Клинические аудиометры представляют собой автоматизированные двухканальные приборы, благодаря которым оценивается состояние и качество слуха по костному и воздушному звукопроведению. Клинический аудиометр дает возможность обнаруживать пороги слышимости и проводить дифференциальную диагностику в свободном поле. Если использовать такой аппарат, можно выявить нарушения уже на раннем этапе.

Одна из основных отличительных особенностей поликлинических аудиометров, которые также называются диагностическими, – это расширенные возможности диагностики. Устройство используется не только для анализа слуха по костной и воздушной проводимости за счет измерения порогов слышимости, но и для оценки качества речи, ее разборчивости. Посредством поликлинических аудиометров проводится анализ параметров (индекс чувствительности к приростам интенсивности, порог восприятия силы звука).

В основе принципа действия тонального аудиометра лежит подача звукового тестового тонального сигнала с известными параметрами (частота, уровень звукового давления) в наружный слуховой проход исследуемого уха.

*УДК 621.317.799:621.382*

## МАТРИЧНЫЙ МОДУЛЬ КОММУТАЦИИ

**Лисенков Б.Н., Гришковец И.А.**

*ОАО «МНИПИ»*
*Минск, Республика Беларусь*

**Аннотация.** Рассмотрена конструкция матричного модуля коммутации. Приведены достигнутые метрологические параметры модуля.
**Ключевые слова:** матричный коммутатор, модуль коммутации, метрологические параметры.

## THE MATRIX SWITCHING MODULE

**Lisenkov B., Grishkovets I.**

*MNIPI*
*Minsk, Belarus*

**Annotation.** The design of the switching matrix module is considered. Metrological parameters of the switch are achieved and given.
**Keywords:** the matrix switcher, the switching module, metrological parameters.

*Адрес для переписки: Лисенков Б.Н., ул. Якуба Коласа 73, г. Минск 220113, Республика Беларусь*
*e-mail: lisenkovmnipi@tut.by*

Модуль коммутации выполнен на герконных реле, включающих основной и вспомогательный герконы. Реле установлены на печатной плате в узлах матрицы коммутации объемом 4×12 на пересечениях линий (A, B, C, D) и колонок (1–12) матрицы. Для повышения технологичности и снижения затрат, выходные порты модуля, связанные с колонками матрицы, выполнены на клеммниках разъемных (вилка на плату). Предусмотрена возможность расширения объема матрицы коммутации путем объединения нескольких модулей.

Для уменьшения паразитных наводок, каждая линия матрицы содержит дополнительное реле, которое служит для отключения остальных реле этой линии, при условии, что ни один из ее узлов не должен быть замкнут.

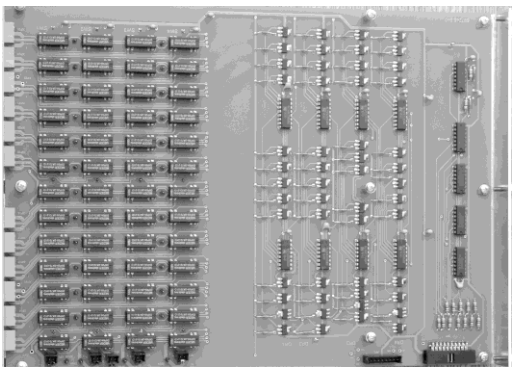
Дальнейшее снижение паразитных наводок и утечек в цепи коммутируемого сигнала достигнуто за счет топологии платы коммутации. Практически вся цепь, по которой распространяется коммутируемый сигнал на плате коммутации, охвачена «охранной» поверхностью, являющейся эквипотенциальной по отношению к коммутируемому сигналу. Источником эквипотенциального сигнала служит измеритель ВАХ, подключенный к линиям (входам) матрицы [1].

Кроме того, линии и колонки матрицы экранированы с помощью «охранной» поверхности соответствующей конфигурации, расположенной по обе стороны платы коммутации на экранирующих платах.

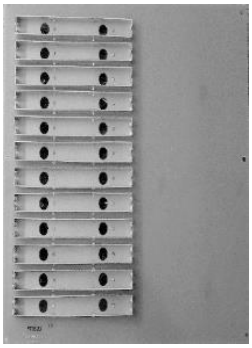
На рис. 1, *а* показано расположение элементов на плате коммутации, содержащей матрицу коммутации и драйверы для управления этой матрицей. На рис. 1, *б* и 1, *в* показана конфигурация и конструктивное исполнение «охранной» поверхности на платах, экранирующих матрицу со стороны колонок и со стороны линий, соответственно.

Проводящие полоски на экранирующих платах подключают к проводнику «охранной» поверхности на плате коммутации в нескольких точках с помощью одноштырьковых разъемов.

Эквипотенциальный сигнал «охраны» коммутируют в узлах матрицы одновременно с основным сигналом с помощью вспомогательного геркона.



а



б в

Рисунок 1 – Плата коммутации (*а*) и платы, экранирующие матрицу со стороны колонок (*б*) и со стороны линий (*в*)

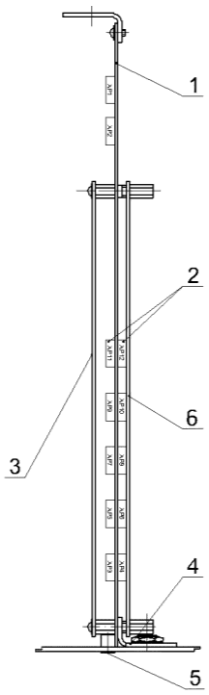
На рис. 2 представлен сборочный чертеж модуля коммутации в составе платы коммутации, двух экранирующих плат и кронштейна для крепления модуля в базовом блоке.

В результате экспериментальных исследований установлено, что искажение коммутируемого сигнала зависит от конфигурации замкнутых узлов в матрице коммутации. Чем больше номер подключенного порта, то есть номер колонки, замкнутой с соответствующей линией в матрице коммутации, – тем больше длина пути сигнала от входа модуля по этой линии до подключенного выходного порта и тем сильнее сказывается влияние паразитных факторов.

Исследования статических параметров модуля были проведены в автоматическом режиме с помощью четырехканального измерителя ВАХ [1, 2].

Исследования динамических параметров выполнены вручную с помощью соответствующих генераторов испытательного сигнала и осциллографа с временем нарастания ПХ 0,35 нс.

Экспериментальные исследования функциональных возможностей матрицы коммутации (объемом 4×48) при измерении емкости проведены с помощью измерителя иммитанса Е7-30. Показана возможность измерения емкостей в диапазоне от 10 пФ до 1000 пФ по схеме 2Т и по схеме 4Т независимо от конфигурации матрицы.




*1* – плата коммутации, *2* – разъемы расширения матрицы коммутации, *3*, *6* – платы экранирующие, *4* – кронштейн, *5* – выходные порты (клеммники разъемные)

Рисунок 2 – Внешний вид модуля коммутации

На частотах 1 и 10 кГц длина соединительного кабеля практически не оказывает влияния на результат измерения емкости.

На частоте 100 кГц погрешность измерения емкости 10 пФ составляет 0,1 пФ (1 %) при длине кабеля 3 м, 0,08 пФ (0,8 %) при длине кабеля 2 м и 0,05 пФ (0,5 %) при длине кабеля 1 м.

Найденные значения метрологических параметров коммутатора представлены в табл. 1.

Таблица 1. Метрологические параметры разработанного матричного коммутатора

| | |
|---|---|
| Ток смещения | ≤ 10 рА (≤ $10^{12}$ А) |
| Сопротивление изоляции | ≥ 1 ТОм (≥ $10^{12}$ Ом) |
| Сопротивление замкнутого канала (в начале срока эксплуатации) | ≤ 0,4 Ом |
| Напряжение смещения (через 3 минуты после замыкания геркона) | ≤ 0,05 мВ |
| Полоса пропускания (Коэффициент передачи на частоте 10 МГц не менее 0,8) | > 10 МГц |
| Время нарастания ПХ (нагрузка 50 Ом) | ≤ 30 нс |
| Погрешность измерения емкости 10 пФ измерителем Е7-30 через коммутатор в диапазоне частот от 1 кГц до 100 кГц | 1 % |

Из табл. следует, что численные значения верхней граничной частоты полосы пропускания АЧХ $f_В$ и времени нарастания ПХ $\tau_н$, найденные экспериментально, согласуются друг с другом согласно известному соотношению ($f_В \approx 350/\tau_н$, где частота $f_В$ выражена в мегагерцах, а время $\tau_н$ – в наносекундах). Измерение емкости с применением матричного коммутатора целесообразно вести на частотах до 100 кГц.

Представленный матричный модуль коммутации разработан для автоматизированного измерительного комплекса в рамках ГНТП «Эталоны и научные приборы» [1].

**Литература**

1. Лисенков, Б. Н. Измерительный комплекс на основе матричного коммутатора / Б. Н. Лисенков, Н. В. Грицев // Приборостроение-2019 : матерериалы 12 международной науч.-техн. конф., 18–20 ноября 2019 г., Минск, Белорус. нац. техн. ун-т / редкол. : О. К. Гусев [и др.]. – Минск : БНТУ, 2019. – С. 46–47.

2. Лисенков, Б. Н. Проверка метрологических характеристик матричного коммутатора / Б. Н. Лисенков, Н. В. Грицев, А. А. Бруек // Опто-, микро- и СВЧ-электроника – 2018 : сборник научных статей Первой международной науч.-техн. конф. – Минск, 2018. – С. 82–85.

*УДК 004.056.5*

## ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ РАСШИРЕННОГО АЛГОРИТМА ОБМЕНА КЛЮЧАМИ В СРЕДСТВАХ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

**Марченков С.Д., Лебедев А.Н.**

*Московский государственный технический университет имени Н.Э. Баумана*
*Москва, Российская Федерация*

**Аннотация.** Представлен расширенный алгоритм обмена ключами со строгой аутентификацией сторон на основе алгоритма Диффи–Хэллмана с заменой операций в конечном коммутативном кольце. Основное внимание уделяется введенной арифметической операции и методу доставки ключевых параметров взаимодействующим сторонам. Рассмотрено возможное применение алгоритма в информационных системах, использующих открытый канал связи и средства криптографической защиты информации.
**Ключевые слова:** конечное поле, конечное коммутативное кольцо, криптография, протокол Диффи–Хеллмана, рассылка защищенных данных, аутентификация.

## PERSPECTIVES OF EXTENDED KEY EXCHANGE ALGORITHM IN CRYPTOGRAPHIC SECURITY TOOLS

**Marchenkov S., Lebedev A.**

*Bauman Moscow State Technical University*
*Moskow, Russia*

**Abstract.** The extended key exchange algorithm with strong side authentication based on the Diffie-Hellman algorithm with replacement of operations in a finite commutative ring is presented. Arithmetic operation and the way of passing key parameters to the interacting parties are analyzed. The possibilities of using the algorithm in information systems using an open communication channel and cryptographic tools for information protection are considered.
**Key words:** finite field, finite ring, cryptography, Diffie-Hellman protocol, authentication, secured data distribution.

*Адрес для переписки: Марченков С.Д., Россия, Москва, ул. 2-я Бауманская, 5, г. Москва 105005, Россия*
*e-mail: marchenkovsd@student.bmstu.ru*

Чтобы гарантировать целостность и конфиденциальность информации при обмене данными между двумя абонентами сети используются гибридные системы, в которых применяются алгоритмы ассиметричного шифрования для выработки секретного ключа и последующего симметричного шифрования непосредственно конфиденциальных данных. Протоколы такого типа используют алгоритмы обмена ключами для установления безопасного канала передачи данных. Для обмена ключами и проверки их подлинности в настоящее время используются комбинации алгоритмов, основанные на модификации классического алгоритма Диффи–Хеллмана [1].

**Протокол.** В статье [2] была предложена модель передачи зашифрованных данных с доступом легитимного пользователя в определенный период времени. При этом ключевые параметры необходимо хранить на защищенных аппаратных носителях информации.

Предполагается использование схемы протокола, приведенного далее, где $S$ – сервер, $U$ – клиент, $M$ – открытый текст, $C$ – шифртекст, $E$ – операция шифрования, $D$ – операция расшифрования.