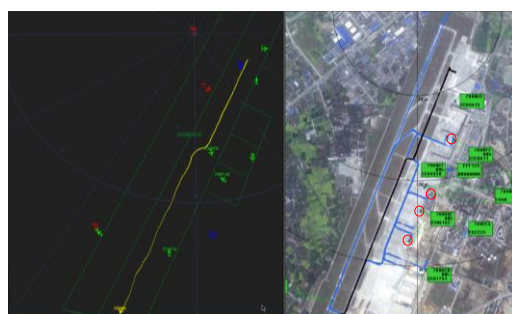


Figure 15. On the scene, the system can not effectively locate the target

## 7. Conclusion

Although the multilateration technology is mature, it suffers many problems when it is applied to ATC. This paper provides a detailed analysis of key technologies and solutions. Some of them have been verified in the concrete project. Test results show that the proposed method can monitor and locate aircrafts that are taking-off, landing, and gliding and other target near the boarding bridge. And the positioning accuracy and the effective range is equivalent to ADS-B.

**Reference:** 1. ZHANG Jun. Modern air traffic management [M]. Beijing: Beijing University of Aeronautics and Astronautics Press, 2005. 2. Miao Q, De-Wei W U, Mao Y Q. Application of Multiple Stations Passive Position Technology in Local Position Network[J]. Modern Radar, 2007. 3. Wang H, Zhong D, Zhou Y. Location Precision Analysis in the Time Difference of Arrival Location System Using Irregular Distribution [J]. Modern Electronics Technique, 2007. 4. Hu L Z. Passive locating [M]. National Defense Industry Press, 2004.

*Southwest China Research Institute of Electronic Equipment,  
Chengdu, P.R. of China,*

*Юго-Западный Китайский научно-исследовательский  
институт электронного оборудования, Чэнду, Р.Р.*

*Поступила в редколлегию 11.06.2017*

*А.Н. ОЛЕЙНИКОВ, канд. техн наук, А.В. БОРОДАВКА*

## ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ СРЕДСТВ АКУСТИЧЕСКОЙ РАЗВЕДКИ

### **Введение**

В настоящее время самым распространенным средством ведения акустической разведки (дистанционного несанкционированного съема акустической информации) являются узконаправленные микрофоны, выполненные в виде единичных акустических приемников или в виде микрофонных решеток (МР). К средствам дистанционного съема акустической информации можно отнести также лазерную систему акустической разведки, которая в данной статье не рассматривается [1 – 2].

Развитие и совершенствование узконаправленных микрофонов условно можно разделить на три этапа: «акусто-механический» этап, этап аналоговый обработки аудиосигналов и этап цифровой обработки аудиосигналов в средствах дистанционного съема информации [2].

Первые средства акустической разведки, представлявшие собой громоздкие акусто-механические системы, были разработаны в начале XX в. и применялись для обнаружения летательных аппаратов и определения положения артиллерийских батарей, уступив место средствам радиолокации перед Второй мировой войной [2].

Узконаправленные микрофоны с аналоговой обработкой аудиосигналов можно отнести ко второму этапу их развития. Микрофоны этой группы разделяют на: комбинированные, рефлекторные и групповые, включающие в себя линейную группу микрофонов, плоскую решетку микрофонов и трубчатые микрофоны [1 – 2].

Основные сравнительные характеристики и параметры этих узконаправленных микрофонов (УНМ) представлены в [1] и сведены в таблицу, в которой приведены формулы для расчета характеристик направленности  $R(\theta)$  микрофонов, значение их индекса направленности (Q) при одинаковых габаритных размерах акустических систем. Параметры УНМ сильно зависят от отношения их габаритных размеров к длине звуковой волны и, как правило, имеют невысокие значения пространственной избирательности на низких частотах. В области высоких частот наилучшей пространственной избирательностью обладает рефлекторный микрофон, который не имеет ограничения по максимально применимой рабочей частоте ( $F_{\max}$ ). На низкой частоте индекс направленности УНМ типа линейной группы микрофонов несколько превышает индекс направленности рефлекторного микрофона, но его значения невысоки (единицы дБ) [1].

В это же время на основе антенных решеток были разработаны первые аналоговые МР с простейшей обработкой электрических сигналов единичных микрофонов решетки [2].

### **Развитие и совершенствование узконаправленных микрофонов с цифровой обработкой сигналов (ЦОС)**

Третьим этапом развития и совершенствования узконаправленных микрофонов (начиная с 90-х годов XX в.) стало использование средств цифровой обработки аудиосигналов в микрофонных решетках [2].

С развитием ЦОС МР стали применяться для решения широкого круга задач, связанных с обработкой речевых сигналов: выделение речи целевого источника в шумах (повышение разборчивости); дистанционное распознавание речи (например, для голосового управления устройствами; определение и трассировка положения источников звука; системы автоматического распознавания речи и речевого управления; слуховые аппараты и др.

Сравнительные характеристики узконаправленных микрофонов (УНМ)

Тип узконаправленного микрофона (УНМ)	Формула для расчета характеристики направленности $R(\theta)$	1. Параметры УНМ 2. Значение индекса направленности $Q$	Обобщающая характеристика УНМ
Комбинированные микрофоны	$R(\theta) = 1 - C + C \times \cos(\theta)$ <p>где <math>C = \frac{E_{\text{зад}}}{(E_0 + E_{\text{зад}})}</math></p>	$C=1$ $Q=4,8$ дБ $C=0,75$ $Q=6$ дБ $C=0,63$ $Q=5,7$ дБ $C=0,5$ $Q=4,8$ дБ $C=0$ $Q=0$ дБ	Низкое значение пространственной избирательности: $Q_{\text{max}} = 6$ дБ
Трубчатые микрофоны	$R(\theta) = \frac{\sin\left(\frac{n \times \pi \times d}{\lambda} \times (1 - \cos(\theta))\right)}{n \times \sin\left(\frac{\pi \times d}{\lambda} \times (1 - \cos(\theta))\right)}$ <p><math>n</math> – число трубок,  <math>d</math> – расстояние приращения трубок,  <math>L</math> – длина наибольшей трубки</p>	при $L = 90$ см, $n = 33$ , $d = 2,8$ см.  $Q = 16$ дБ на частоте 4 кГц	При одинаковых габаритных размерах уступает линейной группе по всем параметрам; ограничение по $F_{\text{max}} \leq \frac{c}{2d}$
Линейная группа микрофонов	$R(\theta) = \frac{\sin\left(\frac{n \times \pi \times d}{\lambda} \times \sin(\theta)\right)}{n \times \sin\left(\frac{\pi \times d}{\lambda} \times \sin(\theta)\right)}$ <p><math>n</math> – число микрофонов,  <math>d</math> – расстояние между микрофонами,  <math>L</math> – общая длина МР</p>	при $L = 90$ см, $n = 21$ , $d = 4,3$ см  $Q = 25$ дБ на частоте 4 кГц	Индекс направленности $Q$ на высокой частоте ниже, чем у рефлекторного УНМ; ограничение по $F_{\text{max}} \leq 1,5 \frac{c}{2d}$ ; возможность применения ЦОС
Рефлекторные микрофоны	$R(\theta) = \frac{2 \times J_1(\psi)}{\psi}$ <p>где <math>\psi = \frac{2 \times \pi}{\lambda} \times \rho_0 \times \sin(\theta)</math>  <math>\rho_0</math> – диаметр параболы отражателя,  <math>J_1(\psi)</math> – функция Бесселя 1-го порядка</p>	$d = 90$ см.  $Q = 30$ дБ на частоте 4 кГц	Обладает наилучшей пространственной избирательностью на высокой частоте, но на низкой частоте уступает УНМ типа линейной группы микрофонов; ограничения по $F_{\text{max}}$ не имеет

Мощным дополнительным импульсом к расширению сферы применения МР стали разработка и серийный выпуск цифровых микроэлектромеханических систем МЭМС микрофонов (в английской транскрипции MEMS – Microelectromechanical systems). МЭМС микрофоны преобразуют аналоговый сигнал в цифровой, позволяя использовать ЦОС, что повышает качество МР и стабильность ее характеристик. Малые размеры микрофонов дают возможность при необходимости повысить максимально применимую рабочую частоту решетки.

Все технологии извлечения речевой информации в МР неразрывно связаны с алгоритмами ЦОС, которые значительно расширяют функциональные возможности узконаправленных микрофонов. В МР наиболее часто используются следующие алгоритмы ЦОС: алгоритм задержки и суммирования (может использоваться самостоятельно или в подрешетках), алгоритм сверхнаправленности, алгоритм подавления боковых лепестков, алгоритм пост-фильтрации Винера [2, 4].

Структурная схема МР, использующая алгоритм задержки и суммирования, представляет собой линейную эквидистантную группу микрофонов, выходы которых соединены с сумматором через элементы, осуществляющие задержку сигналов на время, необходимое для

совмещения сигналов по фазе от всех микрофонов решетки. Этот алгоритм также позволяет осуществить качание луча МР за счет изменения фазового распределения вдоль раскрыва решетки. Большим недостатком таких решеток является их узкополосность, что приводит к сильной зависимости от частоты таких параметров МР, как ширина главного лепестка диаграммы направленности и уровень боковых лепестков.

Для устранения этой частотной зависимости и получения малой вариации величины пространственной избирательности в широком диапазоне частот используют подрешетки с одинаковым количеством микрофонов в каждой подрешетке, но с различными расстояниями между ними. Для каждого частотного участка используется решетка, которая удовлетворяет заданным параметрам по ширине главного лепестка и уровню боковых лепестков. На рис. 1 изображена структурная схема МР, реализующей данный алгоритм с применением полосовых фильтров (ПФ1-ПФ4) для каждого частотного диапазона. Как видно из рисунка, микрофоны используются сразу в нескольких подрешетках, что увеличивает их эффективность [4].

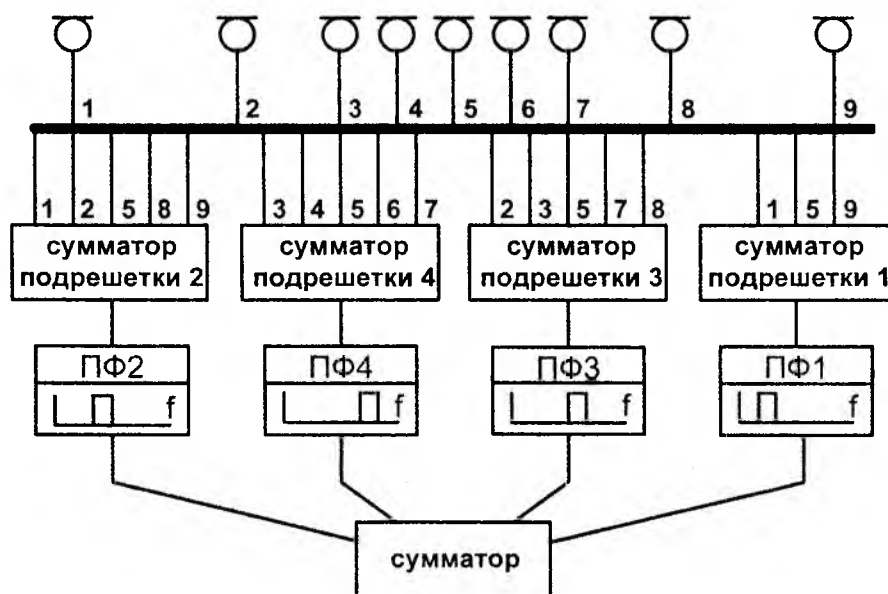


Рис. 1. Структурная схема МР, использующая алгоритм задержки и суммирования в подрешетках

МР, использующая алгоритм сверхнаправленности, имеет структуру, объединяющую в себе дифференциальную микрофонную решетку и МР на основе алгоритма задержки и суммирования.

Дифференциальная микрофонная решетка состоит из двух ненаправленных микрофонов, разнесенных на расстояние  $d$ . Сигнал со второго микрофона задерживается и вычитается из сигнала первого микрофона (рис. 2). Посредством вариации величины задержки  $\tau$  можно изменять диаграмму направленности микрофонной решетки [3].

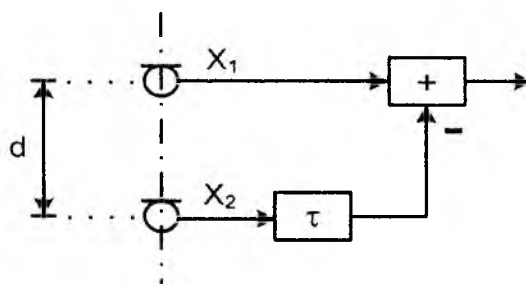


Рис. 2 Структурная схема дифференциальной микрофонной решетки

Недостатком дифференциальной микрофонной решетки является спад ее индекса направленности с увеличением частоты. По индексу направленности дифференциальная микрофонная решетка на более высоких частотах уступает МР, построенной по алгоритму задержки и суммирования. Оптимальной структурой микрофонной решетки для получения максимального индекса направленности является алгоритм сверхнаправленности. Алгоритм сверхнаправленности объединяет преимущества двух алгоритмов дифференциального и задержки и суммирования. На низких частотах используется более эффективный дифференциальный алгоритм  $DIF(\omega)$ , а на более высокой частоте – алгоритм задержки и суммирования  $Q(\omega)$  (рис. 3).

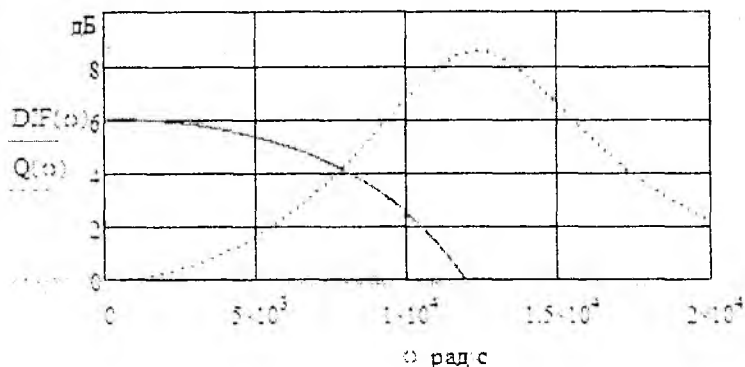


Рис. 3. Частотная зависимость индекса направленности дифференциальной микрофонной решетки и МР с алгоритмом задержки и суммирования

Структурная схема, реализующая алгоритм сверхнаправленности, показана на рис. 4.

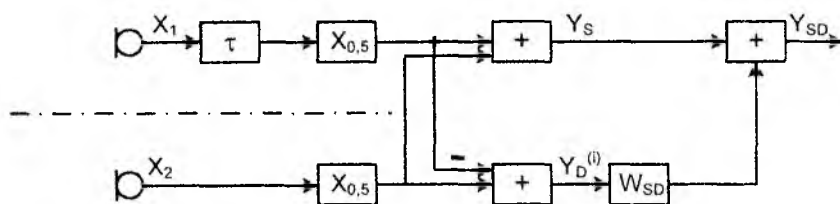


Рис. 4. Структурная схема сверхнаправленной решетки микрофонов (SNPM)

Сигнал  $Y_s$  является суммой сигналов от двух микрофонов с задержкой. Сигнал  $Y_D^{(i)}$  является разностью сигналов от двух микрофонов. Из формулы (1) можно получить диаграмму направленности алгоритма задержки и суммирования [3]:

$$HS(\omega, \theta) = \exp(-j \cdot k \cdot d \cdot 2) \times \cos(k \cdot d \cdot 2 \cdot (1 - \cos(\theta))) \quad (1)$$

Диаграмма направленности дифференциальной МР может быть рассчитана из следующей формулы [3]:

$$H_D^{(i)}(\omega, \theta) = j \cdot \exp\left(-j \cdot \frac{k \cdot d}{2}\right) \times \sin\left(\frac{k \cdot d}{2} \cdot (1 - \cos(\theta))\right) \quad (2)$$

Для того чтобы получить оптимальный сигнал  $Y_{SD}$ , сигнал  $Y_D^{(i)}$  должен пройти фильтр  $W_{SD}$  и затем быть вычтен из сигнала  $Y_s$ . Оптимальным фильтром будет решение Винера [3]:

$$W_{SD}(\omega) = \frac{-j \cdot \sin c(\omega \cdot \tau_a) \times \sin(\omega \cdot \tau_a)}{1 - \sin c(\omega \cdot \tau_a) \times \cos(\omega \cdot \tau_a)} \quad (3)$$

Зависимость индекса направленности от частоты можно рассчитать по формуле

$$DI_{SD}(\omega) = 2 \cdot \frac{1 - \sin c(2 \cdot \omega \cdot \tau_a)}{1 - \sin c^2(\omega \cdot \tau_a)} \quad (4)$$

Алгоритм сверхнаправленности позволяет получить максимум значения индекса направленности двух алгоритмов (рис. 5).

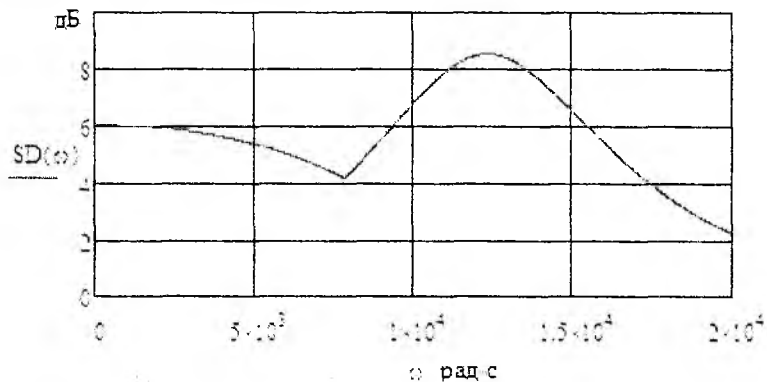


Рис. 5. Частотная зависимость индекса направленности МР с алгоритмом сверхнаправленности

### Построение узконаправленной решетки с использованием подрешеток по алгоритму сверхнаправленности

Алгоритм сверхнаправленности применяется для решетки из двух микрофонов и поэтому невозможно достичь большого индекса направленности и большой рабочей полосы для МР при неизменных размерах всей решетки.

Если в линейной группе микрофонов использовать в качестве элемента группы МР, построенную по алгоритму сверхнаправленности (СНМР) (рис. 6), можно достичь существенного повышения индекса направленности в широкой полосе частот и особенно на низких частотах.

На рис. 7 изображены частотные зависимости индексов направленности двух линейных групп микрофонов:

- 1-я классическая МР с эквидистантным расположением микрофонов (LGM) с параметрами  $d = 4.3$  см,  $n = 21$ ,  $L = 90$  см;
- 2-я МР с использованием в качестве элемента группы, двух микрофонов с ЦОС по алгоритму сверхнаправленности (СНМР) (по схеме на рис. 6) с теми же параметрами  $d = 4.3$  см,  $n = 21$ ,  $L = 90$  см.

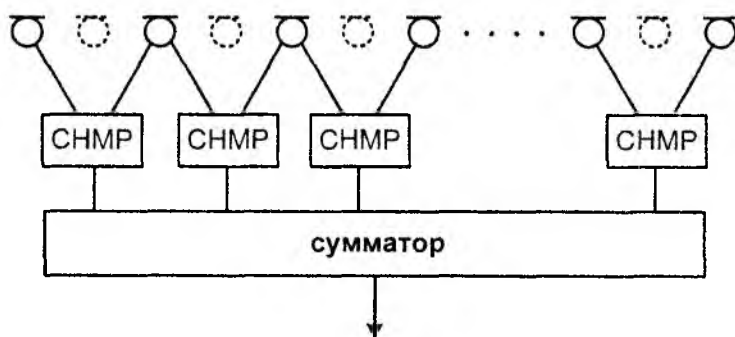


Рис. 6. МР в виде линейной группы микрофонов с использованием в качестве элемента группы, двух микрофонов с ЦОС по алгоритму сверхнаправленности (СНМР)

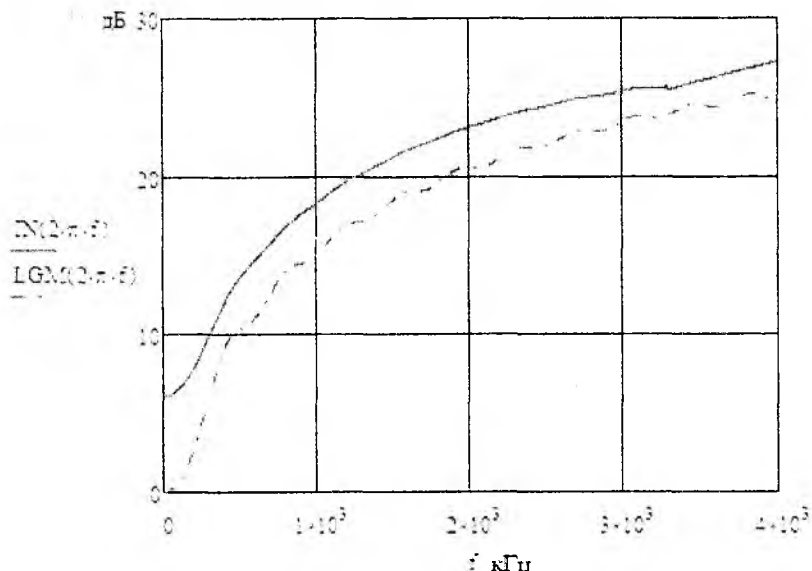


Рис. 7. Зависимость индекса направленности от частоты классической МР (LGM) и МР с ЦОС в подрешетках по алгоритму сверхнаправленности (IN)

### Выводы

Средства акустической разведки развивались вместе с развитием технологий обработки сигналов. Большое влияние на развитие узконаправленных микрофонов оказала ЦОС. Использование решеток, применяющих алгоритм сверхнаправленности, позволяет поднять индекс направленности на низкой частоте, применяя их в качестве подрешеток в более сложных структурах МР. Полученное преимущество в 6 дБ позволяет получить увеличение дальности разведывательного контакта в два раза. Алгоритм подавления боковых лепестков, позволяет подавить мощную помеху, увеличивая отношение сигнал/шум. Алгоритм пост-фильтрации Винера позволяет компенсировать некогерентные помехи, а также снизить уровень помех от когерентных источников, принимаемых боковыми лепестками.

**Список литературы:** 1. Олейников, А.Н., Войтенко, А.О. Сравнительная характеристика параметров узконаправленных микрофонов // Радиотехника. – 2013. – Вып. № 173. – С. 224-231 2. Столбов, М.Б. Применение микрофонных решеток для дистанционного сбора речевой информации // Научно-технический вестник информационных технологий, механики и оптики. – 2015. – Т. 15. – № 4. – С. 661-675 3. Buck, M., Röbber, M. First order differential microphone arrays for automotive applications // Proc. 7th International Workshop on Acoustic Echo and Noise Control, IWAENC. Darmstadt, Germany, 2001, pp. 19 – 22 4. McCowan, I.A. Microphone Arrays: A Tutorial. Available at: <https://www.idiap.ch/~mccowan/arrays/tutorial.pdf> (accessed 01.04.2017).

Харьковский национальный  
университет радиозлектроники

Поступила в редколлегию 17.03.2017

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПК ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

### Введение

В настоящий момент защита персональных данных пользователей приобретает первоочередное значение. Стремительный рост и развитие огромного числа сетевых приложений для выполнения различного рода операций от социальной коммуникации и развлечений (социальные сети, игровые серверы) до проведения крупных платежных транзакций (системы онлайн банкинга, крупные торговые онлайн площадки, личные порталы абонентов) требует комплексных подходов по обеспечению безопасности на всех этапах их реализации. Потенциальный ущерб от кражи персональной информации может исчисляться колоссальными материальными издержками. В этой связи надежность процедуры аутентификации является необходимым обстоятельством, гарантирующим сохранность конфиденциальных данных.

Аутентификация пользователей является одним из наиболее важных и сложных аспектов обеспечения контроля несанкционированного доступа к ресурсам компьютерной системы. Она представляет собой процесс, с помощью которого система проверяет, имеет ли пользователь законное право на доступ к ней. Традиционно выделяют три основных подхода для аутентификации пользователя. К ним относятся [1]:

- методы, основанные на владении дополнительными программно-аппаратными средствами для идентификации пользователя системой (смарт-карты, документы, удостоверяющие личность, ключи для генерации электронных цифровых подписей, аппаратные ключи, USB-токены);
- методы, основанные на уникальном знании пользователей (персональные идентификаторы, логины, пароли, их совместное использование);
- биометрические технологии аутентификации (статические и динамические).

На рис. 1 приведена онтология различных режимов аутентификации, включая биометрические поведенческие модели.

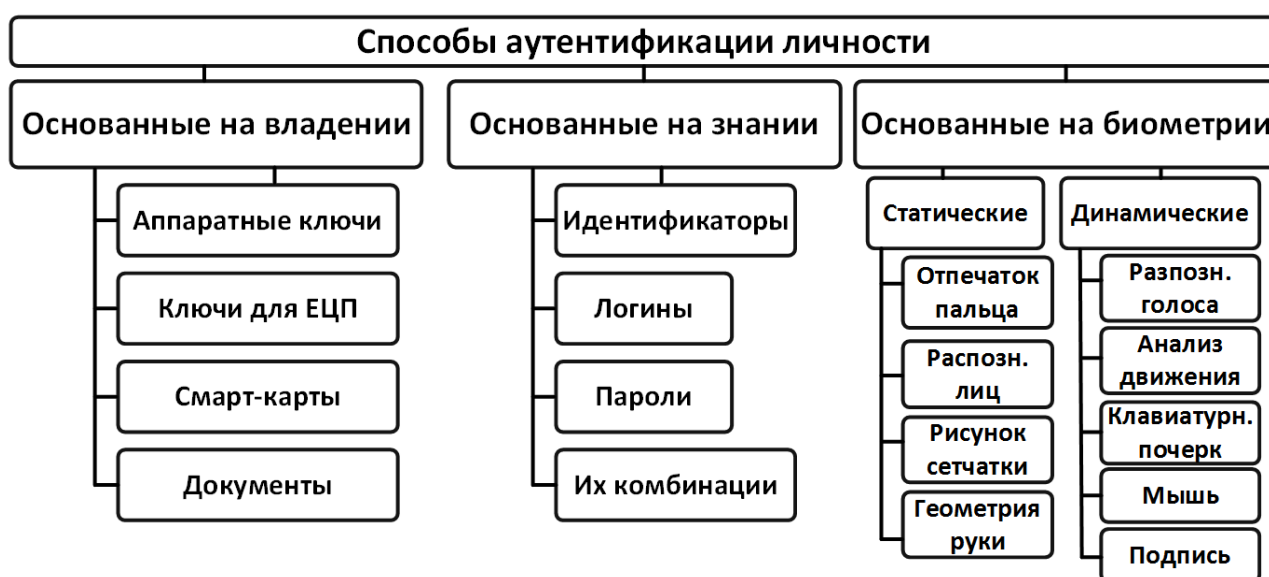


Рис. 1

Наибольший интерес для исследователей представляют биометрические параметры пользователей, которые в отличие от традиционных паролей, достаточно трудно воспроизвести и они не могут быть утеряны, переданы третьим лицам, украдены или забыты.

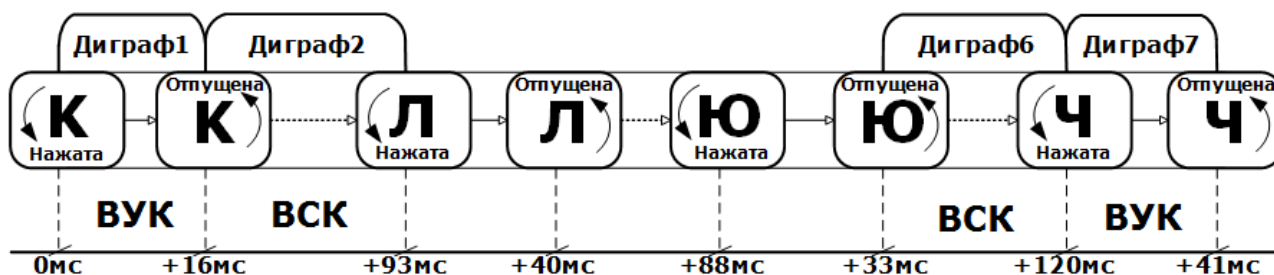
Биометрические характеристики пользователя условно можно разделить на две большие группы: физиологические (статические) и поведенческие (динамические) [2]. Первые – присущи человеку от момента рождения и неизменны на протяжении всей жизни. К ним относятся отпечатки пальцев, распознавание характерных черт лица, геометрии руки, сетчатки глаза и т.д.

Биометрические технологии, основанные на поведенческих моделях пользователя, могут включать: распознавание голоса человека, детекцию и изучение характера движения, анализ подписи, анализ характера работы пользователя с интерфейсом, взаимодействие пользователя с компьютерной мышью, анализ клавиатурного почерка. Данные характеристики все чаще используются в качестве полноценной технологии контроля доступа к ресурсам системы или дополнительной меры, способной повысить безопасность прохождения процедуры аутентификации. На основании собранных и проанализированных данных создаются уникальные профили пользователей, которые в последующем будут участвовать в прохождении процедуры аутентификации. Низкая стоимость реализации и последующего сопровождения такого рода решений, отсутствие необходимости создания дополнительного оборудования, легкость интеграции с существующими системами безопасности привели к бурному росту исследований в данной области [3].

Еще одним преимуществом использования биометрических характеристик на основе поведенческих моделей является то обстоятельство, что аутентификация может производиться на протяжении всего сеанса работы пользователя – так называемая «непрерывная аутентификация» – в отличие от разовой парольной проверки во время первого входа в систему. Это может предотвратить несанкционированное вмешательство в пользовательскую сессию уже после того, как был осуществлен начальный вход в систему.

### Анализ и сравнение методов, основанных на изучении характеристик клавиатурного почерка пользователя

Впервые вопросы использования индивидуальных особенностей работы с клавиатурой были рассмотрены в середине 70-х годов прошлого века [4]. За последних два десятилетия исследователи использовали различные методы, подходы и алгоритмы для сбора и обработки необходимых персональных данных, их представления, классификации и оценки эффективности для изучения возможности построения систем аутентификации на базе обширного парка устройств (персональных компьютеров и ноутбуков с механическими клавиатурами (МК), мобильных платформ (МП) с сенсорными дисплеями (СД), специализированных устройств ввода (СУВ) [5]. При этом наиболее распространенными параметрами для анализа являются временные характеристики (см. рис. 1) нажатия клавиш: время удержания клавиши (ВУК) и время между нажатиями соседних клавиш (ВСК), которые могут быть измерены с точностью до единиц миллисекунд. На рис. 2 два последовательных события клавиатуры образуют диграф, три события – триграф,  $n$  следующих друг за другом событий клавиатуры –  $n$ -граф [6].



Дополнительными пространственными параметрами, извлекаемыми из данных о нажатиях клавиш, могут быть величина давления, положение пальцев на сенсорном экране, частота ошибок при наборе текста, скорость набора и функции коррекции текста [7].

Основными показателями качества работы системы биометрической аутентификации личности являются ошибки трех видов, выраженные в процентном соотношении. К ним относятся: FRR (False Reject Rate) – ошибка первого рода, которая определяется как вероятность ошибочного отказа законному пользователю; FAR (False Accept Rate) – ошибка второго рода, которая определяется как вероятность допуска незарегистрированного пользователя. Общая оценка системы описывается при помощи равного уровня ошибок EER (Equal Error Rates), при котором FAR и FRR равны. Более низкий показатель EER указывает на лучшую эффективность системы аутентификации. Другие критерии оценки системы включают в себя технологичность, производительность и удобство использования.

Одной из важнейших частей системы аутентификации, основанной на анализе какой-либо поведенческой модели, является базовый алгоритм обработки полученных данных. Анализ литературы в данной предметной области показывает, что в более ранних работах большинство методов классификации представляли собой вероятностно-статистические подходы, однако, в настоящее время исследователи сосредоточились на изучении и апробации подходов по классификации параметров клавиатурного почерка, в основе которых лежат современные методы машинного обучения.

В рамках вероятностно-статистических подходов обработки полученных данных чаще всего применяются [8]:

- математическое ожидание и среднее квадратичное отклонение;
- алгоритмы, основанные на вычислении оценок сходства между объектами, например, метод ближайших соседей k-NN (k-nearest neighbors algorithm);
- классификаторы, основанные на измерении геометрических расстояний – Евклидово расстояние (Euclidean distance), расстояние Махаланобиса (Mahalanobis distance), Манхэттенское расстояние (Manhattan distance), расстояние Хемминга (Hamming distance);
- методы, основанные на величине меры энтропии (неупорядоченности) системы;
- алгоритмы динамической трансформации временной шкалы (dynamic time warping);
- скрытые марковские модели (hidden Markov model);
- байесовские классификаторы (Bayes classifier);
- критерии проверки гипотез Колмогорова и Смирнова (Kolmogorov, Smirnov criterions);
- методы дисперсионного анализа ANOVA (Analysis of variance).

Методы машинного обучения включают в себя [9]:

- искусственные нейронные сети ANN (artificial networks);
- деревья принятия решений (decision trees);
- решения на базе элементов нечеткой логики (fuzzy logic);
- эволюционное моделирование (evolutionary computation);
- методы опорных векторов (support vector machines).

Архитектура искусственных нейронных сетей может быть представлена в виде:

- многослойного перцептрона MLP (multilayer perceptron);
- сети радиально-базисных функций RBFN (radial basis function network);
- обучаемого векторного квантования LVQ (learning vector quantization);
- самоорганизующейся карты Кохонена SOM (self-organizing map) или SOFM (self-organizing feature map).

В качестве основы эволюционного моделирования применяются:

- генетические алгоритмы GA (genetic algorithms);
- метод роя частиц PSO (particle swarm optimization);
- муравьиный алгоритм ACO (ant colony optimization algorithms).

В таблице представлены результаты сравнения различных подходов анализа характеристик клавиатурного почерка, использующих наиболее распространенные методы машинного обучения и вероятностно-статистические модели.

Год	Участники эксперимента	Анализируемые параметры	Метод классификации	Вид и длина вводимого текста	Устройство	Результаты, %
<i>Методы, основанные на расчете среднего значения и дисперсии (Mean and STD)</i>						
2005	205	ВСК	<i>Mean and STD</i>	длинный	МК	FAR:0.5 FRR:5
2009	30	ВСК, ВУК	<i>Mean and STD</i>	текст	МП	EER:13
2009	1254	ВСК, ВУК	<i>Mean and STD</i>	короткий	МК	FAR:16 FRR:1
2012	51	ВСК, ВУК	<i>Mean and STD</i>	короткий	МК	EER:8.4
2013	152	ВСК, ВУК, давление	<i>Mean and STD</i>	цифровой	МП	FAR:4.19 FRR:4.59
<i>Подходы, основанные на методе k ближайших соседей (k-NN)</i>						
2002	7	ВСК, ВУК,	<i>k-NN</i>	цифровой	СУВ	EER:78-99
2008	10	давление	<i>k-NN</i>	цифровой	ТС	EER:1.00
2010	120	ВСК, ВУК	<i>k-NN</i>	короткий	МК	EER:1.00
2010	100	ВСК, ВУК	<i>k-NN</i>	текст	МК	EER:2.7
2010	30	ВСК, ВУК	<i>k-NN</i>	цифровой	МК	EER:0.5
2013	40	ВСК, ВУК	<i>k-NN</i>	длинный	МК	EER:6.1
<i>Методы, основанные на измерении геометрических расстояний (Euclidean distance)</i>						
2007	21	ВСК, ВУК	<i>Euclidean distance</i>	короткий	МК	EER:3.8
2008	30	ВСК, ВУК давление	<i>Euclidean distance</i>	цифровой	СУВ	FAR:15 FRR:0 EER:10
2009	16	ВСК, ВУК	<i>Euclidean distance</i>	короткий	МК	EER:4.28
2010	100	ВСК, ВУК	<i>Euclidean distance</i>	текст	МК	EER:2.7
2010	189	ВСК, ВУК	<i>Euclidean distance</i>	длинный	МК	FAR:0.01 FRR:3
2011	51	ВСК	<i>Euclidean distance</i>	длинный	МК	EER:0.84
2011	20	ВСК	<i>Euclidean distance</i>	длинный	МК	FAR:2 FRR:4
<i>Подходы, основанные на величине энтропии системы (Entropy)</i>						
2005	31	ВСК	<i>Entropy</i>	длинный	МК	FAR: 1.99 FRR: 2.42
2005	205	ВСК	<i>Entropy</i>	длинный	МК	FAR: 0.5 FRR: 5
2009	21	ВСК, ВУК	<i>Entropy</i>	длинный	МК	FAR: 0.14 FRR: 1.59
2011	50	ВСК	<i>Entropy</i>	длинный	МК	EER: 10
2011	186	ВСК, ВУК	<i>Entropy</i>	длинный	МК	FAR: 1.65 FRR: 2.75

Год	Участники эксперимента	Анализируемые параметры	Метод классификации	Вид и длина вводимого текста	Устройство	Результаты, %
<i>Подходы, основанные на других статистических методах, а также их комбинациях</i>						
1990	26	ВСК	Baysian, Minimum Distance	короткий	МК	FAR: 2.8 FRR: 8.1
2004	41	ВСК, ВУК	Gaussian mixture modeling	короткий	МК	FAR: 4.3 FRR: 4.8 EER: 4.4
2005	9	ВСК, ВУК, давление,	ANOVA	цифровой	МК	EER: 2.4
2006	100	ВСК, ВУК, давление,	Dynamic time warping	цифровой	МК	EER: 1.4
2006	20	ВСК, ВУК	Hidden Markov model	цифровой	МК	EER: 3.6
2006	20	ВСК, ВУК	Euclidian, Mahalanobis	цифровой	ТС	FAR: 0 FRR: 2.5
2009	25	ВСК, ВУК	Gauss, Parzen, K-NN, K-mein	короткий	МК	EER: 1.00
2009	100	ВСК, ВУК	Bayesian, Euclidean, Hamming	короткий	МК	EER: 6.96
2010	51	ВСК, ВУК	Manhattan distance	короткий	МК	EER: 7.16
2010	35	ВСК	Kolmogorov-Smirnov	длинный	МК	EER: 7.16
2011	100	ВСК, ВУК	Gaussian PDF	короткий	МК	EER: 1.401
2011	55	ВСК, ВУК	Spearman's foot rule distance	длинный	МК	FAR: 2.02 FRR: 1.84
2011	33	ВСК, ВУК	Naive Bayesian	длинный	МК	EER: 1.72
2013	152	ВСК, ВУК, давление, датчики	k-mean	цифровой	МП	FAR: 4.19 FRR: 4.59
2013	10	ВСК, ВУК, датчики	Bayesian	цифровой	ТС	FAR: 0.02 FRR: 0.018
2014	30	ВСК, ВУК	SMD, SED	цифровой	МК	EER: 26
<i>Методы, основанные на деревьях принятия решений (Random forest decision tree, RFDT)</i>						
2010	21	ВСК, ВУК,	RFDT	длинный	МК	FAR: 3.47 FRR: 0 EER: 1.73
2010	28	ВСК, ВУК,	RFDT	цифровой	МК	FAR: 0.03 FRR: 1.51 EER: 1
<i>Методы, основанные на искусственных нейронных сетях (ANN)</i>						
2007	100	ВСК, ВУК,	ANN	короткий	МК	FAR: 1 FRR: 8
2010	25	ВСК, ВУК, давление	ANN	цифровой	МК	FAR: 4.12 FRR: 5.55

Год	Участники эксперимента	Анализируемые параметры	Метод классификации	Вид и длина вводимого текста	Устройство	Результаты, %
<i>Подходы, основанные на методе опорных векторов (SVM)</i>						
2007	24	ВСК, ВУК	SVM	длинный	МК	FAR: 0.76 FRR: 0.81 EER: 1.57
2007	61	ВСК, ВУК	SVM	короткий	–	FAR: 14.5 FRR: 1.78
2007	5	давление	SVM	цифровой	МК	FAR: 0.95 FRR: 5.6
2011	117	ВСК, ВУК	SVM	короткий	МК	EER: 11.8
2014	30	ВСК, ВУК, давление	SVM	цифровой	СД	EER: 2.8
<i>Подходы, основанные на других менее распространенных методах машинного обучения</i>						
2005	43	ВСК, ВУК	Decision trees, Monte Carlo	короткий	МК	FAR: 0.88 FRR: 9.62
2005	53	ВСК, ВУК	Fuzzy ARTMAP	короткий	МК	FAR: 0.87 FRR: 4.4
2007	30	ВСК, ВУК	Sequence alignment algorithms	короткий	МК	FAR: 0.2 FRR: 0.2 EER: 0.4
2014	42	ВСК, ВУК, давление, датчики	Naive, Bayesian	короткий	МП	EER: 12.9
2015	42	ВСК, ВУК, давление, датчики	Two-class	короткий	МП	EER: 3

## Выводы

1. Анализируя приведенные в таблице данные, можно сделать вывод, что конечная точность полученных результатов определяется рядом факторов, главными среди которых являются: основной алгоритм классификации полученных данных, количество участников эксперимента с различной величиной опыта работы с клавиатурой, способ и организация ввода данных и аппаратная платформа, на базе которой производится тестирование системы аутентификации.

2. Использование современных методов машинного обучения дает возможность получить более высокие результаты при аутентификации в сравнении с вероятностно-статистическими, но требует от системы большей вычислительной сложности, что зачастую не оправдано и может быть реализовано лишь частично. Максимальные результаты показывают методы, основанные на деревьях принятия решений и искусственных нейронных сетях.

3. Использование комбинаций вероятностно-статистических подходов анализа особенностей клавиатурного почерка в рамках одного алгоритма позволяет повысить уровень точности системы в целом.

4. Использование дополнительных пространственных параметров клавиатурного почерка (давление, координаты пальцев на сенсорных дисплеях мобильных устройств) дает значительный прирост в показателях точности в сравнении со стандартными механическими

клавиатурами за счет выделения дополнительных информативных признаков анализируемого почерка субъекта.

5. Существенно повысить качество систем аутентификации пользователей ПК можно путем перехода к комплексным моделям, которые учитывают, например, следующие характеристики:

- данные, которые позволят однозначно идентифицировать пользователя (уникальный идентификатор, пароль, цифровые подписи оборудования и т.д.);
- информационный почерк пользователя – клавиатурный почерк и динамику системы «пользователь – мышь»;
- активность пользователя в рамках операционной системы (средний процент использования центрального процессора, средний объем занимаемой памяти, тип наиболее часто открываемых файлов и т.д.);
- сетевая активность пользователя (наиболее часто используемые сетевые сервисы и приложения, тип активности пользователя в сети и т.д.);
- программно-аппаратные изменения в конфигурации ПК (установка нового программного обеспечения, установка или замена внешних устройств и т.д.).

**Список литературы:** 1. Брюхомицкий, Ю.А. Исследование биометрических систем динамической аутентификации пользователей ПК по рукописному и клавиатурному почеркам : учеб.-метод. пособие / Ю.А Брюхомицкий, М.Н. Казарин. – Таганрог, 2004. 2. Kyle O.Bailey, James S. Okolica, Gilbert Peterson, “User identification and authentication using multi-modal behavioral biometrics,” Computers and Security journal, vol.43, pp.77-89, June 2014. 3. Roman V.Yampolskiy, Venu Govindaraju. Behavioural biometrics: a survey and classification // International Journal of Biometrics, vol.1, pp.81-113, November 2008. 4. Gaines, R., Lisowski, W., Press, S. and Shapiro, N. Authentication by keystroke timing: some preliminary results // Technical Report Rand Rep. R-2560-NSF, RAND Corporation, p. 51, 1980. 5. Spillane, R. Keyboard apparatus for personal identification. IBM Technical Disclosure Bulletin, 17(11), 1975. 6. Sim, T. and Janakiraman, R. Are digraphs good for free-text keystroke dynamics? // IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1–6, 2007. 7. Umphress, D., Williams, G. Identity verification through keyboard characteristics // International Journal of Man-Machine Studies, vol. 23(3), pp. 263–273, 1985. 8. Balagani, K.S., Vir V. Phoha, Ray, A. and Phoha, S. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication // Pattern Recognition Letters, vol. 32(7), pp. 1070–1080, 2011. 9. Md Liakat Ali, John Monaco, Charles Tappert, Meikang Qiu. Keystroke Biometric Systems for User Authentication // Journal of Signal Processing Systems, vol. 86(2) pp.175–190, March 2017.

Харьковский национальный  
университет радиоэлектроники

Поступила в редколлегию 25.03.2017

**МЕТОДЫ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ, ОБРАБОТКИ И АНАЛИЗА ДАННЫХ  
METHODS FOR PROTECTED TRANSMISSION, PROCESSING AND ANALYSIS OF DATA**

УДК 681.3.06:519.248.681

**Информационная безопасность и помехозащищенность телекоммуникационных систем в условиях различных внутренних и внешних воздействии** / *И.Д. Горбенко, А.А. Замула, В.Л. Морозов* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 5 – 14.

Рассмотрены проблемы повышения помехозащищенности (скрытности функционирования системы, помехоустойчивости приема сигналов), информационной безопасности телекоммуникационных систем (ТКС) в условиях существования множества помех и преднамеренного воздействия станций противодействия. Показано, что решение указанной проблемы возможно на основе усовершенствования методологических основ построения ТКС, путем разработки методов информационного обмена, синтеза новых классов нелинейных дискретных сложных сигналов с необходимыми ансамблевыми, корреляционными и структурными свойствами.

Табл. 1. Ил. 1. Библиогр.: 11 назв.

УДК 681.3.06:519.248.681

**Інформаційна безпека та завадозахищеність телекомунікаційних систем в умовах різних внутрішніх та зовнішніх впливів** / *І.Д. Горбенко, О.А. Замула, В.Л. Морозов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 5 – 14.

Розглянуто проблему підвищення завадозахищеності (скритності функціонування системи, завадостійкості прийому сигналів), інформаційної безпеки телекомунікаційних систем (ТКС) в умовах існування безлічі перешкод і навмисного впливу станцій протидії. Показано, що рішення зазначеної проблеми можливе на основі вдосконалення методологічних основ побудови ТКС, шляхом розробки методів інформаційного обміну, синтезу нових класів нелінійних дискретних складних сигналів з необхідними ансамблевими, кореляційними і структурними властивостями.

Табл. 1. Іл. 1. Бібліогр.: 11 назв.

UDC 681.3.06:519.248.681

**Information security and interference immunity of telecommunication systems under conditions of various internal and external impacts** / *I.D. Gorbenko, A.A. Zamula, V.L. Morozov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 5 – 14.

The problems of increasing noise immunity (stealth operation of the system, noise immunity of signal reception), information security of telecommunication systems (TCS) in the presence of a lot of interference and deliberate influence of counteraction stations are considered. It is shown that this problem solution is possible on the basis of improving the methodological foundations of the TCS construction by developing methods of information exchange, the synthesis of new classes of nonlinear discrete complex signals with the necessary ensemble, correlation and structural properties.

1 tab. 1 fig. Ref.: 11 items.

УДК 681.518: 004.658.3

**Кибернетический подход к решению задачи реинжиниринга баз данных** / *В.И. Есин* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 15 – 22.

Сформулирована и формализована задача реинжиниринга баз данных информационных систем организационного управления в виде известной из общей теории адаптивных систем задачи структурной адаптации. Предложен способ ее решения.

Ил. 2. Библиогр.: 10 назв.

УДК 681.518: 004.658.3

**Кібернетичний підхід до вирішення задачі реінжинірінгу баз даних** / *В.І. Єсін* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 15 – 22.

Сформульовано та формалізовано задачу реінжинірінгу баз даних інформаційних систем організаційного управління у вигляді відомої із загальної теорії адаптивних систем задачі структурної адаптації. Запропонований спосіб її вирішення.

Іл. 2. Бібліогр.: 10 назв.

UDC 681.518: 004.658.3

**Cybernetic approach to solving the task of database reengineering** / V. I. Yesin // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 15 – 22.

The task of reengineering databases of the organizational management information system is formulated and formalized in the form of the structural adaptation task known from the general adaptive systems theory. The method for its solution is proposed.

2 fig. Ref.: 10 items.

УДК 004.056.53:621.39

**Методика организации мероприятий защиты от технических средств конкурентной разведки** / В.И.Заболотный, А.В. Ермолович // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 23 – 28.

Защита от конкурентной разведки достигается внедрением комплексной системы мер защиты. Разработка мер защиты происходит в соответствии следующие установки перечня работ. Определено, что разработка мер контроля мер защиты направлена на предотвращение и предупреждение невыполнения разработанных мер защиты для разрабатываемого объекта. Основная цель исследований – определение содержательности основных понятий при защите от конкурентной разведки, разграничения и постановка задач для всех основных этапов по разработке мер защиты от конкурентной разведки, разработка методики организации данных работ.

Ил. 1. Библиогр.: 4 назв.

УДК 004.056.53:621.39

**Методика організації заходів захисту від технічних засобів конкурентної розвідки** / В. І. Заболотний, А. В. Єрмолович // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 23 – 28.

Захист від конкурентної розвідки досягається впровадженням комплексної системи заходів захисту. Розробка заходів захисту відбувається відповідно встановленому переліку робіт. Визначено, що розробка заходів контролю заходів захисту направлена на унеможливлення та попередження невиконання розроблених заходів захисту для розроблюваного об'єкту. Основна мета досліджень – визначення змістовності основних понять при захисті від конкурентної розвідки, розмежування та постановка завдань для всіх основних етапів з розробки заходів захисту від конкурентної розвідки, розробка методики організації даних робіт.

1. Іл. Бібліогр.: 4 назви.

UDC 004.056.53:621.39

**Methodology for organization of protection measures against technical means of competitive intelligence** / V.I. Zabolotniy, A.V. Yermolovych // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 23 – 28.

Protection is achieved by introduction of competitive intelligence complex systems of protection. Development of protective measures is in accordance with a defined scope of work. It was determined that the development of control measures protection measures aimed at preventing failure and inability to measures designed to protect the developed object. The main goal of the research is to determine the consistency in defending the basic concepts of competitive intelligence, separation and setting targets for all the major steps to develop measures to protect against competitive intelligence, develop methods of organizing data work.

1 fig. Ref.: 4 items.

УДК 681.142

**Усовершенствованный метод определения альтернативной совокупности чисел в системе остаточных классов** / В. А. Краснобаев, С. А. Кошман, А. С. Янко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 29 – 37.

Проведен анализ наиболее известных практических методов определения альтернативной совокупности (АС) чисел в системе остаточных классов (СОК). Основным недостатком рассмотренных методов является значительное время определения АС. С целью уменьшения время определения АС в СОК, в статье усовершенствован известный метод. Суть совершенствования предложенного в статье метода состоит в том, что при его использовании уменьшается время определения АС чисел в СОК.

*Ключевые слова:* машинная арифметика, система остаточных классов, альтернативная совокупность, диагностика и коррекция ошибок данных.

Табл. 11. Библиогр.: 9 назв.

УДК 681.142

**Вдосконалений метод визначення альтернативної сукупності чисел у системі залишкових класів** / В. А. Краснобаєв, С. О. Кошман, А. С. Янко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 29 – 37.

Проведено аналіз найбільш відомих практичних методів визначення альтернативної сукупності (АС) чисел у системі залишкових класів (СЗК). Основним недоліком розглянутих методів є значний час визначення АС. З метою зменшення часу визначення АС у СЗК, у статті вдосконалений відомий метод. Суть вдосконалення запропонованого у статті методу полягає у тому, що при його використанні зменшується час визначення АС чисел у СОК.

*Ключові слова:* машинна арифметика, система залишкових класів, альтернативна сукупність, діагностика та корекція помилок даних.

Табл. 11. Бібліогр.: 9 назв.

UDC 681.142

**Improved method for determining an alternative set of numbers in a system of residual classes** / V. A. Krasnobayev, S. A. Koshman, A. S. Yanko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 29 – 37.

The most well-known practical methods for alternative set (AS) determining of numbers in the residue number system (RNS) are analyzed. The main disadvantage of the considered methods consists in a considerable time of the AS determining. To reduce the time of the AS determining in the RNS the known method was improved. The essence of the improvement of the proposed method consists in the decrease of time needed for determining the AS numbers in the RNS.

*Key words:* arithmetic of machine, the system of residual classes, alternative set, diagnostics and correction of data errors

11 tab. Ref.: 9 items.

## МЕХАНИЗМЫ И МЕТОДЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ MECHANISMS AND METHODS OF CRYSTALLOGRAPHIC TRANSFORMATIONS

УДК 621.391:519.7

**Оценки вероятности обратимости случайных многочленов, используемых в модифицированной версии криптосистемы NTRU** / А.Н. Алексейчук, А.А. Матійко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 38 – 46.

Методом тригонометрических сумм получены аналитические оценки вероятности обратимости случайных многочленов, используемых в качестве секретных ключей в модифицированной версии криптосистемы NTRU. Продемонстрирована возможность применения полученных оценок на практике при выборе долговременных параметров криптосистемы.

*Ключевые слова:* асимметричная криптография, кольцо усеченных многочленов, NTRU, метод тригонометрических сумм.

Табл. 2. Рис. 2. Библиогр.: 11 назв.

УДК 621.391:519.7

**Оцінки ймовірності оборотності випадкових многочленів, що використовуються в модифікованій версії криптосистеми NTRU** / А.М. Олексійчук, А.А. Матійко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 38 – 46.

Методом тригонометричних сум отримано аналітичні оцінки ймовірності оборотності випадкових многочленів, що використовуються в якості секретних ключів у модифікованій версії криптосистеми NTRU. Продемонстрована можливість застосування отриманих оцінок на практиці при виборі довгострокових параметрів криптосистеми.

*Ключові слова:* асиметрична криптографія, кільце зрізаних многочленів, NTRU, метод тригонометричних сум.

Табл. 2. Рис. 2. Бібліогр.: 11 назв.

UDC 621.391:519.7

**Estimates of the probability of reversibility of random polynomials used in the modified version of NTRU cryptosystem** / A.N. Alekseychuk, A.A. Matiyko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. –

2017. – №189. – P. 38 – 46.

Using the trigonometric sums method we obtain analytical bounds for the probability of reversibility of polynomials used as secret keys in a modified version of NTRU encryption scheme. We show that the obtained bounds are applicable in practice to choosing the long-term parameters of the encryption scheme.

*Key words:* asymmetric cryptography, ring of truncated polynomials, NTRU, trigonometric sums method.

Tab. 2. Fig. 2. Ref.: 11 items.

УДК 004.056.55

**Алгебраической иммунитет нелинейных узлов симметричных шифров** / А.А. Кузнецов, Ю.И. Горбенко, И.Н. Белозерцев, А.В. Андрушкевич, А.П. Нарезный // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 47 – 58.

Исследуются методы вычисления алгебраической иммунности криптографических булевых функций и нелинейных узлов замен (подстановок) симметричных шифров. Приводятся результаты сравнительного анализа алгебраической иммунности нелинейных узлов симметричных шифров.

Табл. 1. Ил. 2. Библиогр.: 29 назв.

УДК 004.056.55

**Алгебраїчний імунітет нелінійних вузлів симетричних шифрів** / О.О. Кузнецов, Ю.І. Горбенко, І.М. Білозерцев, А.В. Андрушкевич, О.П. Наріжний // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 47 – 58.

Досліджуються методи обчислення алгебраїчної імунності криптографічних булевих функцій і нелінійних вузлів заміни (підстановок) симетричних шифрів. Наводяться результати порівняльного аналізу алгебраїчної імунності нелінійних вузлів симетричних шифрів.

Табл. 1. Іл. 2. Бібліогр.: 29 назв.

UDC 004.056.55

**Algebraic immunity of non-linear components of symmetric ciphers** / AA Kuznetsov, Yu.I. Gorbenko, I.N. Bilozertsev, A.V. Andrushkevych, A.P. Narezny // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 47 – 58.

Methods for calculating the algebraic immunity of cryptographic Boolean functions and non-linear components (substitutions) of symmetric ciphers have been studied. The results of the comparative analysis of algebraic immunity of non-linear nodes of symmetric ciphers are given.

1 tab. 2 fig. Ref.: 29 items.

УДК 004.056.55

**Алгоритмы электронной цифровой подписи на основе алгебраического кодирования** / А.А. Кузнецов, А.И. Пушкарёв, А.С. Киян // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 59 – 74.

Рассматриваются кодовые криптосистемы, задача криптоанализа в которых сводится к решению NP-сложной задачи декодирования случайного линейного кода. Предлагается новая схема ЭЦП с использованием алгебраических кодов, приводятся сравнительные оценки эффективности по различным показателям (стойкость, сложность формирования и проверки ЭЦП, объемы ключевых данных, длина подписи и пр.).

Табл. 1. Ил. 1. Библиогр.: 43 назв.

*Ключевые слова:* кодовая криптосистема, электронная цифровая подпись, постквантовая криптография.

УДК 004.056.55

**Алгоритми електронного цифрового підпису на основі алгебраїчного кодування** / А.А. Кузнецов, А.І. Пушкарьов, А.С. Киян // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 59 – 74.

Розглядаються кодові криптосистеми, завдання криптоаналізу в яких зводиться до вирішення NP-складної задачі декодування випадкового лінійного коду. Пропонується нова схема ЕЦП з використанням алгебраїчних кодів, наводяться порівняльні оцінки ефективності за різними показниками (стійкість, складність формування і перевірки ЕЦП, обсяги ключових даних, довжина підпису та ін.).

*Ключові слова:* кодова криптосистема, електронний цифровий підпис, пост-квантова криптографія.

Табл. 1. Іл.1. Бібліогр.: 43 назв.

UDC 004.056.55

**Algorithms of electronic digital signature based on algebraic coding** / A.A. Kuznetsov, A.I. Pushkarev, A.S. Kiyan // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 59 – 74.

The code cryptosystems are considered, the cryptanalysis problem in them is reduced to solving an NP-complex problem of decoding a random linear code. A new scheme of the EDS using algebraic codes is proposed, comparative evaluations of efficiency are carried out for various indicators (stability, complexity of formation and verification of the EDS, volumes of key data, length of signature, etc.).

*Key words:* code cryptosystem, electronic digital signature, post-quantum cryptography.

1 tab. 1 fig. Ref.: 43 items.

УДК 004.056.55

**Исследование применимости SMT/SAT доказательств в криптоанализе хеш-функций семейства Кескак** / Е.Г. Качко, Д.К. Телевний // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 75 – 80.

Статья посвящена проблеме использования средств доказательства теорем в криптоанализе функций Кескак-р на разных этапах преобразования. В статье описаны возможности использования SMT/SAT на примере поиска дифференциальных характеристик в начальных раундах преобразования хеш-функции, приводятся основные подходы SMT верификации при моделировании преобразований, описаны существующие средства доказательства теорем.

*Ключевые слова:* SMT, SAT, теорема, криптоанализ, Кескак, КНФ.

Табл. 1. Ил.1. Библиогр.: 7 назв.

УДК 004.056.55

**Дослідження використання SMT/SAT доказів в криптоаналізі хеш-функцій сімейства Кескак** / О.Г. Качко, Д.К. Телевний // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 75 – 80.

Стаття присвячена проблемі використання засобів доведення теорем в криптоаналізі функції Кескак-р на різних етапах перетворення. В статті описані можливості використання SMT/SAT на прикладі пошуку диференційних характеристик в початкових раундах перетворення хеш-функції, наведені основні способи SMT верифікації при моделюванні перетворень, описані існуючі засоби доведення теорем.

*Ключові слова:* SMT, SAT, теорема, криптоанализ, Кескак, КНФ.

Табл. 1. Іл.1. Бібліогр.: 7 назв.

UDC 004.056.55

**A study of the applicability of the SMT/SAT-based theorem proves for Keccak hash functions cryptanalysis** / O.Kachko, D.Televnyi // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 75 – 80.

The study is devoted to the problem of using the SMT proves for Keccak-p cryptanalysis in different steps. The article describes the possibilities to use the SMT/SAT exemplified with the search for pre-images of hash-function, SMT approaches to formal verifications in modeling, descriptions of existing tools and libraries.

*Key words:* SMT, SAT, theorem, cryptanalysis, Keccak, CNF.

Tab. 1. Fig. 1. Ref.: 7 items.

УДК 621. 3.06

**Закон распределения вероятностей смещений таблиц линейных аппроксимаций случайных подстановок** / К.Е. Лисицкий // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 81 – 89.

Приводится уточнённое доказательство закона распределения вероятностей смещений таблиц линейных аппроксимаций случайных подстановок, а также показывается допустимость аппроксимации этого закона нормальным законом распределения вероятностей.

*Ключевые слова:* случайная подстановка, закон распределения вероятностей, таблица линейных аппроксимаций, маски входа, маски выхода, последовательности из двоичных элементов

Табл. 2. Библиогр.: 10 назв.

УДК 621. 3.06

**Закон розподілу ймовірностей змішень таблиць лінійних апроксимації випадкових підстановок** / *К.Е. Лисицький* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 81 – 89.

Наводиться уточнене доведення закону розподілу ймовірностей змішень таблиць лінійних апроксимацій випадкових підстановок, а також показується допустимість апроксимації цього закону нормальним законом розподілу ймовірностей

*Ключові слова:* випадкова підстановка, закон розподілу ймовірностей, таблиця лінійних апроксимацій, маски входу, маски виходу, послідовності з довічних елементів

Табл. 2. Бібліогр.: 10 назв.

UDC 621. 3.06

**Law of probability distribution of displacements tables of random substitution linear approximations** / *K.E. Lisitzky* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 81 – 89.

We give a refined proof of the law of distribution of the probabilities of bias of tables of linear approximations of random permutations, and also the admissibility of the approximation of this law by the normal law of probability distribution

*Key words:* random substitution, law of probability distribution, table of linear approximations, input masks, exit masks, sequences of binary elements

Table. 2. Ref.: 10 items.

УДК 004.056.5

**Проблема совершения условных транзакций в закрытых Blockchain-системах** / *П.И. Стеценко, Г.З. Халимов* // Радіотехніка : Всеукр. межвед. науч.-техн. сб. – 2017. – Вип. 189. – С. 90 – 99.

Представлена проблема совершения условных транзакций, которая предотвращает совершение пользователями наиболее популярных Blockchain-систем условных транзакций в случае разворачивания закрытого, частного регистра Blockchain. Рассмотрены связи представленной проблемы с другими проблемами и показано, что она не ограничивается технологией Blockchain проекта Ethereum, но и потенциально может распространяться на частные, закрытые регистры Blockchain, использующие механизм достижения консенсуса proof-of-stake. Проблема совершения условных транзакций может привести к потере цифровых активов или атакам двойной траты. Возможным способом предотвращения возникновения данной проблемы может быть создание смарт-контрактов вместо использования обычных транзакций, но это добавляет сложности и применимо только для систем с Тьюринг-полным языком программирования.

Ил. 2. Библиогр.: 22 назв.

УДК 004.056.5

**Проблема здійснення умовних транзакцій в закритих Blockchain-системах** / *П.І. Стеценко, Г.З. Халімов* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 81 – 89.

Представлено проблему здійснення умовних транзакцій, яка запобігає вчиненню користувачами найбільш популярних Blockchain-систем умовних транзакцій в разі розгортання закритого, приватного регістра Blockchain. Розглянуто зв'язки представленої проблеми з іншими проблемами і показано, що вона не обмежується технологією Blockchain проекту Ethereum, але потенційно може поширюватися і на приватні, закриті регістри Blockchain, що використовують механізм досягнення консенсусу proof-of-stake. Проблема здійснення умовних транзакцій може призвести до втрати цифрових активів або атакам подвійної витрати. Можливим засобом запобігання виникненню даної проблеми може бути створення смарт-контрактів замість використання звичайних транзакцій, але це додає складності і може бути застосовано тільки для систем з Тьюринг-повною мовою програмування.

Лл. 2. Бібліогр.: 22 назв.

UDC 004.056.5

**The problem of performing conditional transactions in private Blockchain-systems** / *P.I. Stetsenko, G.Z. Khalimov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 81 – 89.

The problem of performing conditional transactions is presented. This problem prevents users of the most popular Blockchain-systems from performing conditional transactions in the closed, private Blockchain

ledgers. The paper discusses the links of the presented problem with other problems and shows that it is not limited to the Ethereum Blockchain technology, but it can potentially extend to the closed, private Blockchain ledgers which use proof-of-stake consensus mechanism. The problem of performing conditional transactions can lead to the loss of digital assets or double-spending attacks. A possible way to prevent this problem is to create smart-contracts instead of using usual transactions, but this will add complexity and is only applicable to systems with the Turing-complete programming language.

Fig. 2. Ref.: 22 items.

УДК 621.3.06

**Постквантовый малоресурсный симметричный блочный шифр «Кипарис»** / М.Ю. Родинко, Р.В. Олейников // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 100– 107.

Предложен постквантовый малоресурсный симметричный блочный шифр «Кипарис». Алгоритм шифрования основан на сети Фейстеля, в качестве цикловой функции используется ARX-преобразование. Блочный шифр «Кипарис» обеспечивает высокий уровень криптографической стойкости против переборных атак (поддерживает длину ключа 256 и 512 бит). По показателям быстродействия на различных программно-аппаратных платформах предложенный шифр «Кипарис» значительно превышает блочный шифр AES (в 2,5-3 раза). Блочный шифр имеет компактную реализацию, которая не требует использования таблиц предвычислений.

Табл. 4. Ил. 3. Библиогр: 9 назв.

УДК 621.3.06

**Постквантовый малоресурсный симметричный блочный шифр «Кипарис»** / М.Ю. Родинко, Р.В. Олейников // Радиотехника : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 100– 107.

Запропонований постквантовый малоресурсный симметричный блочный шифр «Кипарис». Алгоритм шифрування заснований на мережі Фейстеля, у якості циклової функції використовується ARX-перетворення. Блочний шифр «Кипарис» забезпечує високий рівень криптографічної стійкості проти перебірних атак (підтримує довжину ключа 256 та 512 біт). За показниками швидкодії на різних програмно-апаратних платформах запропонований шифр «Кипарис» значно перевищує блочний шифр AES (у 2,5-3 рази). Блочний шифр має компактну реалізацію, яка не потребує використання таблиць передобчислень.

Табл. 4. Іл. 3. Бібліогр: 9 назв.

UDC 621.3.06

**Post- quantum lightweight symmetric block cipher “Cypress”** / M.Yu. Rodinko, R.V. Oliynykov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 100– 107.

The post-quantum lightweight block cipher “Cypress” is proposed. The encryption algorithm is based on the Feistel network, an ARX-transformation is used as a round function. The block cipher “Cypress” provides a high level of cryptographic strength against exhaustive search attacks (it supports 256 and 512 bits key length). In terms of performance on various hardware and software platforms the proposed cipher “Cypress” significantly exceeds the AES block cipher (2.5-3 times). This block cipher has a compact implementation that does not require the use of pre-calculation tables.

4 tab. 3 fig. Ref.: 9 items.

УДК 004.056.55

**Использование технологий параллельных вычислений в графических процессорах для генераторов потокового шифрования** / Н.А. Полуяненко, А.В. Потий // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 108 – 114.

Рассмотрена возможность переноса части вычислительного процесса с центрального процессора на графический процессор с помощью программно-аппаратной платформы для организации параллельных вычислений на GPU NVIDIA CUDA. Проведено сравнение производительности генерации регистрами сдвига с нелинейной обратной связью на CPU и GPU.

Табл. 2. Ил. 5. Библиогр.: 16 назв.

УДК 004.056.55

**Використання технологій паралельних обчислювань у графічних процесорах для генераторів потокового шифрування** / М.О. Полуяненко, О.В. Потій // Радиотехника : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 108 – 114.

Розглянуто можливість переносу частини обчислювального процесу з центрального процесору до графічного процесору за допомогою програмно-апаратної платформи для організації паралельних обчислювань на GPU NVIDIA CUDA. Проведено порівняння швидкодії генерування регістрами зсуву з нелінійним зворотнім зв'язком у CPU та у GPU.

Табл. 2. Іл. 5. Бібліогр.: 16 назв.

UDC 004.056.55

**Using parallel computing technologies in graphics processors for stream cipher generators /**

*N. Poluyanenko, O. Potii // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 108 – 114.*

The possibility of transferring a part of the computational process from the central processing unit to the graphics processing unit with help of software platform, using of technology in organization of concurrent computing with GPU NVIDIA CUDA is considered. Comparison of performance of the nonlinear feedback shift registers generation on CPU and GPU is carried out.

2 tab. 5 fig. Ref.: 16 items.

УДК 003.026:004.056

**Анализ потенциальных постквантовых механизмов электронных подписей на основе хеш-функций / Ю.И. Горбенко, Т.В. Мельник., И.Д. Горбенко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 115 – 131.**

Приводятся результаты анализа электронных подписей с одноразовыми ключами для пост квантового периода. Обосновываются требования, приводится усовершенствованный механизм электронной подписи по критериям пространственной сложности ключей и подписей. Предлагается модель нарушителя и угроз. Обосновываются основные виды атак на электронную подпись с одноразовыми ключами. Приводятся основные полученные результаты соотношения оценки сложности пост квантового криптоанализа. Даются основные рекомендации и основные сферы использования электронной подписи в пост квантовом периоде.

Табл. 8. Библиогр.: 15 назв.

УДК 003.026:004.056

**Аналіз потенційних постквантових механізмів електронних підписів на основі геш-функцій / Ю.І. Горбенко, Т.В. Мельник., І.Д. Горбенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 115 – 131.**

Наводяться результати аналізу електронних підписів з одноразовими ключами для постквантового періоду. Обґрунтовуються вимоги та наводиться удосконалений механізм електронного підпису по критеріям просторової складності ключів та підписів. Пропонується модель порушника та загроз. Обґрунтовуються основні види атак на електронний підпис з одноразовими ключами. Наводяться основні отримані співвідношення оцінки складності постквантового криптоаналізу. Даються основні рекомендації та основні сфери використання електронного підпису в постквантовому періоді.

Табл. 8. Бібліогр.: 15 назв.

UDC 003.026:004.056

**Analysis of potential post-quantum mechanisms of electronic signatures based on hash functions / Yu.I. Gorbenko, T.V. Melnik., I.D. Gorbenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 115 – 131.**

The results of the analysis of electronic signatures with one-time keys for the post-quantum period are given. The requirements are justified and an improved mechanism of electronic signature is presented for the criteria of spatial complexity of keys and signatures. A model of the violator and threats is proposed. The main types of attacks on the electronic signature with one-time keys are substantiated. The main relations of the post-quantum cryptanalysis complexity estimation are presented. The main recommendations and the main spheres of using the electronic signature in the post-quantum period are given.

8 tab. Ref.: 15 items.

**РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ  
RADIO ENGINEERING AND TELECOMMUNICATION SYSTEMS AND NETWORKS**

УДК 621.396.967.2

**Синтез и анализ оптимального обнаружителя сигналов запроса в самолетных ответчиках**

**вторичных систем наблюдения** / *И.И. Обод, И.В. Свид, И.А. Штых* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 132 – 135.

Синтезирована структура оптимального по критерию Неймана - Пирсона обнаружителя сигналов запроса в самолетных ответчиках с несколькими антенными системами приема вторичных систем наблюдения воздушного пространства и приведен анализ качества обнаружения. Показано, что реализация совместной обработки сигналов запроса всех пространственно разделенных каналов самолетного ответчика приводит к повышению показателей качества обнаружения сигналов запроса.

*Ключевые слова:* системы наблюдения, оптимальный обнаружитель сигналов, сигнал запроса.

Ил. 2. Библиогр. 5 назв.

УДК 621.396.967.2

**Синтез та аналіз оптимального виявлювача сигналів запиту у літакових відповідачах вторинних систем спостереження** / *И.И. Обод, И.В. Свид, И.А. Штых* // Радиотехника : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вып. 189. – С. 132 – 135.

Синтезовано структуру оптимального за критерієм Неймана - Пирсона виявлювача сигналів запиту у літакових відповідачах з декількома антенними системами прийому вторинних систем спостереження повітряного простору та наведено аналіз якості виявлення. Показано, що реалізація сумісної обробки сигналів запиту усіх просторово розділених каналів літакового відповідача призводить до підвищення показників якості виявлення сигналів запиту.

*Ключові слова:* системи спостереження, оптимальний виявлювач сигналів, сигнал запиту.

Іл.2. Бібліогр.: 5 назв.

UDC 621.396.967.2

**Synthesis and analysis of request signals optimal detector in aircraft responders of secondary observation systems** / *I.I. Obod, I.V. Svyd, I.A. Shtyh* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №188. – P. 132 – 135.

The structure of the detector optimized for the Neumann - Pearson criterion of the request signals in aircraft transponders with several antenna systems for receiving secondary airspace surveillance systems was synthesized and the analysis of the detection quality was carried out. It was shown that implementation of joint processing of the request signals of all spatially separated channels of the aircraft transponder resulted in an improvement in the quality of the request signals detection.

*Key words:* observation systems, optimal signal detector, request signal.

Fig. 2. Ref.: 5 items.

УДК 551.501.8:621.396.96

**Методические погрешности измерения метеовеличин при корреляционной обработке сигналов систем радиоакустического зондирования. Сообщение 2** / *В.М.Карташов, С.И.Бабкин, Е.Г.Толстых* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 136 – 140.

Проведена оцінка методических погрешностей вимірювання вологості повітря, що виникають за рахунок априорної неопределенності висотного розподілу інших метеорологічних величин. Оцінено їх вплив при реєстрації вертикальних профілів вимірюваної метеорологічної величини з використанням кореляційної обробки прийнятих сигналів систем радиоакустического зондирования. Показано, що при произвольном выборе пары зондирующих звуковых частот методическая погрешность измерения относительной влажности даже при термической турбулентности может достигать 100%. Влияние ветра и рефракционных эффектов звуковых волн на формирование методической погрешности измерения можно снизить рациональным выбором технических параметров антенных устройств зондирующей системы.

Библиограф.: 12 назв.

УДК 551.501.8:621.396.96

**Методичні похибки вимірювання метеовеличин при кореляційній обробці сигналів систем радиоакустического зондування. Повідомлення 2** / *В.М. Карташов, С.И. Бабкин, Е.Г. Толстых* // Радиотехника : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вып. 189. – С. 136 – 140.

Проведено оцінку методических похибок вимірювання вологості повітря, що виникають за рахунок априорної невизначеності висотного розподілу інших метеорологічних величин. Оцінено їх вплив при реєстрації вертикальних профілів вимірюваної метеорологічної величини з використанням кореляційної обробки прийнятих сигналів систем радиоакустического зондування. Показано, що при довільному виборі пари зондирующих звуковых частот методична похибка вимірювання відносної

вологості навіть при термічній турбулентності може досягати 100%. Вплив вітру та рефракційних ефектів звукових хвиль на формування методичної похибки вимірювання можна знизити раціональним вибором технічних параметрів антенних пристроїв зондуючої системи.

Бібліограф.: 12 назв.

UDC 551.501.8:621.396.96

**Methodical errors in meteorological measurements during correlation processing of signals from radio acoustic sensing systems. Communication 2** / V.M. Kartashov, S.I. Babkin, E.G. Tolstykh // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 136 – 140.

Methodological errors estimation of the air humidity measurement arising from the a priori uncertainty of other meteorological parameters altitude distribution is made. Their influence in recording vertical profiles of the measured meteorological value is estimated using correlative processing of the received signals of radio acoustic sensing systems. It is shown that for an arbitrary choice of a pair of sounding audio frequencies, the methodical error of measuring the relative humidity can reach 100% even with a thermal turbulence. The influence of a wind and sounding wave refractive effects on the formation of the methodical measurement error can be reduced by rational selecting technical parameters of the sounding system's antenna arrangement.

Ref.: 12 items.

УДК 621.396.9: 551.508.855

**Оценка параметров спектров рассеянных сигналов в РЛС вертикального зондирования атмосферы** / В.Н. Олейников, С.В. Дорошенко, В.Д. Пшеничный // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 141 – 147.

Рассмотрены особенности методов оценки параметров рассеянных сигналов в радиолокационных станциях вертикального зондирования атмосферы. На основе экспериментальных результатов зондирования атмосферы предложена модель рассеянных сигналов. Методом имитационного моделирования исследованы оценки точности измерения скорости ветра, получаемые различными методами параметризации спектров. Предложены методы снижения смещения оценок моментов спектра мощности рассеянного сигнала за счёт отражений от земной поверхности и краевых эффектов при параметризации спектров.

Ил. 8. Библиогр.: 8 назв.

УДК 621.396.9: 551.508.855

**Оцінка параметрів спектрів розсіяних сигналів в РЛС вертикального зондування атмосфери** / В.М. Олейніков, С.В. Дорошенко, В.Д. Пшеничний // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 141 – 147.

Розглянуто особливості методів оцінки параметрів розсіяних сигналів в радіолокаційних станціях вертикального зондування атмосфери. На основі експериментальних результатів зондування атмосфери, запропонована модель розсіяних сигналів. Методом імітаційного моделювання досліджено оцінки точності вимірювання швидкості вітру, що одержані різними методами параметризації спектрів. Запропоновано методи зниження зміщення оцінок моментів спектра потужності розсіяного сигналу за рахунок віддзеркалень від земної поверхні і крайових ефектів при параметризації спектрів.

Л. 8. Бібліогр.: 8 назв.

UDC 621.396.9: 551.508.855

**Estimation of parameters of the scattered signals spectra in the radar of vertical sounding of atmosphere** / V.M. Oleynikov, S.V. Dorochenko, V.D. Pshenichniy // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 141 – 147.

Features of methods for estimating parameters of scattered signals in radar stations of vertical atmospheric sounding are considered. Based on the experimental results of sounding the atmosphere, a model of the scattered signals is proposed. Estimation of the accuracy of the wind speed measurement, obtained by various methods of spectra parametrization, is investigated using imitation modeling. Methods are proposed for reducing the shift in estimates of the moments of the spectrum of the scattered signal power due to reflections from the earth's surface and edge effects in the parametrization of the spectra.

8 fig. Ref.: 8 items.

УДК 621.396.677.49

**Модель выявления и устранения уязвимостей в программно-конфигурируемых сетях связи на основе аппарата марковских процессов / Ю.Ю. Коляденко, И.Г. Лукинов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 188. – С. 148 – 154.**

Разработана модель выявления и устранения уязвимостей в программно-конфигурируемых сетях связи на основе аппарата марковских процессов. С помощью данной модели, зная интенсивности потоков, можно в реальном масштабе времени моделировать процессы поступления заявок на обнаружение уязвимостей.

Ил.4. Библиогр.: 5 назв.

УДК 621.396.677.49

**Модель виявлення і усунення вразливостей в програмно-конфігурованих мережах зв'язку на основі апарату марківських процесів / Ю.Ю. Коляденко, І.Г. Лукинов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 148 – 154.**

Розроблено модель виявлення та усунення вразливостей в програмно-конфігурованих мережах зв'язку на основі апарату марківських процесів. За допомогою даної моделі, знаючи інтенсивності потоків, можна в реальному масштабі часу моделювати процеси надходження заявок на виявлення вразливостей.

Л. 4. Бібліогр.: 5 назв.

UDC 621.396.677.49

**Model for identifying and eliminating vulnerabilities in software-configurable communication networks based on the apparatus of Markov processes / Y. Kolyadenko, I. Lukinov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 148 – 154.**

A model for identifying and eliminating vulnerabilities in software-configurable communication networks based on the apparatus of Markov processes is developed. Using this model, knowing the intensity of the flows, it is possible to simulate the processes of receipt of applications for the vulnerabilities detection in real time.

4 fig. Ref.: 5 items.

УДК 551.5

**О проблеме астероидно-кометной опасности / А.А. Глущенко, Е.А. Медведев, Д.Ю. Горелов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 155 – 161.**

Рассчитана вероятность столкновения гипотетических родительских тел метеорных потоков и ассоциаций каталога ХНУРЭ (5160 орбит) с Землей, учитывая изменения элементов орбиты космического тела в ходе его эволюции. Показано, что большинство самых опасных потоков имеют орбиты астероидного типа, а их потенциальные родительские тела принадлежат астероидам группы Атена.

Ил. 9. Библиогр.: 6 назв.

УДК 551.5

**Про проблему астероїдно-кометної небезпеки / А.О. Глущенко, Є.О. Медведєв, Д.Ю. Горелов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 155 – 161.**

Розраховано вірогідність зіткнення гіпотетичних батьківських тіл метеорних потоків та асоціацій каталогу ХНУРЕ (5160 орбіт) із Землею, що враховує зміни в параметрах орбіти космічного тіла в ході його еволюції. Показано, що більшість найнебезпечніших потоків мають орбіти астероїдного типу, а їх потенціальні батьківські тіла належать астероїдам групи Атена.

Л. 9. Бібліогр.: 6 назв.

UDC 551.5

**On the problem of asteroid-comet hazard / A.A. Glushenko, E.A. Medvedev, D.Y. Gorelov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 155 – 161.**

The probability of collision of hypothetical parent bodies of meteor streams and associations from the KNURE (5160 orbits) catalog with the Earth, taking into account changes in the orbital elements of the cosmic body during its evolution, is calculated. It is shown that most of the most dangerous streams have orbits of an asteroid type, and their potential parental bodies belong to the Aten asteroids.

9 fig. Ref.: 6 items.

**ФИЗИКА ПРИБОРОВ, ЭЛЕМЕНТОВ И СИСТЕМ**  
**PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS**

УДК 539.27

**Распределение плотности потока фотонов в дифракционной картине от одной и двух параллельных щелей** / *А.В. Безуглый, А.М. Петченко* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 162 – 165.

Предлагается квантовомеханическая модель явления дифракции света на одной и двух щелях в бесконечно тонком металлическом экране. Из предположения о том, что фотоны, проходя через щели взаимодействуют с электронами вещества путем упругого столкновения, получено распределение интенсивности света в дифракционной картине для случаев дифракции частиц на одной и двух щелях.

Ил. 2. Библиогр.: 8 назв.

УДК 539.27

**Розподіл густини потоку фотонів в дифракційній картині від однієї і двох паралельних щілин** / *А.В. Безуглий, О.М. Петченко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 162 – 165.

Пропонується квантовомеханічна модель явища дифракції світла на двох щілинах в нескінченно тонкому металевому екрані. З припущення про те, що фотони, проходячи через щілини взаємодіють з електронами речовини шляхом пружного зіткнення, одержано розподіл інтенсивності світла в дифракційній картині для випадків дифракції частинок на одній і двох щілинах.

Л. 2. Бібліогр.: 8 назв.

UDC 539.27

**Distribution of the flux of fotons in the diffraction pattern from one and two parallel slits** / *A.V. Besougly, A.M. Petchenko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 162 – 165.

The paper proposes a quantum mechanical model of the phenomenon of light diffraction on one and two slits in an infinitely thin metal screen. Based on the assumption that the photons passing through the slits interact with the electrons of the matter through elastic collisions, the resulting distribution of light intensity in the diffraction pattern for the cases of diffraction of particles in one and two cracks was obtained.

2 fig. Ref.: 8 items.

УДК 535.015

**Определение зависимости характеристик фотонной запрещенной зоны от показателя преломления материала** / *А.И. Филипенко, А.Н. Донсков* // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 166 – 171.

Рассмотрено распространение электромагнитных волн в фотонном кристалле, изготовленном из GaAs. Рассмотрено распространение поперечной составляющей электромагнитного излучения (ТЕ-волны) в диапазоне длин волн от 0,2 до 2 мкм. Определена зависимость характеристик фотонной запрещенной зоны от показателя преломления используемого материал.

Табл. 1. Ил. 10. Библиогр.: 3 назв.

УДК 535.015

**Визначення залежності характеристик фотонної забороненої зони від показника заломлення матеріалу** / *О.І. Филипенко, О.М. Донсков* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 166 – 171.

Розглянуто поширення електромагнітних хвиль в фотонному кристалі, виготовленому з GaAs. Розглянуто поширення поперечної складової електромагнітного випромінювання (ТЕ-хвилі) в діапазоні довжин хвиль від 0,2 до 2 мкм. Визначено залежність характеристик фотонної забороненої зони від показника заломлення матеріал, який використовувався.

Табл. 1. Л. 10. Бібліогр.: 3 назви.

UDC 535.015

**Investigation of the characteristics of the band gap on a refractive index of materials** / *A. I. Filipenko, A.N. Donskov* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 166 – 171.

Propagation of electromagnetic waves in a photonic crystal made of GaAs was considered. The propagation of the transverse component of the electromagnetic radiation (TE wave) in the wavelength range from 0.2 to 2 microns was also considered. Dependence of the characteristics of the photonic band gap on the refractive index of the used material was defined.

1 tab. 10 fig. Ref.: 3 items.

УДК 621.385.6

**Многокомпонентные полупроводниковые структуры в конструкциях солнечных элементов** / О.Ю. Бабыченко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 172 – 178.

Представлены солнечные элементы как основные ячейки альтернативных энергетических систем. Рассмотрены условия и основные конструкции для эффективной работы солнечных элементов. Представлены основные требования к технологиям их получения и математическим моделям.

Ил. 9. Библиогр.: 4 назв.

УДК 621.385.6

**Багатокомпонентні напівпровідникові структури в конструкціях сонячних елементів** / О.Ю. Бабыченко // Радиотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 172 – 178.

Представлені сонячні елементи як основні комірки альтернативних енергетичних систем. Розглянуті умови та основні конструкції для ефективної роботи сонячних елементів. Представлені основні вимоги до технології їх отримання та математичних моделей.

Л. 9. Бібліогр.: 4 назви.

UDC 621.385.6

**Multicomponent semiconductor structures in the construction of solar cells** / O. Babychenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 172 – 178.

The solar cells are presented as the main cells of alternative energy systems. Conditions and basic designs for the effective operation of solar cells are considered. The main requirements for the technologies for their production and mathematical models are presented.

9 fig. Ref.: 4 items.

УДК 62-742

**Применение наземной многопозиционной технологии в управлении воздушным движением** / Ли Хе Пинг // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 179 – 188.

Существующая система управления воздушным движением (УВД) не в состоянии контролировать летательные аппараты, которые взлетают, совершают посадку или перемещаются в аэропорту. Рассмотрены требования аналитической миссии УВД и преимущества использования наземной многопозиционной технологии в УВД. Изучены ключевые проблемы, такие, как режим компоновки станции, подавление многолучевости и определение временной разности. Проведены испытания, результаты которых показывают, что предлагаемый метод является эффективным и надежным.

*Ключевые слова:* управление воздушным движением; наземная многопозиционная технология (мультилатерация); Разница во времени; Точность местоопределения.

Ил. 15. Библиогр.: 4 назв.

УДК 62-742

**Застосування наземної багатопозиційної технології в управлінні повітряним рухом** / Ли Хе Пинг // Радиотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 179 – 188.

Чинна система управління повітряним рухом (УПР) не в змозі контролювати літальні апарати, які піднімаються у повітря, здійснюють посадку або переміщуються в аеропорту. Розглянуто вимоги аналітичної місії УПР та визначено доцільність застосування наземної багатопозиційної технології в УПР. Розглянуто ключові проблеми, такі як режим компоновки станції, подавлення многолучевости та визначення часової різниці. Результати випробувань доводять ефективність і надійність запропонованого методу.

*Ключові слова:* керування повітряним рухом, наземна багатопозиційна технологія (мультілатерація); різниця в часі; точність місцевизначення.

Л. 15. Бібліогр.: 4 назви.

UDC 62-742

**The application of multilateration technology in air traffic control / Li He Ping // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 179 – 188.**

In view of the problem that the existing Air Traffic Control (ATC) system is unable to monitor aircrafts which are taking off, landing or moving in the airport. On the basis of the analyzing mission requirements of ATC and the advantage of the multilateration, this paper introduces the multilateration into the ATC application. And the key problems, such as station layout mode, multipath suppression and time difference extraction, are intensively studied. Several tests have been implemented in an airport, and the results illustrate that the proposed method is effective and reliable.

*Key words:* Air Traffic Control; Multilateration; Time difference; Location precision.

15 fig. Ref.: 4 items.

## СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ SYSTEMS OF TECHNICAL PROTECTION OF INFORMATION

УДК 004.056.53

**Основные направления совершенствования средств акустической разведки / А.Н. Олейников, А.В. Бородавка // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 189 – 194.**

Самым распространенным средством ведения акустической разведки являются узконаправленные микрофоны. Развитие и совершенствование узконаправленных микрофонов можно разделить на три этапа: «акусто-механический» этап, этап аналоговый обработки аудиосигналов и этап цифровой обработки аудиосигналов в средствах дистанционного съема информации. Большое влияние на развитие узконаправленных микрофонов оказала цифровая обработка сигналов. Использование решеток, применяющих алгоритм сверхнаправленности, позволяет поднять индекс направленности на низкой частоте, применяя их в качестве подрешеток в более сложных структурах микрофонных решеток. Полученное преимущество в 6 дБ позволяет получить увеличение дальности разведывательного контакта в два раза.

Табл. 1. Ил. 7. Библиогр.: 4 назв.

УДК 004.056.53

**Основні напрямки вдосконалення засобів акустичної розвідки / А. М. Олейніков, А. В. Бородавка // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2017. – Вип. 189. – С. 189 – 194.**

Найпоширенішим засобом ведення акустичної розвідки є вузькоспрямовані мікрофони. Розвиток та вдосконалення вузькоспрямованих мікрофонів можна поділити на три етапи: «акусто-механічний» етап, етап аналогової обробки аудіосигналів та етап цифрової обробки аудіосигналів в засобах дистанційного зняття інформації. Великий вплив на розвиток вузькоспрямованих мікрофонів здійснила цифрова обробка сигналів. Використання решіток, що застосовують алгоритм зверхспрямованості, дозволяє підвищити індекс спрямованості на низькій частоті, використовуючи їх в якості підрешіток в більш складних мікрофонних решітках. Отримана перевага в 6 дБ дозволяє отримати збільшення дальності розвідувального контакту в два рази.

Табл. 1. Іл. 7. Бібліогр.: 4 назв.

UDC 004.056.53

**The main directions of improving acoustic intelligence devices / A. N. Oleynikov, A. V. Borodavka // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – №189. – P. 189 – 194.**

Directional microphones are the most popular devices for acoustic intelligence. Development and improvement of directional microphones can be divided into three stages: “acousto-mechanical” stage, analog signal processing stage, digital signal processing stage. Digital signal processing has a significant influence on the directional microphones development. If super-directive arrays are using as sub-arrays, directivity index will be increased at low frequencies. Advantage in 6 dB increases distance of recording two times.

1 tab. 7 fig. Ref.: 4 items.

УДК 621.369:534

**Сравнительный анализ перспективных технологий аутентификации пользователей ПК по клавиатурному почерку** / В.А. Алексеев, Д.В. Маслий, Д.Ю. Горелов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2017. – Вып. 189. – С. 195 – 201.

Приведен сравнительный анализ результатов исследований в направлении решения задач аутентификации пользователей ПК по клавиатурному почерку за последние несколько десятилетий с учетом использования распространенных вероятностно-статистических моделей и алгоритмов машинного обучения. Сформулированы главные критерии эффективности построения систем аутентификации, основанных на анализе особенностей клавиатурного почерка.

Табл. 1. Ил. 2. Библиогр.: 9 назв.

УДК 621.369:534

**Порівняльний аналіз перспективних технологій автентифікації користувачів ПК за клавіатурним почерком** / В.О. Алексеев, Д.В. Маслий, Д.Ю. Горелов // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. – 2017. Вип. – 189. – С. 195 – 201.

Наведено порівняльний аналіз результатів досліджень в напрямку вирішення завдань автентифікації користувачів ПК за клавіатурним почерком впродовж останніх десятиліть з урахуванням використання поширених ймовірносно-статистичних моделей і алгоритмів машинного навчання. Сформульовано головні критерії ефективності побудови систем автентифікації, заснованих на аналізі

особливостей клавіатурного почерку.

Табл. 1. Ил. 2. Библиогр.: 9 назв.

UDC 621.369:534

**Comparative analysis of advanced technologies for authenticating users by keystroke dynamics** / V.A. Alekseev, D.V. Masliy, D.Y. Gorelov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2017. – № 189. - P. 195 – 201.

A comparative analysis of research results in the direction of authenticating users by keystroke dynamics over the past few decades with using common probabilistic statistical models and machine learning algorithms is given. The main criteria for the effectiveness of authentication systems based on the analysis of the keystroke dynamics features are formulated.

1 tab. 2 fig. Ref.: 9 items.