ние выборки, полученной при помощи модели с полиномиальными признаками меньше, чем в случае линейной модели – 4,48 против 10,48 соответственно. Аналогичный результат наблюдается и для выборки, полученной при помощи прибора, стандартное отклонение которой равно 12,51.

Таким образом, было показано, что использование инструментов машинного обучения с использованием библиотек языка Python для прогнозирования значений статической твердости по Бринеллю по данным динамического индентирования позволяет устранить грубые ошибки измерения и снизить погрешность косвенного определения твердости в 2 раза и более. При этом в большинстве случаев эта погрешность не превышает 10 HB, что является труднодостижимым результатом при использовании обычных эмпирических зависимостей между динамической и статической твердостью.

Благодарности. Работа выполнена при поддержке БРФФИ. Проект Т23УЗБ-035.

Литература

1. Rudnitsky, V. A., Determining yield strength of metals by microindentation with a spherical tip / V. A. Rudnitsky, A. P. Kren, G. A. Lantsman // Russian Federationn Journal of Nondestructive Testing. – 2019. – V. 55, – P. 162–168.

2. Ben Chaabene, W. Machine learning prediction of mechanical properties of concrete: Critical review / W. Ben Chaabene Construction and Building Materials. – 2020. – T. 260. Elsevier BV. – P. 119889.

3. Крень, А. П. Контроль физико-механических характеристик чугуна прибором ИФМХ-Ч / А. П. Крень, В. А. Рудницкий, Г. А. Ланцман. // Литье и металлургия. – 2019. – №3. – С. 65–69.

УДК 004.056.53

КОМПЛЕКСНАЯ ОЦЕНКА ФУНКЦИОНАЛЬНЫХ СВОЙСТВ АКУСТИЧЕСКИХ СЕЙФОВ ДЛЯ ЗАЩИТЫ СМАРТФОНОВ ОТ НЕСАНКЦИОНИРОВАННОЙ АКТИВАЦИИ

Кудина А. В.[1], Франко Е. П.[1], Денскевич А. Д.[1], Есьман Г. А.[2]

[1]Белорусский государственный университет информатики и радиоэлектроники
[2]Белорусский национальный технический университет
Минск, Республика Беларусь

Аннотация. Представлены результаты расчетов комплексных показателей качества акустических сейфов. Показана диаграмма распределения этих показателей, позволяющая выбрать наиболее оптимальную модель акустического сейфа для смартфона.

Ключевые слова: защита информации, акустические сейфы, технические параметры, комплексные показатели качества.

COMPREHENSIVE ASSESSMENT OF THE FUNCTIONAL PROPERTIES OF ACOUSTIC SAFES TO PROTECT SMARTPHONES FROM UNAUTHORIZED ACTIVATION

Kudina A.[1], Franko E.[1], Dzenskevich A.[1], Esman G.[2]

[1]Belarusian State University of Informatics and Radioelectronics
[2]Belarusian National Technical University
Minsk, Republic of Belarus

Abstract. The results of calculations of complex quality indicators of acoustic safes are presented. A diagram of the distribution of these indicators is shown, which allows you to choose the most optimal model of an acoustic safe for a smartphone.

Key words: information protection, acoustic safes, technical parameters, comprehensive quality indicators.

Адрес для переписки: Денскевич А. Д., ул. Барыкина, 95, г. Червень 223232, Республика Беларусь
e-mail: denskevichad@gmail.com

Введение. Акустические сейфы являются сложными техническими средствами, предназначенными для защиты информации по акустическим каналам и создания защищенной зоны. Применяя направленные акустические волны, они подавляют звуковые колебания и предотвращают несанкционированное прослушивание смартфонов. Основой их работы служат передовые алгоритмы и технологии звуковой обработки, позволяющие фильтровать нежелательные аудиосигналы.

В настоящее время на рынке представлено множество моделей таких сейфов, что затрудняет выбор оптимальной с точки зрения технических характеристик, требуя детального анализа параметров [1].

Основная часть. Для решения данной задачи может быть применен комплексный метод оценки качества изделий, обеспечивающий учет всех принятых во внимание технических характеристик и их численных значений [2, 3]. Комплексный метод оценка предполагает использование комплексных показателей, одним из которых является средневзвешенный арифметический показатель, вычисляемый по установленной математической формуле

$$K_{\text{ариф}} = \sum_{i=1}^{m} \alpha_{\text{Н}i} k_{\text{Н}i}, \quad (1)$$

где $k_{\text{Н}i}$ – нормированный i-й единичный показатель; $\alpha_{\text{Н}i}$ – нормированный коэффициент, характеризующий вес (значимость, важность) i-го единичного показателя; m – количество единичных показателей, принятых во внимание.

Поскольку технические параметры акустических сейфов представлены в различных размерностях, для корректного применения формулы (1) требуется их приведение к безразмерным величинам путем нормировки. Нормировка осуществляется на основании соответствующего выражения

$$K_{\text{Н}i} = \frac{k_i - k_{\text{кр}\,i}}{k_{\text{опт}\,i} - k_{\text{кр}\,i}}, \quad (2)$$

где k_i – исходное значение i-го единичного показателя; $k_{\text{кр}\,i}$ – критическое значение i-го единичного показателя; $k_{\text{опт}\,i}$ – оптимальное значение i-го показателя; $k_{\max\,i}$ – максимальное значение i-го показателя; $k_{\min\,i}$ – минимальное значение i-го показателя.

Исходные значения k_i должны лежат в пределах $k_{\text{кр}\,i} < k_i < k_{\text{опт}\,i}$ или $k_{\text{опт}\,i} < k_i < k_{\text{кр}\,i}$. Коэффициенты значимости $\alpha_{\text{Н}i}$ для формулы (1) должны выбираться таким образом, чтобы обеспечивалось условие

$$\sum_{i=1}^{m} \alpha_{\text{Н}i} = 1, \quad (3)$$

тогда нормированные значения $K_{\text{Н}i}$ будут лежать в пределах $0 < K_{\text{Н}i} < 1$.

В качестве единичных показателей для акустических сейфов были выбраны следующие технические параметры: стоимость, уровень шума, эффективность шумового спектра, продолжительность непрерывной работы, габариты устройства, масса устройства, рабочее напряжение, размер отсека для хранения смартфонов, а также максимальное количество защищаемых смартфонов. Для сравнительного анализа было отобрано 37 моделей акустических сейфов различных производителей.

Для вычисления числовых значений комплексных показателей качества акустических сейфов требуется предварительная подготовка и трансформация исходных данных. Этот процесс включает:

– преобразование параметров, представленных несколькими числовыми значениями, в показатели, выраженные единым числовым значением;

– установление численных значений для параметров, данные по которым не найдены;

– присвоение параметрам коэффициентов значимости;

– выбор оптимальных и критических значений параметров для их нормировки;

– выполнение нормирования коэффициентов значимости.

После выполнения всех преобразований количество параметров увеличилось до 14.

Для присвоения параметрам коэффициентов значимости был использован экспресс-метод, основанный на разделении параметров на группы по важности, каждой из которых присваивались числовые диапазоны, равномерно распределенные друг относительно друга. Таким образом техническим характеристикам были выбраны значения от 1 до 10. Характеристикам были присвоены следующий приоритет: стоимость – 6, уровень шума – 8, эффективность шумового спектра – 9, продолжительность непрерывной работы – 6.5, габариты устройства – 7, масса устройства – 6, рабочее напряжение – 7.5, размер отсека для хранения смартфонов – 7.5 и максимальное количество смартфонов – 8 [4].

Результаты расчетов, проведенные по формуле (1) с учетом выражений (2) и (3), в виде столбиковой диаграммы (рисунок 1).

Результаты расчетов показали, что наилучшие значения комплексных показателей качества наблюдаются у модели ASU-20A (0,624), на втором месте расположена модель ЛАГ-105 (0,617), а третье место заняла модель Чаша-Люкс (0,601). Внешний вид данных моделей представлен на рисунке 2.

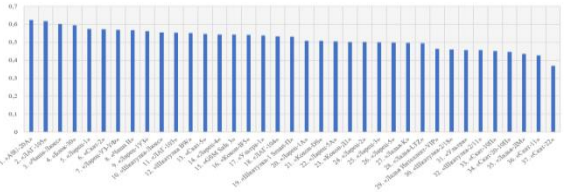

Рисунок 1 – Распределение комплексных показателей качества акустических сейфов

а – *ASU*-20*A*; *б* – ЛАГ-105; *в* – Чаша-Люкс

Рисунок 2 – акустические сейфы

Диаграмма демонстрирует три группы акустических сейфов с близкими значениями показателей внутри каждой группы и значительными различиями между группами: группа 1 (занимающая 1-3 места, с показателями от 0,624 до 0,601); группа 2 (4-19 места, с показателями от 0,595 до 0,530); группа 3 (20-37 места, с показателями от 0,508 до 0,368).

Заключение. Таким образом, комплексная оценка качественных характеристик акустических сейфов, ориентированная на обеспечение защиты смартфонов, позволила провести сравнительный анализ различных моделей. Учитывая технические параметры и их численные значения, удалось определить наилучшую модель акустического сейфа для защиты смартфонов от несанкционированного прослушивания, обеспечивая высокую безопасность данных.

Литература

1. Принципы действия и назначение акустических сейфов [Электронный ресурс]. – Режим доступа: https://www.bargas.ru/info/articles/printsip_deystviya_i_naznachenie_akusticheskikh_seyfov/. – Дата доступа: 21.09.2024.

2. Алефиренко, В. М. Выбор состава технических средств для систем обеспечения безопасности / В. М. Алефиренко // Доклады БГУИР. – 2017. – № 2 (104). – С. 39–44.

3. Алефиренко, В. М. Комплексный анализ технических характеристик блокираторов сотовой связи и беспроводного доступа / В. М. Алефиренко, А. Д. Денскевич, А. М. Асиненко // Журнал «Science Time»: Материалы Междунар. науч.-практ. мероприятий Общества Науки и Творчества за июнь 2022 года / Казань, 2022. – № 6 (102). – С. 5–9.

4. Акустические сейфы для защиты от перехвата конфиденциальной информации [Электронный ресурс]. – Режим доступа: https://detsys.ru/catalog/zashchita_telefonov/. – Дата доступа: 21.09.2024.

УДК 004.9, 519.688

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ КРИПТОМОДУЛЯ С ПРИМЕНЕНИЕМ МИНИМАЛЬНО ИЗБЫТОЧНЫХ МОДУЛЯРНЫХ СИСТЕМ СЧИСЛЕНИЯ ДЛЯ ШИФРОВАНИЯ ДАННЫХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Ломако А. А., Козлова Е. И.

НИУ «Институт прикладной физических проблем имени А. Н. Севченко» БГУ
Минск, Республика Беларусь

Аннотация. На сегодняшний день одним из актуальных направлений в шифровании информации является использование модулярных систем счисления. В работе описываются минимально избыточные модулярные системы счисления и их применение для шифрования изображений, регистрируемых при дистанционном зондировании Земли. На основании экспериментальных вычислений выявлено, что скорость шифрования данных за счет использования параллельных вычислений повышается в 3,8 раза.

Ключевые слова: обработка изображений, параллельные вычисления, беспилотные летательные аппараты, модулярная арифметика.

THE CRYPTOMODULE WITH MINIMALLY REDUNDANT MODULAR NUMBER SYSTEMS EFFECTIVENESS FOR REMOTE SENSING DATA ENCRYPTING

Lamaka A., Kazlova A.

A. N. Sevchenko Institute of Applied Physical Problems of Belarusian State University
Minsk, Republic of Belarus

Abstract. One of the most relevant directions in information encryption is the use of the mathematical apparatus of elliptic curves and modular number arithmetic systems. The paper describes minimally redundant modular number systems and their application to encrypt images recorded during remote sensing. It was revealed after the experimental calculations that the data encryption speed increases by 3.8 times due to the use of parallel computing.

Key words: image processing, parallel computing, unmanned aerial vehicles, modular arithmetic.

Адрес для переписки: Ломако А. А., пр. Независимости, 65, г. Минск 220113, Республика Беларусь
e-mail: remsens@mail.ru

В последнее время получили развитие исследования в области криптографии, направленные на согласование математического аппарата эллиптических кривых и арифметики модулярных систем счисления [1; 2]. Этот подход позволяет разрабатывать высокопроизводительные криптосистемы различного назначения [2]. Одной из областей применения такого криптомодуля может быть шифрование данных, получаемых при дистанционном зондировании Земли (ДЗЗ). При этом шифрование может использоваться как для засекречивания данных космической съемки (в том числе, мульти- или гиперспектральных изображений), так и для обработки видеопотоков данных, передаваемых от беспилотных летательных аппаратов их операторам по радиоканалу. При этом использование особенности модулярных вычислительных систем как архитектурно параллельных в совокупности с характерной для данных ДЗЗ целочисленностью значений в пикселях изображений позволяет существенно увеличить скорость обработки информации. Целью данного исследования стала численная оценка увеличения скорости шифрования изображений за счет использования параллельных вычислений.

Минимально избыточные модулярные системы счисления. Использование в различного рода числовых системах кодовой избыточности позволяет существенно улучшить арифметические и другие свойства таких систем. Для минимально избыточных модулярных систем счисления (МИМСС) отображение, описывающее кодирование, определяется следующим образом:

$$\nu: D \to Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_k}, \qquad (1)$$

где m_1, m_2, …, m_k – модули МИМСС, D – кодируемое множество (прообраз кодового пространства), Z_{M_k} – диапазон таких целых чисел, что набору модулей m_1, m_2, …, m_k числа $X \in Z$ отвечает некий модулярный код (χ_1, χ_2,…, χ_k). При этом мощность диапазона D меньше, чем у диапазона $Z_{\bar{M}_k}$ классической неизбыточной модулярной системы счисления с тем же базисом [2].