



Рис. 2. Схема асимметричного алгоритма шифрования

Производительность: симметричные алгоритмы демонстрируют в 100–1000 раз более высокую скорость обработки данных. Например, AES показывает скорость около 1–2 Гбит/с на современном оборудовании, в то время как RSA 2048-bit – всего 5–10 Мбит/с.

Криптостойкость: асимметричные алгоритмы требуют значительно большей длины ключей для обеспечения сопоставимой стойкости. Эквивалентная стойкость достигается при $\text{AES-128} \approx \text{RSA-3072}$ и $\text{AES-256} \approx \text{RSA-15360}$.

Управление ключами: симметричные алгоритмы требуют безопасного канала для передачи ключа, что создает проблему $n(n-1)/2$ ключей для n пользователей. Асимметричные алгоритмы решают эту проблему через открытые ключи.

В реальных условиях оба типа алгоритмов используются совместно в гибридных системах: симметричное шифрование для передачи сеансового ключа и симметричное шифрование для основного обмена данными.

Такое сочетание позволяет использовать преимущества обоих подходов, таких как высокую скорость симметричного шифрования и безопасное распределение ключей асимметричных методов.

Сравнительный анализ показывает комплементарный характер двух классов алгоритмов. Оптимальный выбор зависит от конкретных требований к безопасности, производительности и масштабируемости системы. Современные реализации должны учитывать необходимость гибридного подхода для достижения максимальной эффективности защиты.

Литература

1. Тимофеев, А. М. Криптографическая защита информации : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2020. – 112 с.
2. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. – М. : СОЛОН-Пресс, 2009. – 256 с.

ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ UI-ДИЗАЙНА ДЛЯ МЕДИЦИНСКИХ ПРИЛОЖЕНИЙ НА ПРИМЕРЕ ПРОГРАММНОГО СРЕДСТВА ДИАГНОСТИКИ И КОРРЕКЦИИ ХРОНИЧЕСКОГО ПОСТИНСУЛЬТНОГО БОЛЕВОГО СИНДРОМА

А. А. Кушнер, Е. М. Косарева

Белорусский государственный университет информатики
и радиоэлектроники, г. Минск

Рассмотрены принципы проектирования компонентов пользовательских интерфейсов медицинских приложений на примере диагностического приложения для врачей-неврологов.

Ключевые слова: пользовательский интерфейс, медицинские диагностические системы, юзабилити-инжиниринг.

UI DESIGN PRINCIPLES FOR MEDICAL APPLICATIONS USING THE EXAMPLE OF A SOFTWARE TOOL FOR DIAGNOSTICS AND CORRECTION OF CHRONIC POST-STROKE PAIN SYNDROME

A. A. Kushner, E. M. Kosareva

Belarusian state university of informatics and radioelectronics, Minsk

This article examines the design principles of user interface components for medical applications using the example of a diagnostic application for neurologists.

Keywords: user interface, medical diagnostic systems, usability engineering.

Тенденция к цифровизации, охватывающая все отрасли функционирования государства, оказывает существенное влияние и на медицину. К примеру, в сфере неврологии наблюдается переход от бумажной фиксации к применению автоматизированных систем для сбора анамнеза и проведения тестирования с целью оценки различных показателей при диагностике неврологических синдромов у пациентов.

В работе с постинсультными пациентами одним из аспектов является периодическая диагностика болевого синдрома. Предлагаемым подходом к решению данной задачи является веб-приложение «PainMetrika». Оно позволяет осуществлять оценку болевого синдрома неврологических пациентов на основе опросов.

Цветовая схема интерфейса разработана с целью обеспечения визуальной гармонии, эмоционального комфорта пользователей. Оттенок синего (#2E67F6) был выбран в качестве основного цвета интерфейса исходя из принципов эргономики восприятия и эмоциональной нейтральности. Дополнительные синие оттенки (#2E7CF6, #5391F2, #D4E6FF) используются для создания глубины интерфейса и выделения функциональных элементов без чрезмерной визуальной нагрузки.

Нейтральная палитра серых цветов (от #262626 до #F9F9F9) применяется для обеспечения читаемости текстовой информации и визуального баланса. Более темные оттенки применяются для отображения текста, при этом достигается уровень контрастности AAA, что свидетельствует о соблюдении принципа доступности [1]. Более светлые оттенки серого служат фоновыми тонами, формируя структурированное визуальное пространство. В качестве цвета фона используется белый цвет (#FFFFFF).

Для отображения предупреждений и сообщений об ошибках используется оттенок красного (#E43D3D), который обеспечивает визуальное выделение и легкое считывание информации.

Цветовая схема интерфейса представлена на рис. 1.

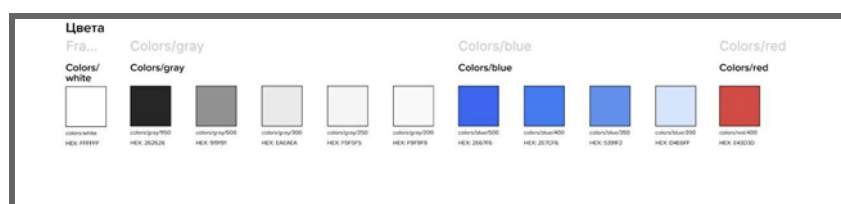


Рис. 1. Цветовая схема интерфейса

В качестве основного шрифта интерфейса выбран *Proxima Nova* [2], отличающийся высокой читаемостью и нейтральным визуальным стилем. Благодаря сбалансированным пропорциям и оптимальному межбуквенному интервалу шрифт снижает зрительную нагрузку, повышая комфорт при длительном использовании приложения. В качестве базового размера шрифта был выбран основной текст (*p*) размером в 12 *pt*; остальные размеры были вычислены на основании *Major third* с множителем 1.25.

Пример экрана приложения представлен на рис. 2.

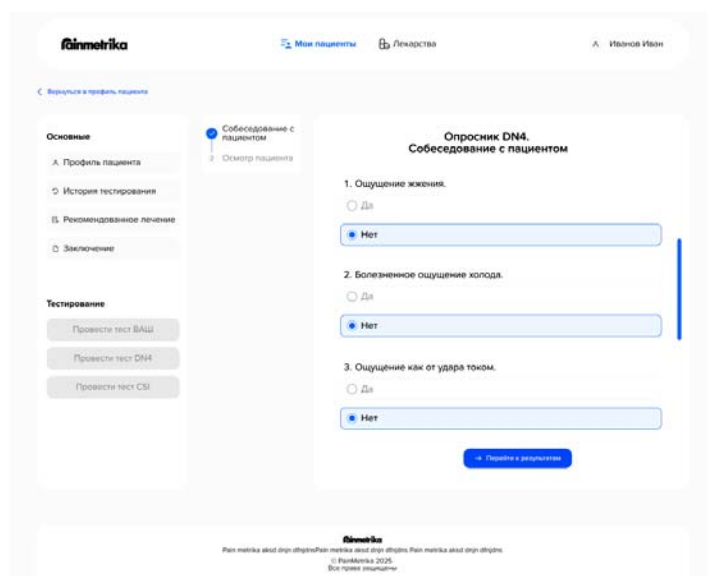


Рис. 2. Пример экрана прохождения теста

Описанные принципы лежат в основе проектирования *UI* более двадцати экранов. Для оценки качества полученного решения планируется апробировать результаты путем проведения моделируемого тестирования и тестирования доступности.

Литература

1. WCAG 2. – URL: <https://www.w3.org/WAI/standards-guidelines/wcag/> (дата обращения: 10.10.2025).
2. Proxima nova. – URL: <https://fonts-online.ru/fonts/proxima-nova> (дата обращения: 10.10.2025).

МОБИЛЬНОЕ ПРИЛОЖЕНИЕ ДЛЯ ОПРЕДЕЛЕНИЯ ЗАБОЛЕВАНИЙ КОЖИ ЧЕЛОВЕКА С ИСПОЛЬЗОВАНИЕМ ЛАМПЫ ВУДА

Ю. А. Лазарева, Ю. А. Скудняков

Белорусский государственный университет информатики
и радиоэлектроники, г. Минск

Данная работа посвящена актуальной теме – автоматизации проведения диагностики кожных заболеваний человека. Целью выполнения работы является разработка мобильного приложения, которое работает на основе созданных графовых, структурно-функциональной и алгоритмической моделей для проведения диагностики кожных заболеваний человека. Мобильное приложение разработано при использовании фреймворка *ReactNative* с интеграцией библиотеки *OpenCV*, которая работает на основе компьютер-