**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине «Технологии аутентификации в информационных системах»
для студентов направления подготовки
10.03.01 Информационная безопасность
направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Ставрополь,
2026

## СОДЕРЖАНИЕ

Введение
Лабораторная работа № 1-3. Общие сведения об аутентификации в информационных системах
Лабораторная работа № 4-6. Аутентификация с помощью биометрических характеристик
Лабораторная работа № 7-9. Протоколы аутентификации в локальных сетях
Лабораторная работа № 10. Аппаратные средства аутентификации и хранения ключевой информации

# ВВЕДЕНИЕ

## 1. Цель и задачи освоения дисциплины (модуля)

Целью изучения дисциплины «Технологии аутентификации в информационных системах» является формирование у студентов набора профессиональных компетенций по направлению подготовки 10.03.01 Информационная безопасность позволяющих обучаемым администрировать подсистемы информационной безопасности объекта информатизации, обеспечивать разграничение доступа к информационным ресурсам и контролировать защищённость от несанкционированного доступа средств связи сетей электросвязи, организовать управление защищенностью объекта в соответствии с нормативными документами.

Основными задачами изучения дисциплины являются:

1. Изучение основных естественнонаучных законов для адекватного применения математического аппарата и выявления сущности проблем, возникающих в сфере защиты информации и информационной безопасности.

2. Формирование способностей применять методы теории систем и системного анализа при проведении предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.

3. Формирование способностей самостоятельно проводить эксперименты по заданной методике, обрабатывать результаты, оценивать погрешность и достоверность результатов.

## 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

| Код, формулировка компетенции | Код, формулировка индикатора | Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов |
|---|---|---|

| | | |
|---|---|---|
| **ПК-1** Способен обеспечивать защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации (06.030 В) | ИД-2 ПК-1 Способен к управлению функционированием СССЭ, защищённостью от НСД сооружений СССЭ (06.030 В/02.6) | - понимает особенности применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД;<br>- использует встроенные механизмы защиты от НСД в составе СССЭ;<br>- устанавливает и настраивает программное обеспечение, необходимое для управления СССЭ и средствами защиты от НСД |

Лабораторная работа 1-3

**Темы: Общие сведения об аутентификации в информационных системах**
**Парольная аутентификация**
**Аутентификация с помощью атрибутивных методов**

# ПОДГОТОВКА СТЕНДА, УСТАНОВКА И НАСТРОЙКА ПО, ПОДГОТОВКА ЭЛЕКТРОННЫХ КЛЮЧЕЙ eToken

## Цель работы

Подготовить стенд для выполнения работ по теме «Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin. Типовые решения». Подготовить к работе электронные ключи eToken.

### *Общие сведения о ключах eToken*

*Смарт-карты и USB-ключи*

Смарт-карты, как и Memory-карты, представляют собой пластиковые карты с встроенной микросхемой. Однако смарт-карта — достаточно сложное устройство, которое содержит микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления.

Несмотря на название — устройство для чтения смарт-карт — большинство оконечных устройств или устройств сопряжения (IFD) способны как считывать, так и записывать, если позволяют возможности смарт-карты и права доступа. Устройства для чтения смарт-карт могут подключаться к компьютеру с помощью:

- последовательного порта;
- слота PCMCIA;
- порта USB.

Устройства чтения смарт-карт могут быть интегрированы в клавиатуру.

Некоторые производители выпускают другие аппаратные устройства, в которых смарт-карта объединена с ее устройством чтения. По характеристикам памяти и вычислительным возможностям они аналогичны смарт-картам. Наиболее распространены аппаратные ключи, использующие порт USB. USB-ключи привлекательны для некоторых организаций, поскольку USB становится стандартом, находящим все большее распространение в новых компьютерах: организации не нужно приобретать для пользователей какие бы то ни было считыватели.

Для получения доступа к цифровым сертификатам пользователя на этапе аутентификации в систему и для хранения закрытых ключей пользователей для связки Kerberos + + PKINIT в ОС Windows 2000/2003 используются смарт-карты. Служба управления ресурсами смарт-карт интегрирована в операционную систему, и для настройки аутентификации по сертификатам достаточно активизировать данную службу, установив драйверы считывателей смарт-карт. При нахождении в домене графический интерфейс ОС Windows 2000/2003 (GINA) заменяется вариантом с поддержкой работы со смарт-картами.

На смарт-карту записывается цифровой сертификат и связанный с ним закрытый ключ, выписанные на доменном центре сертификации с использованием политик, предусматривающих возможность его использования для интерактивной аутентификации пользователя в системе.

При подключении смарт-карты к рабочей станции для аутентификации пользователя хранящийся на ней сертификат используется для запроса TGT, а операция с закрытым ключом, возможная после ввода PIN-кода, используется для подписи этого запроса.

### *Модели eToken*

Ключ eToken — персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронными цифровыми подписями (ЭЦП). eToken выпускается в форм-факторах USB-ключа или смарт-карты.

USB-ключ eToken подключается к компьютеру через порт USB (Universal Serial Bus) и не требует наличия устройства чтения смарт-карт.

eToken обладает защищенной энергонезависимой памятью и используется в качестве хранилища секретных данных (ключей шифрования, имен пользователя, паролей, учетных записей, сертификатов и пр.).

В лабораторных работах будет использоваться электронный ключ eToken PRO в форм-факторе USB-ключа.

*eToken PRO*

eToken PRO имеет микросхему смарт-карты Infineon SLE66C, аппаратно реализующую алгоритмы RSA, DES, TripleDES, SHA-1. eToken PRO снабжен встроенным генератором ключевых пар алгоритма RSA. При этом закрытые ключи никогда не покидают микросхему смарт-карты. Микросхемы семейства Infineon SLE66C работают под управлением операционной системы Siemens CardOS и обеспечивают высокий уровень безопасности (сертификат ITSEC LE4).

Кроме PIN-кода пользователя в eToken PRO предусмотрен пароль администратора. С его помощью, например, можно сменить забытый PIN-код. Пароль администратора также можно менять.

eToken PRO можно форматировать с помощью утилиты eToken Properties, входящей в состав набора драйверов eToken Run Time Environment 3.65. При форматировании:

- из памяти eToken PRO удаляется вся информация;
- устанавливается PIN-код;
- возможно задание пароля администратора;
- возможно задание ключа форматирования для предотвращения несанкционированного переформатирования.

# Описание работы

Для изучения возможностей продуктов Microsoft Windows Server 2003 и электронных ключей eToken для обеспечения безопасности доступа к данным информационной системы работа делится на три части:

- установка и настройка стенда;
- установка и настройка программного обеспечения для работы с ключами eToken;
- подготовка ключей eToken.

## *Установка и настройка стенда*

Данная часть работы предназначена для настройки стенда (хоста и виртуальных машин) и подготовки их к выполнению основной части лабораторной работы. Для выполнения данной части работы необходимо:

- подготовить и настроить рабочую станцию (хостовый компьютер);
- настроить виртуальную машину VM SRV;
- настроить виртуальную машину VM WS;
- настроить виртуальную сеть;
- проверить работу стенда;
- проанализировать полученный результат.

## *Установка и настройка программного обеспечения для работы с ключами eToken*

Данная часть работы предназначена для настройки программного обеспечения, необходимого для работы с электронными ключами eToken. Для работы с электронными ключами eToken необходимо установить и настроить программное обеспечение eToken RTE.

Для выполнения данной части работы необходимо:

- установить eToken RTE;
- установить eToken RTE Russian User Interface;
- проверить работу утилиты «Свойства eToken»;
- проанализировать полученный результат.

## *Подготовка ключей eToken*

Данная часть работы предназначена для подготовки электронных ключей eToken. Для использования ключей eToken для аутентификации в среде ОС Windows необходимо настроить параметры качества PIN-кодов, отформатировать ключи и задать PIN-коды администратора и пользователя.

Для выполнения данной части работы необходимо:

- установить расширенный режим работы утилиты «Свойства eToken»;
- отформатировать eToken;
- настроить параметры ключей eToken;
- проверить параметры ключей eToken;
- проанализировать полученный результат.

## Задание

1. Изучить теоретические вопросы, изложенные в начале лабораторной работы.
2. Подготовить стенд.
3. Установить и настроить программное обеспечение, необходимое для работы с ключами eToken.
4. Подготовить к работе ключи eToken.
5. Оформить отчет по лабораторной работе.
6. Ответить на контрольные вопросы.

## Порядок выполнения работы

*Описание стенда*

Для обеспечения проверки возможности настройки режимов работы встроенных (штатных) средств обеспечения безопасности Windows Server 2003 и Windows XP, построенных на основе технологий смарт-карт и основных концепциях построения PKI-систем, на базе Windows Server 2003 CA, ключей и смарт-карт eToken используется стенд.

В состав тестового стенда входят две виртуальные машины, построенные на основе VMware 6.0:

1. На базе ОС Windows Server 2003 Enterprise Edition R2 Rus.
2. На базе ОС Windows XP Pro Rus.

Для проведения лабораторной работы используется исходное состояние стенда, построенного на виртуальных машинах VMware 6.0.

Стенд для проведения лабораторных работ представляет собой рабочую станцию, на которой имитируется работа локальной сети предприятия. Он состоит из рабочей станции и созданных на ней двух виртуальных машин, работающих под управлением VMware 6.0. Для удобства дальнейшего изложения материала введены следующие обозначения:

- хост (host) — рабочая станция слушателя;
- VM SRV — виртуальная машина с операционной системой Windows Server 2003, сервер предприятия;
- VM WS — виртуальная машина с операционной системой Windows XP, рабочая станция предприятия.

Для нормального функционирования стенда рекомендуется следующая минимальная конфигурация рабочей станции:

- центральный процессор — Pentium III 1 ГГц;
- оперативная память — 1 Гб;
- объем свободного места на жестком диске — 20 Гб;
- наличие порта USB версии 2.0.

Кроме того, для настройки и последующей работы стенда потребуется следующее программное обеспечение:

- операционная система Windows XP Professional;
- VMware версии 6.0 или выше;
- CD-ROM с дистрибутивом (либо образ диска) Windows 2003 Server;

**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1

*Дополнительная:* 1

*Методическая литература: 1-3*

*Интернет-ресурсы:* 1-4

Лабораторная работа 4-6

**Темы: Аутентификация с помощью биометрических характеристик**

**Аутентификация с помощью одноразовых паролей**

**Инфраструктура открытых ключей (PKI)**

# УСТАНОВКА И НАСТРОЙКА ЦЕНТРА СЕРТИФИКАЦИИ, ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ ETOKEN В ДОМЕНЕ WINDOWS SERVER 2003

## Цель работы

Для выполнения работ по теме «Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin. Типовые решения» установить и настроить Центр сертификации Windows Server 2003 CA и научиться использовать электронные ключи eToken для аутентификации пользователей в домене Windows Server 2003.

### *Общие сведения об аутентификации пользователей в домене Windows Server 2003 с помощью цифровых сертификатов и ключей eToken*

*Инфраструктура открытых ключей (PKI)*

Основой построения инфраструктуры открытых ключей (PKI) на базе Windows Server 2003 является Центр сертификации (Certification Authority, CA) — один из компонентов сервера Windows Server 2003. Центр сертификации получает и обрабатывает запросы на издание цифровых сертификатов (X.509), идентифицирует и подтверждает такие запросы, издает сертификаты, используя шаблоны сертификатов, обновляет и аннулирует сертификаты, публикует сертификаты, создает и обрабатывает Списки аннулированных сертификатов (Certificate revocation lists, CRLs), а также сохраняет в журнале все операции с сертификатами.

Центр сертификации (CA) также выполняет операции по хранению и восстановлению закрытых ключей.

CA интегрирован со службой каталогов (Active Directory, AD) и использует AD для получения информации о пользователях и для хранения ключевых контейнеров.

При использовании электронных ключей eToken CA позволяет копировать цифровые сертификаты и закрытые ключи в защищенную память eToken.

## Описание работы

Для изучения возможностей Microsoft Windows Server 2003 CA и электронных ключей eToken для обеспечения аутентификации пользователей в домене Windows Server 2003 и безопасности доступа к данным информационной системы работа делится на две части:

- установка и настройка Центра сертификации (CA), подготовка его консоли, издание сертификатов;
- использование ключей eToken для регистрации в домене, для запуска приложений от имени другого пользователя и для подключения сетевых дисков с использованием прав доступа другого пользователя.

### *Установка и настройка Центра сертификации (CA), подготовка консоли Центра сертификации, издание сертификатов*

Данная часть работы предназначена для установки и настройки Центра сертификации, подготовки к работе консоли Центра сертификации и издания сертификатов, которые будут использоваться при выполнении основной части лабораторной работы. Для выполнения данной части работы необходимо:

Установить Центр сертификации на виртуальную машину VM SRV.

Настроить Центр сертификации:

- Создать шаблон сертификата.
- Включить шаблоны сертификатов.

Настроить консоль Центра сертификации:

- Установить пакет Windows Server 2003 Administration Tools.
- Подготовить консоль Центра сертификации.
- Подготовить консоль управления доменными политиками.
- Установить групповую политику для автоматической выдачи сертификатов. Издать сертификаты:
- Настроить станцию выписки сертификатов.
- Добавить Центр сертификации в список доверенных узлов.
- Подготовить консоль управления сертификатами.
- Получить сертификат агента получения заявок.
- Издать сертификаты с помощью агента получения заявок.
- Издать сертификаты без помощи агента получения заявок.
- Скопировать сертификаты с закрытыми ключами на eToken.
- Проверить работу стенда.
- Проанализировать полученный результат.

### *Использование ключей eToken для регистрации в домене, для запуска приложений от имени другого пользователя и для подключения сетевых дисков с использованием прав доступа другого пользователя*

Данная часть работы предназначена для обучения использованию ключей eToken при выполнении основных операций по безопасному доступу к информационным ресурсам домена Windows Server 2003 — регистрация пользователя в домене, запуск приложений и подключение сетевых дисков от имени другого пользователя с использованием электронных ключей eToken. Для выполнения данной части работы необходимо:

- Выполнить регистрацию в домене с помощью eToken.
- Установить для пользователя требование использования смарт-карты при интерактивном подсоединении к компьютеру.
- Установить групповую политику требования использования смарт-карты при интерактивном подсоединении к компьютеру.
- Установить блокирование компьютера и принудительный выход пользователя при отключении eToken.

Выполнить запуск приложений от имени другого пользователя:

- С использованием графического интерфейса.
- С использованием командной строки.

Выполнить подключение сетевых дисков с использованием прав доступа другого пользователя:

- С использованием графического интерфейса.
- С использованием командной строки.

Проанализировать полученный результат.

## Задание

1. Изучить теоретические вопросы, изложенные в начале данной лабораторной работы.
2. Установить и настроить Центр сертификации.
3. Выписать сертификаты, скопировать их в ключи eToken.
4. Выполнить регистрацию пользователя в домене с использованием eToken.
5. Выполнить запуск приложений от имени другого пользователя с использованием eToken.
6. Выполнить подключение сетевых дисков с использованием прав доступа другого пользователя с использованием eToken.
7. Оформить отчет по лабораторной работе.
8. Ответить на контрольные вопросы.

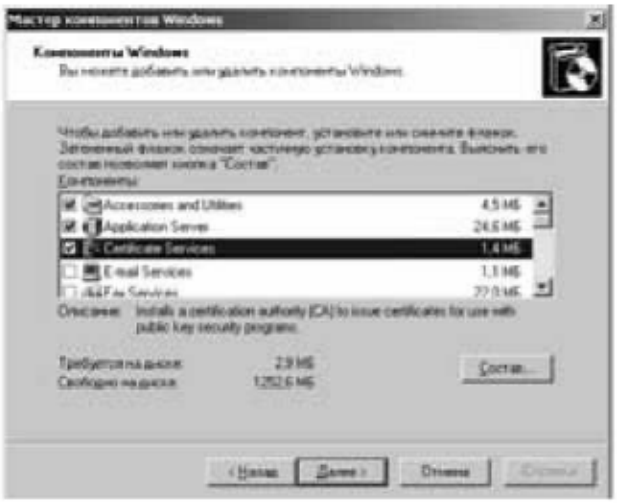
## Порядок выполнения работы

*Установка Центра сертификации*

Для установки Центра сертификации на контроллер домена выполните следующие шаги: Зарегистрируйтесь на компьютере VM SRV под именем пользователя с правами администратора.

**Выполните Пуск ^ Настройка ^ Панель управления ^ Установка и удаление программ (Start ^ Control Panel ^ Add or Remove Programs).**

Нажмите **Установка компонентов Windows** (Add/Remove Windows Components). Выберите пункт **Certificate Services** и нажмите **Далее** (Next).



## *Издание сертификатов*

Для издания сертификатов пользователей необходимо настроить станцию выписки сертификатов и получить сертификат агента получения заявок. Выписывать сертификаты можно как с помощью агента получения заявок, так и без него.

Кроме того, необходимо произвести настройку хоста для выписки сертификатов на устройство eToken. Необходимость настройки хоста вызвана особенностями работы VMware с портами USB. Для настройки хоста требуется внести изменения в реестр Windows, чтобы это сделать выполните следующие шаги:

Создайте в программе Notepad («Блокнот») или любом другом текстовом файле файл данных реестра (Registration Entries, *.reg), например vm_usb_correct.reg.

Введите следующий текст:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmusb\Parameters]
@=""
"PowerStateOnOpen—dword:00000000
"PowerStateOnClose"=dword:00000000"
"EnableRemoteWakeup"=dword:00000001
"MinPowerStateUsed"=dword:00000003
"MinPowerStateUnused"=dword:00000003
"AbortPipesOnPowerDown"=dword:00000001
"SuppressPnPRemoveDlg"=dword:00000001
"RequestTimeout'—dword:00002710
"ShortTransferOk'—dword:00000001
"MaxIsoPackets"=dword:00000040
"UnconfigureOnClose'—dword:00000001
"ResetDeviceOnClose"—dword:00000000
```

Сохраните файл и запустите его. На предложение внести данные в реестр ответьте Да (Yes).

После успешного внесения данных в реестр нажмите OK.

> ***Примечание.*** *Если не внести указанные изменения в реестр Windows, то выписать сертификат можно будет только на смарт-карту eToken. На USB-ключ eToken выписать сертификат будет невозможно — при попытке это сделать будет выведено окно с сообщением о неизвестной ошибке.*

### *Настройка станции выписки сертификатов*

#### *Добавление Центра сертификации в список доверенных узлов*

Для выписки сертификатов с использованием приложения Internet Explorer необходимо предварительно настроить его параметры безопасности. Для этого:

Запустите приложение Internet Explorer. Откройте пункт меню Сервис ^ Свойства обозревателя (Tools ^ Internet Options). Откройте вкладку Безопасность (Security).

Выберите зону Надежные узлы (Trusted sites) и нажмите кнопку Узлы (Sites). Введите адрес Центра сертификации (http://server.northwind.ru/certsrv) и нажмите Добавить (Add). Нажмите OK.

Чтобы обновленная политика начала действовать немедленно, выполните на контроллере домена команду gpupdate /force.

*Издание сертификатов без помощи агента получения заявок*

Для дальнейшего выполнения лабораторной работы выпишите сертификат для пользователя «и8ег_»Инициалы вашего имени и фамилии» без помощи агента получения заявок, используя шаблон Aladdin Exchange Sign & Encrypt.

Для того чтобы подать заявку на сертификат пользователя, получить сертификат и записать его в память eToken, следуйте приведенной ниже инструкции:

Запустите Microsoft Internet Explorer.

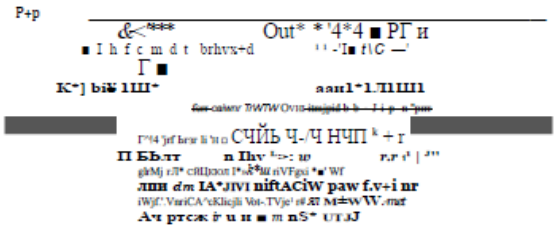
На домашней странице веб-узла службы сертификации http://server.northwind.ru/certsrv нажмите Request a certificate (Запросить сертификат).

На странице Request a Certificate (Запрос сертификата) нажмите advanced certificate request (расширенный запрос сертификата).

Нажмите Create and submit a request to this CA (Создать и представить на рассмотрение запрос к ЦС).

В разделе Certificate Template (Шаблон Сертификата) выберите шаблон Aladdin Exchange Sign & Encrypt. В поле Name (Имя) укажите имя пользователя, для которого вы выписываете сертификат, а в поле E-mail укажите его E-mail адрес.

В разделе Key Options (Настройки Ключа) все параметры оставьте без изменений:



## Содержание отчета

Отчет оформляется один на бригаду из одного-двух исполнителей.

В отчете с титульным листом установленной формы (Приложение А) необходимо представить следующие сведения:

1. Наименование и цели работы.
2. Краткую характеристику учебного стенда (по составу доступных пользователю функций управления и индикаций, распределению ресурсов, функций, вариантов набора преобразований).
3. Функциональную схему учебного стенда с пояснениями и комментариями.
4. Выполненные настройки Центра сертификации, шаблоны сертификатов, созданные в ходе выполнения лабораторной работы.
5. Подготовиться для устных ответов по контрольным вопросам.

## Контрольные вопросы

1. Какие дополнительные средства (утилиты) необходимо установить для того, чтобы подготовить к работе Центр сертификации?
2. Какие поля можно задавать в шаблоне сертификата?
3. Как издать сертификаты без помощи агента получения заявок?
4. Каким образом можно скопировать сертификат в память ключа eToken?
5. Как можно выполнить запуск приложений от имени другого пользователя с использованием командной строки?

**Список литературы, рекомендуемый к использованию по данной теме.**
*Основная:* 1
*Дополнительная:* 1
*Методическая литература: 1-3*
*Интернет-ресурсы:* 1-4

Лабораторная работа 7-9

**Темы: Протоколы аутентификации в локальных сетях**

**Механизмы аутентификации при осуществлении сетевых подключений**

**Аутентификация при защищённых соединениях**

# ИСПОЛЬЗОВАНИЕ eToken ДЛЯ БЕЗОПАСНОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ, ДЛЯ ШИФРОВАНИЯ И ДЛЯ ЭЦП

## Цель работы

Изучить возможности использования ключей eToken для безопасного доступа к информационным ресурсам организации, для шифрования информации и для ЭЦП в приложениях MS Office.

### *Общие сведения о безопасном доступе к информационным ресурсам организации*

*Удаленный доступ к рабочему столу (RDP)*

В Windows XP существует возможность выполнять аутентификацию пользователей по ключу eToken при входе в систему терминального клиента. Аутентификация производится с помощью цифрового сертификата X.509, хранящегося в памяти ключа, точно так же, как если бы пользователь физически находился за данной рабочей станциеи. В предыдущих лабораторных работах по теме «Обеспечение безопасности доступа к данным информационной системы организации с использованием продуктов Microsoft и Aladdin. Типовые решения» такие сертификаты уже использовались при регистрации пользователя в домене Windows Server 2003, при запуске приложений и для доступа к сетевым дискам от имени другого пользователя.

Помимо аутентификации при терминальном подключении все приложения, работающие со смарт-картами, к которым пользователь обращается в течение сеанса, могут использовать ключ eToken.

Для того чтобы пользователи имели доступ к рабочему столу, необходимо предоставить им такую возможность средствами ОС Windows. Программа «Подключение к удаленному рабочему столу» позволяет с легкостью подключаться к серверу терминалов или другому компьютеру, работающему под управлением Windows. При необходимости имеется возможность указать параметры каждого подключения и сохранить их в файле для последующего использования.

По умолчанию удаленный доступ к рабочему столу предоставляется администраторам. Чтобы обычные пользователи могли также подключаться к рабочему столу, необходимо предоставить им соответствующие права. Кроме того, можно предоставить пользователю право удаленно подключаться к контроллеру домена.

*Виртуальные частные сети (VPN)*

При развертывании PKI в основу использования виртуальной частной сети (Virtual Private Network, VPN) положен протокол расширенной аутентификации (Extensible Authentication Protocol, EAP). Подключаться к сети через VPN-соединения могут только те пользователи, учетные записи которых настроены для таких подключений. Возмож-

ность подключения пользователей к корпоративным серверам через VPN-соединения задается настройками сервера. Кроме сервера и учетной записи пользователя необходимо также соответствующим образом настроить рабочую станцию — установить сертификат ЦС, а также создать и настроить VPN-соединение.

*Общие сведения о протоколе EAP*

Для проверки подлинности подключений виртуальных частных сетей (VPN), поддерживающих протокол PPTP или L2TP, применяются методы проверки на уровне пользователей, основанные на протоколе PPP. К этим методам относятся протоколы:

— Password Authentication Protocol (PAP);
— Challenge Handshake Authentication Protocol (CHAP);
— Shiva Password Authentication Protocol (SPAP);
— Microsoft Challenge Authentication Protocol (MS-CHAP);
— Extensible Authentication Protocol (EAP).

Благодаря новым возможностям, предлагаемым протоколами EAP и IPSec (Internet Protocol security), виртуальные частные сети обеспечивают повышенную безопасность для удаленных пользователей.

Протокол EAP является расширением протокола Point-to-Point Protocol (PPP). На нем основаны несколько методов проверки подлинности, предусматривающих обмен учетными записями и прочими сведениями произвольного объема. Протокол EAP был разработан с учетом растущей потребности в средствах проверки подлинности, использующих более широкий круг устройств системы безопасности; он предлагает стандартную архитектуру для поддержки дополнительных методов проверки подлинности в рамках PPP.

С помощью EAP можно реализовать поддержку нескольких алгоритмов проверки подлинности — так называемых типов EAP, к числу которых относятся:

— генераторы кода доступа:
— одноразовые пароли;
— средства проверки подлинности на основе открытых ключей с помощью смарт-карт, сертификатов и др.

Сочетание протокола со строгими типами является ключевым компонентом технологии безопасных подключений виртуальных частных сетей (VPN). Например, строгие типы EAP, основанные на сертификатах, обеспечивают более надежную защиту от попыток «грубого» взлома системы или подбора пароля, чем другие протоколы проверки подлинности, использующие пароли, такие как CHAP и MS-CHAP.

Операционная система Windows XP включает поддержку двух типов EAP:

— EAP-MD5 CHAP (аналог протокола проверки подлинности CHAP);
— EAP-TLS (применяется для проверки подлинности на основе сертификатов пользователей).

EAP-TLS — это метод взаимной проверки подлинности, при котором и клиент, и сервер должны предоставлять доказательства своей подлинности. В ходе сеанса EAP-TLS клиент удаленного доступа отправляет свой сертификат пользователя, а сервер удаленного доступа — свой сертификат компьютера. Если хотя бы один из этих сертификатов не будет передан или окажется недействительным, подключение разрывается.

*Защищенное подключение к Web-серверу (HTTPS)*

Для исключения несанкционированного доступа к веб-северу используется защищенный протокол HTTPS. Рекомендуется создать новый защищенный веб-сервер и для исключения несанкционированного доступа к такому серверу рекомендуется максимально ограничить возможности аутентификации пользователя, исключив анонимную

аутентификацию, а также другие стандартные способы аутентификации. При работе с общими настройками сервера способы аутентификации ограничиваются на уровне сервера целиком, и эти изменения применяются ко всем сайтам данного сервера.

Ограничив способы идентификации на уровне сервера, можно приступать к настройке сайтов (правильное задание DNS-имени для нового сервера и настройки доступа по протоколу HTTPS).

Следует отметить, что после настройки веб-сервера доступ ко всем его сайтам по протоколу HTTP станет невозможным.

Важно отметить, что в целях безопасности развертывать Центр сертификации на веб-сервере не рекомендуется.

*Шифрование и использование ЭЦП*

Microsoft Office 2003 использует технологию Microsoft Authenticode, позволяющую снабжать электронные документы (файлы) электронной цифровой подписью (ЭЦП).

Электронная цифровая подпись представляет собой зашифрованную с помощью закрытого ключа автора контрольную сумму электронного документа. Для вычисления контрольной суммы используется известный автору и адресату алгоритм (хэш-функция). Для того, чтобы проверить электронную цифровую подпись, используется открытый ключ автора документа. Открытый ключ автора содержится в сертификате ключа подписи и распространяется вместе с ним. Такой механизм позволяет, с одной стороны, проверить целостность электронного документа, а с другой — удостоверить его авторство.

Для проверки электронной цифровой подписи пользователь должен иметь действующий сертификат (формата X.509) отправителя. Поэтому при отправке подписанного сообщения адресату передается его электронная цифровая подпись, а также, как правило, сертификат ключа подписи автора.

При успешной проверке электронной цифровой подписи адресат подтверждает, что документ был получен от владельца сертификата ключа подписи (автора) и документ не был изменен.

Microsoft Office 2003 позволяет создавать ЭЦП в документах, создаваемых с помощью приложений: Word 2003, Excel 2003, Power Point 2003.

## Описание работы

Для изучения возможностей использования ключей eToken для безопасного доступа к информационным ресурсам организации, для шифрования информации и для ЭЦП в приложениях MS Office работа делится на четыре части:

- удаленный доступ к рабочему столу с использованием eToken (RDP);
- настройка виртуальной частной сети (VPN);
- создание защищенного веб-сервера и настройка доступа по HTTPS;
- использование шифрования и ЭЦП в приложениях MS Office.

### *Удаленный доступ к рабочему столу с использованием eToken*

Данная часть работы предназначена для настройки сервера и рабочей станции и подготовки их к проверке удаленного подключения с помощью eToken. Для выполнения данной части работы необходимо:

- Настроить возможность удаленного доступа к компьютеру.
- Настроить рабочую станцию.

- Настроить контроллер домена.
- Настроить подключение к удаленному компьютеру с помощью eToken.
- Предоставить обычным пользователям возможность удаленного доступа к компьютеру.
- Предоставить пользователям права Log on through Terminal Services на контроллере домена.
- Проверить удаленный доступ к рабочему столу сервера с рабочей станции.
- Проанализировать полученный результат.

### *Настройка виртуальной частной сети*

Данная часть работы предназначена для настройки сервера маршрутизации с использованием протокола EAP, а также для настройки учетной записи пользователя для использования VPN-соединений на примере организации удаленного доступа пользователей к рабочему столу (RDP).

Для выполнения данной части работы необходимо:

- Настроить сервер маршрутизации и удаленного доступа.
- Настроить учетную запись пользователя для использования VPN-соединений.
- Установить сертификат Центра сертификации на рабочую станцию.
- Создать VPN-соединение на рабочей станции.
- Настроить параметры VPN-соединения на рабочей станции.
- Установить VPN-соединение.
- Проверить сведения об установленном VPN-соединении.
- Проанализировать полученный результат.

### *Создание защищенного веб-сервера и настройка доступа по HTTPS*

Данная часть работы предназначена для создания дополнительного защищенного веб-сервера, настройке подключения к защищенному веб-серверу с использованием протокола HTTPS и проверке доступа к защищенному веб-сайту, созданному на защищенном веб-сервере.

Для выполнения данной части работы необходимо:

- Создать дополнительный защищенный веб-сервер.
- Настроить подключение к новому веб-серверу по протоколу HTTPS.
- Создать DNS-имя для нового веб-сервера.
- Настроить рабочую станцию.
- Настроить сетевые подключения на хосте.
- Настроить файл hosts на хосте.
- Проверить доступ к веб-сайту по HTTPS.
- Проанализировать полученный результат.

### *Использование шифрования и ЭЦП в приложениях MS Office*

Данная часть работы предназначена для настройки использования электронной цифровой подписи (ЭЦП) в приложениях MS Word 2003 и MS Outlook 2003, а также для защиты электронных сообщений при использовании технологии Outlook Web Access.

Для выполнения данной части работы необходимо:

- Создать ЭЦП в MS Word 2003.
- Проверить работу с ЭЦП в MS Word 2003.
- Настроить MS Outlook 2003 для шифрования и ЭЦП сообщений.
- Настроить MS Outlook 2003 для нового пользователя.
- Настроить параметры MS Outlook 2003 для шифрования и ЭЦП сообщений.
- Настроить Outlook Web Access для шифрования и ЭЦП сообщений.
  - Проверить использование MS Outlook 2003 для защиты сообщений электронной почты.
- Создать сообщения с ЭЦП.
- Создать зашифрованное сообщение.
- Открыть зашифрованные сообщения.
- Проверить ЭЦП в сообщении.
- Проанализировать полученный результат.

## Задание

1. Изучить теоретические вопросы, изложенные в начале данной лабораторной работы.
2. Настроить стенд, рабочую станцию и контроллер домена.
3. Установить и настроить защищенный веб-сервер.
4. Настроить и проверить удаленный доступ к рабочему столу с использованием eToken.
5. Настроить и проверить работу виртуальной частной сети с использованием eToken.
6. Создать защищенный веб-сервер и настроить доступ по протоколу HTTPS.
7. Настроить и проверить использование шифрования и ЭЦП в MS Word 2003 и в MS Outlook 2003.
8. Оформить отчет по лабораторной работе.
9. Ответить на контрольные вопросы.

## Содержание отчета

Отчет оформляется один на бригаду из одного-двух исполнителей.

В отчете с титульным листом установленной формы (см. Приложение А) необходимо представить следующие сведения:

1. Наименование и цели работы.
2. Краткую характеристику учебного стенда (по составу доступных пользователю функций управления и индикаций, распределению ресурсов, функций, вариантов набора преобразований).
3. Функциональную схему учебного стенда с пояснениями и комментариями.
4. Описание настроек сервера и рабочей станции для удаленного доступа к рабочему столу.
5. Описание настроек виртуальной частной сети.
6. Настройки созданного нового защищенного веб-сервера для доступа к нему по протоколу HTTPS.
7. Настройки MS Word 2003 и MS Outlook 2003 для применения ЭЦП.
8. Подготовиться для устных ответов по контрольным вопросам.

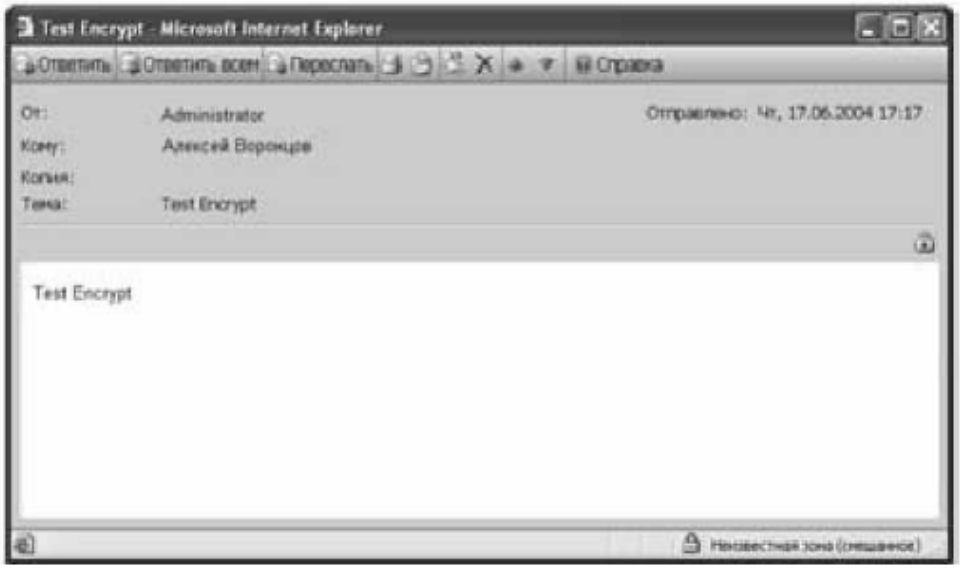
Для того чтобы в Outlook 2003 открыть зашифрованное сообщение, необходимо вы-

## Контрольные вопросы

1. Как настроить учебный стенд для работы виртуальной частной сети?
2. Как использовать ЭЦП в MS Word 2003?
3. Как создать защищенный веб-сервер?
4. Каким образом можно настроить MS Outlook 2003 для шифрования сообщений?
5. В чем заключаются отличия протоколов PPP и EAP?

Дважды щелкните мышью на зашифрованное сообщение.

В окне будет представлено само сообщение (расшифрованное), а справа внизу в заголовке письма будет стоять значок зашифрованного сообщения.




**Список литературы, рекомендуемый к использованию по данной теме.**

*Основная:* 1

*Дополнительная:* 1

*Методическая литература: 1-3*

*Интернет-ресурсы:* 1-4

Лабораторная работа 10

**Темы:** Аппаратные средства аутентификации и хранения ключевой информации

# СОПРОВОЖДЕНИЕ ФУНКЦИОНИРОВАНИЯ ЦЕНТРА СЕРТИФИКАЦИИ, ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ СИСТЕМ НА ОСНОВЕ WINDOWS SERVER 2003

## Цель работы

Изучить практические вопросы по сопровождению функционирования Центра сертификации и рассмотреть практические советы по повышению защищенности систем на основе Windows Server 2003.

### *Общие сведения по сопровождению функционирования Центра сертификации и повышению безопасности систем на основе Windows Server 2003*

*Архивирование и восстановление ЦС*

В данной лабораторной работе будут рассмотрены практические вопросы по сопровождению функционирования Центра сертификации, которое, помимо изученных ранее операций настройки и выпуска сертификатов, включает архивирование и восстановление состояния системы (компьютера, на котором установлен ЦС), архивирование и восстановление собственно самого ЦС, а также такие операции, как архивирование сертификатов, аннулирование и удаление сертификатов.

Первая часть работы посвящена вопросам архивирования сертификатов. Кроме того, специалистами компании Microsoft рекомендовано регулярное архивирование данных на компьютере, выполняющем функции Центра сертификации. В процессе сопровождения функционирования Центра сертификации также может потребоваться архивирование данных и самого Центра сертификации.

В процессе выполнения работы слушатели познакомятся с рекомендациями специалистов компании Microsoft по сопровождению функционирования Центра сертификации.

*Обеспечение безопасности клиентов нижнего уровня*

Степень безопасности всякой системы определяется степенью безопасности ее самого слабого звена. Именно поэтому необходимо постоянно выявлять такие звенья и повышать уровень их защищенности.

Обеспечение безопасности клиентов нижнего уровня — задача не из легких. Кроме того, она относится к разряду задач, которыми часто пренебрегают при внедрении новой операционной системы. Хотя настройку защиты Windows 9x и Windows NT вряд ли можно назвать увлекательной работой, однако глубокое понимание всех проблем, связанных с безопасностью этих систем, поможет лучше подготовиться к настройке доменов Windows.

Все методы и средства, которые используются для защиты клиентов нижнего уровня, имеют аналоги в системах Windows 2000/XP: оснастке Group Policy соответствует редак-

тор системной политики System Policy Editor, Security Configuration Manager — Security Configuration and Analysis, SMB-подпись — IPSec. Это не означает, что данные инструменты и методы защиты идентичны — они просто призваны решать сходные проблемы и нередко позволяют получить примерно одинаковые результаты.

Для обеспечения защиты клиентов нижнего уровня нужно выполнить следующие действия:

- установить клиент AD;
- включить обязательный режим аутентификации NTLMv2;
- при необходимости включить режим подписи SMB;
- использовать Security Configuration Manager и System Policy Editor для дополнительной защиты клиентов;
- тщательно тестировать все новые безопасные конфигурации.

Тематика второй части лабораторной работы посвящена настройкам, позволяющим в той или иной степени повысить безопасность систем на основе Windows Server 2003.

Рекомендации по сопровождению функционирования Центра сертификации (ЦС)

Специалисты компании Microsoft рекомендуют при работе с развернутой инфраструктурой открытых ключей (PKI) на базе Microsoft Windows Server 2003 CA придерживаться следующих правил:

- Держать корневой ЦС отключенным от сети и хранить его в физически защищенном месте, например в сейфе. В данной лабораторной работе Центр сертификации и контроллер домена находятся на одном компьютере, исходя из удобства изложения материала. В действительности же лучше создать Центр сертификации независимо от контроллера домена.
- Не создавать в больших организациях, интенсивно использующих структуру PKI и соответствующие приложения, более четырех уровней иерархии ЦС. При необходимости лучше расширять иерархию, создавая на соответствующих уровнях дополнительные, специализирующиеся на определенных типах сертификатов ЦС, а также оптимизировать распределение ЦС по предприятию.
- Возобновлять сертификаты ЦС задолго до истечения их срока действия.
- Обеспечивать регулярное и своевременное обновление публикуемого CRL, чтобы учесть и потребности в своевременном извещении об отозванных сертификатах, и необходимость выполнения репликации изменений. Иными словами, нужно следить, чтобы CRL не устаревал еще до того, как он будет реплицирован на всех доменах всеми контроллерами доменов.
- Защищать резервную копию секретного ключа ЦС и базы данных и хранить их в надежном месте.
- Своевременно обновлять программное обеспечение с помощью сервисных пакетов и модулей обновления.
- Заблаговременно отрабатывать и проверять план действий в нештатных ситуациях.

## Описание работы

Для изучения практических вопросов по сопровождению функционирования Центра сертификации и повышению безопасности систем на основе Windows Server 2003 работа делится на две части:

- сопровождение функционирования Центра сертификации;
- повышение безопасности клиентов нижнего уровня.

*Обслуживание Центра сертификации*

Данная часть работы предназначена для ознакомления с практическими советами по сопровождению функционирования Центра сертификации. Для выполнения данной части работы необходимо:

- Научиться проводить архивирование сертификата вместе с закрытым ключом.
- Выполнить резервное копирование и восстановление состояния системы.
- Научиться проводить отзыв и удаление сертификата.
- Провести архивирование и восстановление Центра сертификации.
- Научиться переиздавать сертификат корневого Центра сертификации.
- Научиться корректно удалять Центр сертификации.
- Изучить практические рекомендации по работе с центром сертификации.
- Проанализировать полученные результаты.

*Повышение безопасности клиентов нижнего уровня*

Данная часть работы предназначена для ознакомления с практическими советами и рекомендациями по повышению уровня безопасности клиентов нижнего уровня в системах, построенных на основе Windows Server 2003. Для выполнения данной части работы необходимо:

- Изучить отказ от аутентификации LM, NTLM v.1:
  - — провести установку алгоритма аутентификации NTLM v.2 на клиенте;
  - — запретить алгоритмы аутентификации LM и NTLM v.1 на контроллере домена.
- Настроить запрет создания и хранения значений хэш-функций LM на контроллере домена.
- Настроить парольную политику домена.
- Изучить возможность усиления безопасности на уровне сетевого трафика:
  - — выполнить отключение протокола NetBIOS;
  - — выполнить включение SMB-подписи.
- Проанализировать полученный результат.

## Задание

1. Изучить теоретические вопросы, изложенные в начале данной лабораторной работы.
2. Провести архивирование сертификата вместе с закрытым ключом.
3. Выполнить резервное копирование и восстановление состояния системы.
4. Переиздать сертификат корневого Центра сертификации.
5. Корректно удалить Центр сертификации.
6. Изучить практические рекомендации по работе с центром сертификации.
7. Выполнить отказ от аутентификации LM, NTLM v.1.
8. Настроить запрет создания и хранения значений хэш-функций LM на контроллере домена.
9. Выполнить отключение протокола NetBIOS.
10. Выполнить включение SMB-подписи.
11. Оформить отчет по лабораторной работе.
12. Ответить на контрольные вопросы.

## Содержание отчета

Отчет оформляется один на бригаду из одного-двух исполнителей.

В отчете с титульным листом установленной формы (см. Приложение А) необходимо представить следующие сведения:

1. Наименование и цели работы.
2. Краткую характеристику учебного стенда (по составу доступных пользователю функций управления и индикаций, распределению ресурсов, функций, вариантов набора преобразований).

425



3. Функциональную схему учебного стенда с пояснениями и комментариями.
4. Описание настроек протокола аутентификации на сервере и на рабочей станции.
5. Описание действий по архивации и восстановлению Центра сертификации.
6. Подготовиться для устных ответов по контрольным вопросам.

## Контрольные вопросы

1. Как проводить процедуры резервного копирования и восстановления Центра сертификации?
2. Как настроить использование протокола аутентификации NT LM v.2?
3. Как усилить безопасность на уровне сетевого трафика?
4. Какие есть рекомендации по работе с центром сертификации и PKI-службой?

**Перечень литературы необходимый для освоения дисциплины**

**Основная литература:**

Краковский Ю.М. Методы защиты информации: учебное пособие для вузов / Ю.М. Краковский. - 3-е изд., перераб. - Санкт-петербург: Лань, 2021. - 236 с.: ил. https://eJanbook.eom/reader/book/156401/#2

**Дополнительная литература:**

Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.

**Методическая литература:**

Конспект лекций по дисциплине «Технологии аутентификации в информационных системах».

Методические рекомендации по лабораторным работам.

Методические рекомендации по практическим занятиям.

**Интернет-ресурсы:**

Windows Server. Официальный сайт. http ://www.microsoft.com/Rus/windows-

server/default.mspx
Oracle Database 10g Release 2 (10.2) Documentation
http://www.oracle.com/technology/documentation/database10gr2.html
Oracle E-Business Suite. Каталог. http://download.oracle.com/otndocs/ebs/oracle-ebs-catalogue-full.pdf

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических занятий
по дисциплине «Технологии аутентификации в информационных системах»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Ставрополь,
2026

## СОДЕРЖАНИЕ

Введение

Практическое занятие № 1-4. Разделение речи дикторов и сравнение сигналов с использованием комплекса криминалистического исследования фонограмм речи «икар лаб»

Практическое занятие № 5-9. Исследование модулей «сравнение формант» и «сравнение основного тона» комплекса криминалистического исследования фонограмм речи «икар лаб»

Практическое занятие № 10-18. Исследование модулей «сравнение речевых признаков» и «сравнение основного тона» комплекса криминалистического исследования фонограмм речи «икар лаб»

## 1. Цель и задачи освоения дисциплины (модуля)

Целью изучения дисциплины «Технологии аутентификации в информационных системах» является формирование у студентов набора профессиональных компетенций по направлению подготовки 10.03.01 Информационная безопасность позволяющих обучаемым администрировать подсистемы информационной безопасности объекта информатизации, обеспечивать разграничение доступа к информационным ресурсам и контролировать защищённость от несанкционированного доступа средств связи сетей электросвязи, организовать управление защищенностью объекта в соответствии с нормативными документами.

Основными задачами изучения дисциплины являются:

1. Изучение основных естественнонаучных законов для адекватного применения математического аппарата и выявления сущности проблем, возникающих в сфере защиты информации и информационной безопасности.

2. Формирование способностей применять методы теории систем и системного анализа при проведении предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.

3. Формирование способностей самостоятельно проводить эксперименты по заданной методике, обрабатывать результаты, оценивать погрешность и достоверность результатов.

## 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

| Код, формулировка компетенции | Код, формулировка индикатора | Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов |
|---|---|---|

| | | |
|---|---|---|
| **ПК-1** Способен обеспечивать защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации (06.030 В) | ИД-2 ПК-1 Способен к управлению функционированием СССЭ, защищённостью от НСД сооружений СССЭ (06.030 В/02.6) | - понимает особенности применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД;<br>- использует встроенные механизмы защиты от НСД в составе СССЭ;<br>- устанавливает и настраивает программное обеспечение, необходимое для управления СССЭ и средствами защиты от НСД |

## Практическое занятие № 1-4

**Тема:** Разделение речи дикторов и сравнение сигналов с использованием комплекса криминалистического исследования фонограмм речи «ИКАР Лаб»

**Цель занятия:**

Ознакомиться с теоретическим материалом предназначенным для формирования у обучающегося базовых знаний для дальнейшего изучения комплекса криминалистического исследования фонограмм речи «ИКАР Лаб», получение практических навыков в обработке и сравнении сигналов, с использованием комплекса криминалистического исследования фонограмм речи «ИКАР Лаб».

**Формируемые компетенции:** ПК-1

**Структура лабораторной работы**

**Вводная часть**

| | |
|---|---|
| Проверка готовности студентов к лабораторной работе | 10 мин |
| Вступительная часть | 10 мин |

**Вопросы (задачи), подлежащие исследованию**

| | |
|---|---|
| Изучение теоретических данных | 40 мин |

**Заключительная часть**

| | |
|---|---|
| Защита отчетов по лабораторной работе | 20 мин |
| Подведение итогов | 5 мин |
| Задание студентам для самостоятельной работы | 5 мин |

## 1 Теоретические сведения для выполнения лабораторной работы

Модуль разделения дикторов в диалоге предназначен для автоматической маркировки речевых сегментов по дикторам на записях естественной речи. Надежность работы модуля разделения дикторов в значительной степени зависит от степени качества речи входных фонограмм. Максимальное качество разделения речи дикторов (93-95% правильной маркировки по дикторам) достигается при ОСШ не менее 20 дБ и длительности речи каждого из дикторов на фонограмме не менее 16 секунд.

Модуль «Автоматическое сравнение» осуществляет автоматическую идентификацию и сравнение дикторов на основе следующих методов:

— Метод статистик основного тона (ОТ).

— Спектрально-формантный метод

— Метод полной изменчивости (СГР).

Идентификация диктора на основе первых трёх методов включает два основных этапа: построение соответствующих методу моделей речевого сигнала диктора и сравнение построенных моделей с принятием идентификационного решения. По результатам использования автоматических методов идентификации принимается обобщенное решение и его результат является наиболее точным. Обобщенное решение является взвешенным усреднённым результатом идентификации по каждому из использованных частных методов, указанных выше.

### МЕТОД СТАТИСТИК ОСНОВНОГО ТОНА

Метод идентификации дикторов на основе сравнения статистик основного тона голоса Данный метод использует шестнадцать различных статистических характеристик кривой основного тона (ОТ) голоса для всего исследуемого речевого материала: среднее значение ОТ, максимальное, минимальное значения ОТ, максимум -3% значений ОТ, минимум +1% значений ОТ, процент участков с возрастающим тоном, дисперсия логарифма ОТ, медиана, асимметрия и эксцесс гистограммы логарифма тона и гистограммы производной логарифма ОТ, средняя скорость изменения, возрастания и уменьшения тона, дисперсия производной логарифма тона. Значение равновероятностной ошибки пропуска/отклонения

целевого диктора (EER) для метода сравнения статистик основного тона голоса в зависимости от длительности сравниваемых речевых фрагментов составляет 16–20%. Реализация данного алгоритма стала возможной благодаря созданию специалистами ООО «ЦРТ» полностью автоматического высокоточного алгоритма выделения основного тона. Характеристики статистик ОТ голоса зависят от эмоционально-психологического и физического состояния диктора в момент произнесения, от стиля речи (чтение – спонтанная речь – публичное вступление/подготовленная речь), от окружающей акустической обстановки (Ломбард-эффект). Поэтому при сравнении дикторов важно учитывать сопоставимость речевого материала сравниваемых дикторов и, при наличии факторов, существенно влияющих на изменение ОТ, учитывать это при принятии общего идентификационного решения. Построение модели голоса диктора производится следующим образом. Выделение основного тона (ОТ) осуществляется с помощью спектрального анализа сигнала фонограммы. Основу метода составляет алгоритм, который базируется на анализе значений гармоник ОТ в спектре сигнала. Алгоритм направлен на преодоление проблем, связанных с подавлением части спектра сигнала в канале.

Например, в телефонном канале в полосе от 0 до 300 Гц сигнал отсутствует, однако именно в этом диапазоне чаще всего находится значение частоты ОТ. В этом случае алгоритм выделения ОТ позволяет решить поставленную задачу за счёт учёта гармоник частоты ОТ в полосе от 0,3 до 3,4 кГц. Данный метод идентификации достаточно устойчив и к отношению сигнал/шум. Если уровень гармоник частоты основного тона хотя бы на несколько децибел превышает уровень шума, алгоритм с помощью специальных методов «подчеркивания» гармоник ОТ позволяет определить искомую частоту. На этапе вычисления статистических характеристик ОТ вычисляется набор значений статистик ОТ по полученным кривым ОТ, который содержит такие характеристики как среднее, максимальное и минимальное значения ОТ; значения частоты, выше которой находятся 3 % значений ОТ, и частоты, ниже которой находятся 1 % значений ОТ; медиана; процент участков с возрастающим ОТ; дисперсия; асимметрия и эксцесс гистограммы логарифма ОТ и гистограммы

производной логарифма ОТ; средняя скорость изменения ОТ, усредненная скорость изменения, нарастания и убывания частоты ОТ. По получаемым статистическим оценкам характеристик ОТ строится модель диктора с использованием аппроксимации данных с использованием Смеси Гауссовых Распределений (СГР). На этапе принятия решения об идентификации производится сравнение статистических характеристик ОТ, вычисляются значения ошибок первого и второго рода (FA и FR) по каждому из полученных значений статистик ОТ, а также значения FA и FR по результирующей метрике статистик ОТ как взвешенная сумма всех относительных отклонений значений статистик ОТ для двух сравниваемых фонограмм. Производится бэггирование по длительности речевого сигнала (оценки FR/FA зависят от длительности речевого сигнала, по которому построена каждая из сравниваемых СГР-моделей).

## СПЕКТРАЛЬНО-ФОРМАНТНЫЙ МЕТОД ИДЕНТИФИКАЦИИ ДИКТОРОВ

Данный метод основан на тезисе об уникальности геометрии вокального тракта у каждого человека и отражении данного факта в различных спектральных характеристиках речи. Наиболее явно различие спектральных характеристик проявляется во взаимном расположении формант в частотной области. Данный метод основан и на выделении и сравнении положения и динамики поведения трёх и более формант (защищён российским патентом). Применение спектрально-формантного метода обеспечивает значение величины EER до 6–7 %. Значение этого показателя для конкретного случая зависит от длительности и качества сравниваемых речевых фрагментов. Спектрально-формантный метод довольно устойчив к широкополосному равномерному шуму типа белого или шума помещения, а также к различиям в сигналах за счет различных типов каналов звукозаписи. Построение модели голоса диктора производится следующим образом. Строится средний спектр речевого сигнала, используемого для построения идентификационной модели диктора. Далее на его основе для данной фонограммы строится нормализующая функция, используемая для вычисления мгновенных

спектров (кадров) речевого сигнала. На каждом нормализованном кадре определяется положение всех максимумов, из которых выделяются формантные.

**МЕТОД ПОЛНОЙ ИЗМЕНЧИВОСТИ**

Учитывается относительная непрерывность траектории формант и их типовые частотные области расположения каждой из формант для мужских и женских голосов. В качестве идентификационных признаков используются положения 3-х спектральных максимумов, наиболее соответствующих формантам речевого сигнала на каждом спектральном срезе, где их удалось достаточно надёжно выделить. Эти признаки в наибольшей степени определяют индивидуальные особенности геометрии голосового тракта. Плотность распределения идентификационных признаков моделируется с использованием СГР. Непосредственное принятие решения об идентификации производится на основе использования SVM-классификатора. По результирующей дистанции SVM вычисляются ошибки первого/второго рода FR/FA. Производится бэггирование по длительности речевого сигнала (оценки FR/FA зависят от длительности речевого сигнала, по которому построена каждая из сравниваемых СГР-моделей).

Метод, названный в данной системе СГР или TotV (Total Variability, «полная изменчивость»), является наиболее современным методом идентификации по голосу. Построение модели голоса диктора производится следующим образом. Вычисляются речевые признаки MFCC (Mel Fourier Cepstrum coefficients, кепстральные коэффициенты по шкале мел) – характеристики, описывающие покадровое спектральное представление речевого сигнала на тональных участках речи. Плотность распределения идентификационных признаков моделируется с использованием смеси гауссовых распределений (СГР). Параметры СГР-модели далее с помощью специально адаптированного факторного анализа представляются в виде вектора малой размерности в так называемом пространстве «полной изменчивости», в котором строятся подпространства так называемых «собственных каналов» и «собственных голосов», используемых в алгоритме JFA (Joint Factor Analysis, объединённый факторный анализ). Отличительной особенностью такого представления СГР-модели является её высокая информативность и малый размер

данных. На этапе сравнения моделей дикторов соответствующие им вектора признаков сравниваются с помощью алгоритма на основе SVM-классификатора (Support Vector Machine, машина опорных векторов), хорошо зарекомендовавшего себя с точки зрения скорости и качества идентификационного решения. По результирующей дистанции SVM вычисляются ошибки первого/второго рода FR/FA. Производится бэггирование по длительности речевого сигнала (оценки FR/FA зависят от длительности речевого сигнала, по которому построена каждая из сравниваемых СГР-моделей). Таблицы для определения вероятностей совпадения, различия дикторов по полученной дистанции между сравниваемыми сигналами получаются на этапе обучения системы путем обработки большого массива фонограмм совпадающих и разных дикторов (тысячи дикторов, различные каналы звукозаписи).

## 2. Практическая часть

### 2.1 Выполнение разделения речи дикторов

Чтобы выполнить автоматическую маркировку речи дикторов в диалоге по репликам, выберите в меню Модули Разделение дикторов в диалоге.

В диалоговом окне Разделение дикторов (рис. 1) установите максимальный промежуток времени между речевыми участками одного диктора, при котором данные участки будут считаться единым фрагментом.

Задайте параметры Имена марок диктора 1 и Имена марок диктора 2, которыми будут обозначаться фрагменты речи каждого диктора.

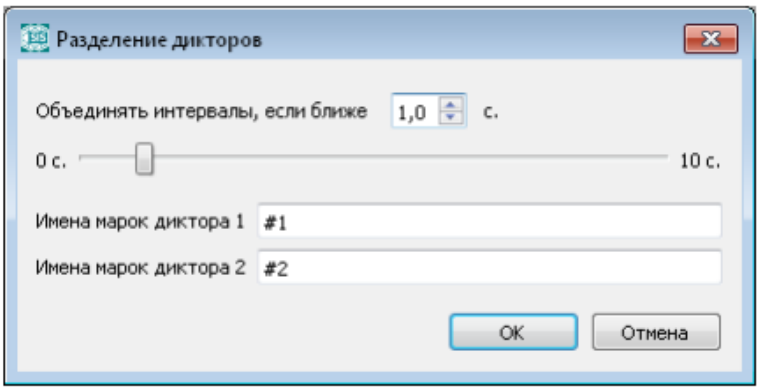



Рисунок 1– Окно «Разделение дикторов»

Для запуска процесса разделения речи дикторов нажмите кнопку ОК. После выполнения операции разделения речи дикторов в окне данных появятся марки интервалов, отмечающие участки фонограммы, содержащие речь двух дикторов. В списке марок во вкладках с именами марок для двух дикторов будут перечислены интервалы, относящихся к данным группам. При необходимости можно откорректировать интервалы вручную средствами SIS II.

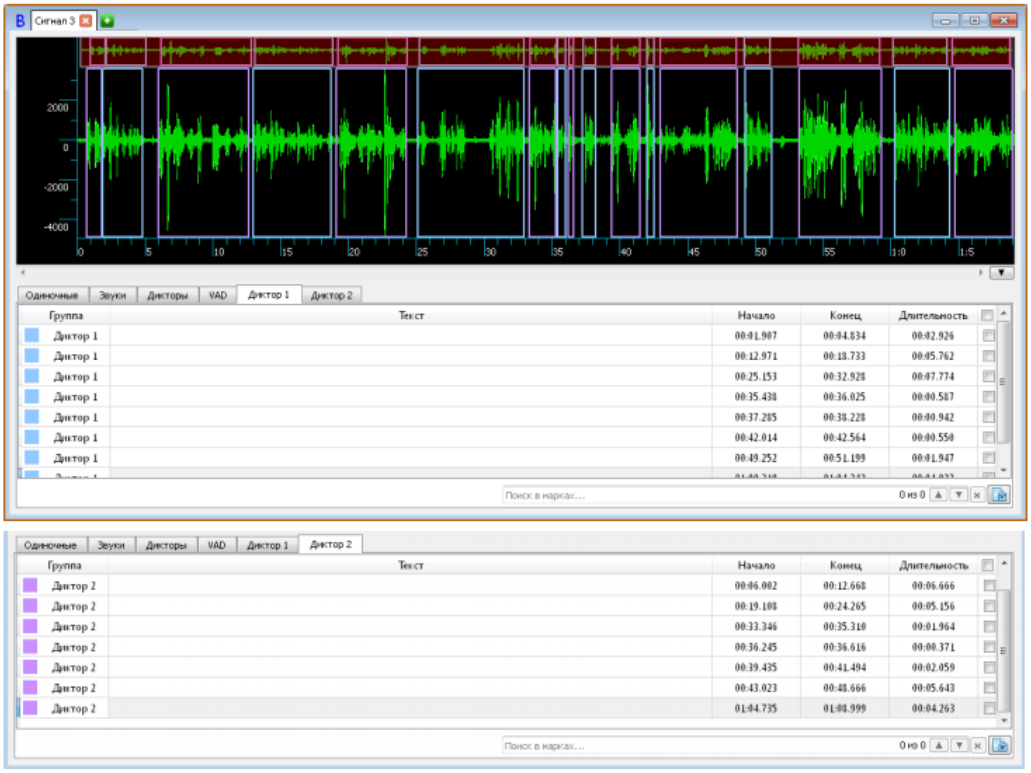



Рисунок 2 – Окно данных и вкладки списка фрагментов речи дикторов

Общие количество марок и общую их длину можно получить, если выбрать группы с названием меток для каждого диктора на вкладке Марки панели управления.

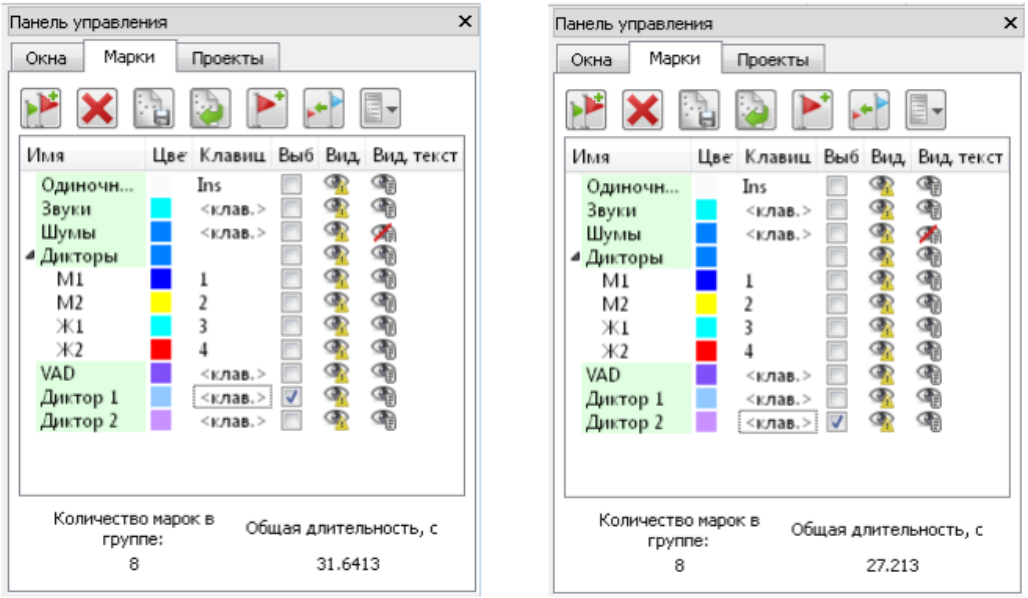



Рисунок 3 – Марки, отмечающие участки фонограммы, содержащие речь каждого диктора

В том случае, если разделение речи дикторов выполнено неточно, т.е. границы фрагментов речи на осциллограмме не соответствуют их реальному положению, существует возможность проведения коррекции.

Для сдвига одной из границ интервала наведите курсор мыши на эту границу, нажмите на клавиатуре клавишу Shift и, удерживая нажатыми клавишу Shift и левую кнопку мыши, переместите границу парной марки в нужное место.

Для сдвига всего интервала наведите курсор мыши на одну из границ интервала, нажмите на клавиатуре клавишу Ctrl и удерживая нажатыми клавишу Ctrl и левую кнопку мыши, переместите марку интервала в нужное место.

Чтобы удалить марку интервала, воспользуйтесь одним из способов:

1) Наведите курсор мыши на одну из границ удаляемой марки и нажмите клавиши Ctrl+Delete.

2) Наведите курсор мыши на одну из границ удаляемой марки, нажмите правую кнопку мыши и в появившемся контекстном меню выберите пункт Удалить марку

## 2.2 Выполнение сравнения

### 2.2.1 Автоматическое сравнение

Для автоматической идентификации диктора, необходимо выбрать пункт Автоматическое сравнение в меню Модули.

В диалоговом окне Автоматическое сравнение (рис. 4) выбрать файлы для сравнения в выпадающих списках Файл 1 и Файл 2, выбрать источник сигнала (Микрофон или Телефон) и нажать кнопку Сравнить.

### 2.2.2 Сравнение на основе метода основного тона

Сравнение на основе метода ОТ возможно только в случае совпадения эмоционального состояния.

Для выбора скорректированного основного тона для сравнения установить флаг Использовать для модели ОТ.

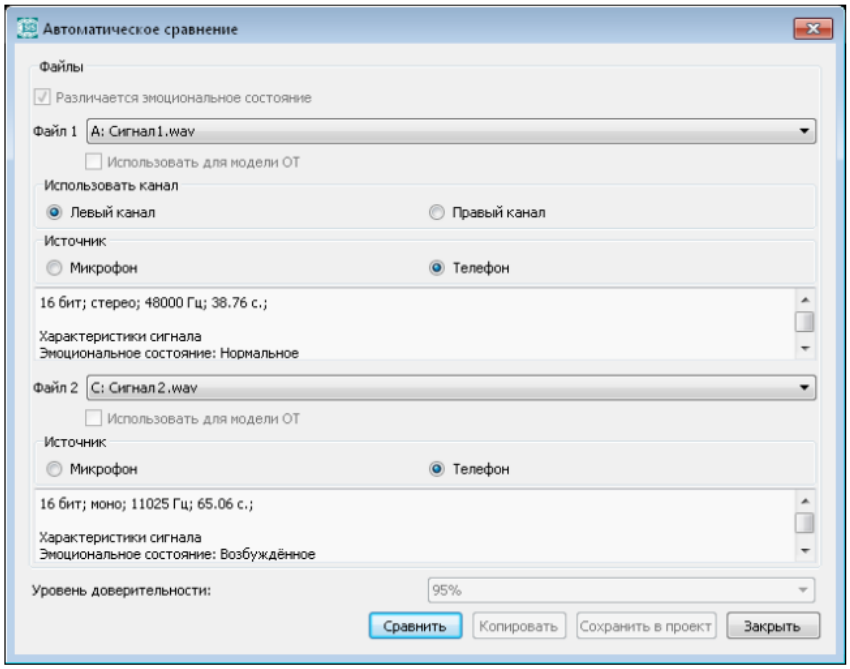



Рисунок 4 – Пример окна «Автоматическое сравнение» до начала выполнения операции сравнения

Для отмены операции идентификации нажать кнопку Закрыть. Перед началом работы с данным модулем рекомендуется запустить модуль Детектирования речи для каждого сигнала, предполагаемого для дальнейшей процедуры автоматической идентификации.

Данный модуль проводит автоматическую сегментацию сигналов на участки речи, пауз и шума. Обычно целесообразно проверить и при необходимости откорректировать вручную результаты работы этого модуля. При сегментации все шумы и паузы будут исключаться из речевого сигнала аналогично тому, как это происходит в модуле детектирования речи  при установке всех флажков на его панели управления. Результат детектирования шумов за пределы модуля не выдаётся и в данном модуле не может быть проверен и откорректирован оператором. В случае слишком короткого или низкокачественного сигнала чистой речи может оказаться недостаточно для идентификации. В этом случае целесообразно просмотреть и по возможности откорректировать результаты сегментации речи с использованием модуля «Детектирование речи». Процесс идентификации требует определённого времени для построения моделей и отображается в окне Выполнение заданий и в заголовке окна Автоматическое сравнение. Процесс можно прервать, если нажать кнопку справа от индикатора хода выполнения задания в окне Выполнение заданий.

### 2.3 Результаты идентификации

После окончания идентификации результаты отобразятся в таблице окна Автоматическое сравнение (рис. 5).

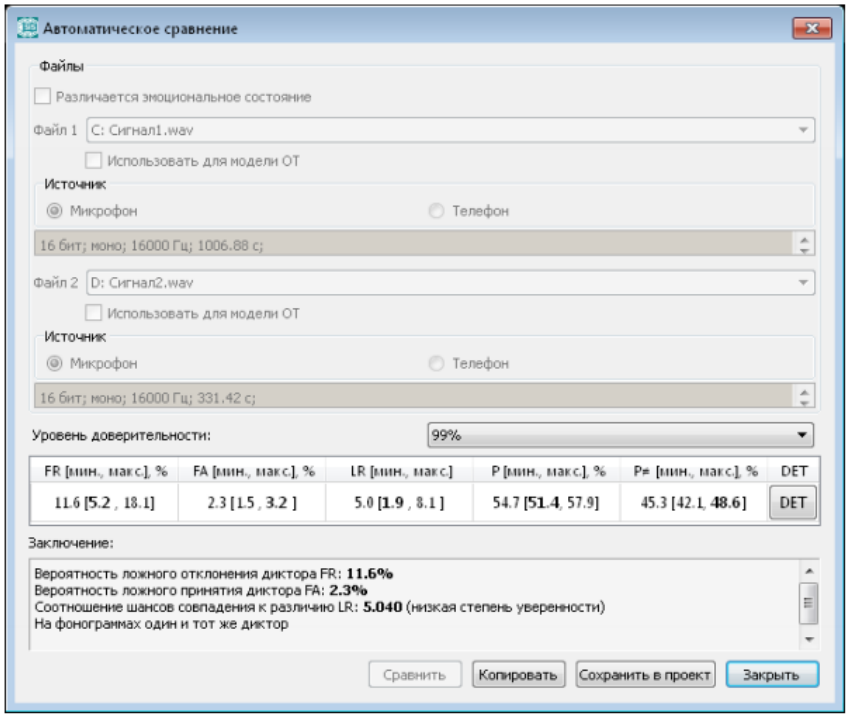



Рисунок 5 – Пример окна «Автоматическое сравнение» после выполнения операции сравнения

Для получения подробных результатов для различных методов наведите курсор на поле результатов, после чего отобразиться всплывающее окно (рис. 6).

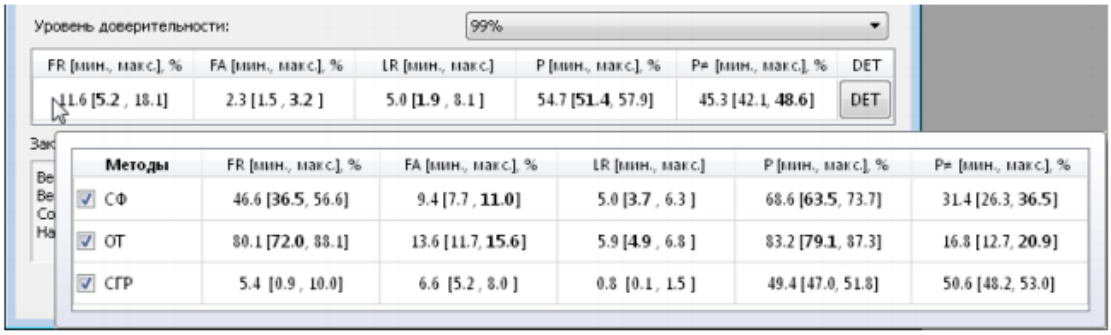



Рисунок 6 – Результаты операции сравнения для различных методов

Все результаты идентификации носят вероятностный характер, и поэтому для каждой характеристики имеется некоторый диапазон, куда при обнаруженной мере близости между сравниваемыми сигналами попадает ее значение при выбранном уровне статистической доверительности, который задается в выпадающем списке Уровень доверительности. В таблице результатов приводятся средние и возможные

при данном уровне доверительности максимальные и минимальные значения величин. Пояснения относительно доверительных интервалов приводятся в приложении Б. Соответствующие принятому идентификационному решению значения каждой характеристики отмечены жирным шрифтом. Например, при установленном тожестве дикторов внутри интервалов возможных значений для FR и P выбираются (являются результатом идентификации) минимальные значения, а для остальных характеристик – максимальные. В данной таблице: FR – False Rejection («ложное отклонение»), интегральная вероятность ложного принятия совпадающих дикторов за различающихся. FA – False Acceptance («ложное принятие»), интегральная вероятность ложного принятия различающихся дикторов за совпадающих. LR – Likelyhood Ratio («отношение правдоподобия»), отношение шансов (вероятности) совпадения дикторов к шансам (вероятности) различия дикторов. P – псевдовероятность совпадения дикторов. P≠ – псевдовероятность различия дикторов. Результаты сравнения можно скопировать в буфер обмена, нажав на кнопку , и вставить в отчёт в текстовом редакторе. Также результаты сравнения могут быть сохранены в текущий проект. Для этого нажмите кнопку . Чтобы сохранить результаты автоматического сравнения в проект, в программе должен быть, по крайней мере, один активный проект.

Для получения графиков FR-FA и DET (рис. 8) по каждому из методов нажмите кнопку в строке данного метода.

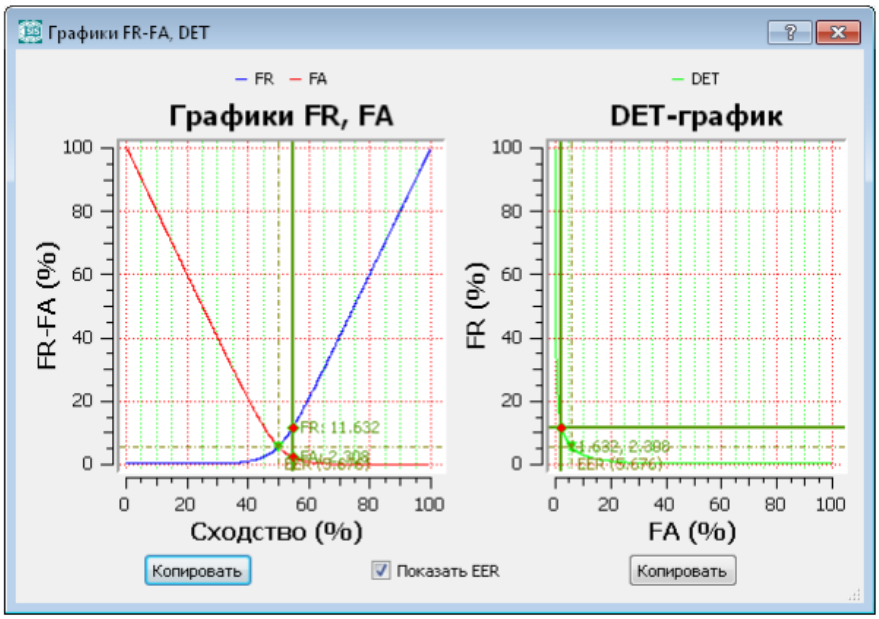



Рисунок 7 – Примеры графиков FR-FA и DET Установка флажка

Показать EER отображает или убирает на графиках значение EER. Кнопки позволяют копировать в буфер обмена каждый из графиков, чтобы затем вставить их в отчёт в текстовом редакторе.

### 2.4. Обработка сигналов

В случае, когда в ходе работы с сигналами были выделены постоянными марками и отмечены в комментарии к ним одинаковые слова, то программа позволяет найти их в двух загруженных в настоящий момент в редактор сигналах.

Для того, чтобы найти одинаковые слова необходимо:

- В меню Сервис выбрать команду Поиск общих слов.
- Появится окно Поиск общих слов.
- В выпадающих списках выбрать Первый сигнал: и Второй сигнал: данного окна выбрать сравниваемые сигналы и нажать кнопку Применить.
- Рабочее поле окна будет разделено на две колонки, которые озаглавлены именами выбранных сигналов. Ниже в колонках перечисляются совпадающие комментарии с указанием соответствующего им интервала в сигнале.
- Если необходимо посмотреть комментарий к слову нужно дважды щёлкнуть левой кнопкой мыши по найденному комментарию (слову) в одной из

колонок, то вкладка, содержащая данный сигнал, станет активной, а интервал, соответствующий выбранному слову, будет выделен как фрагмент и отображён в видимой области соответствующего окна данных.

Для выполнения обработки сигналов с использованием криминалистического исследования фонограмм речи «ИКАР Лаб» необходимо произвести ряд действий:

- Обработка сигналов осуществляется с использованием команд меню Обработка или соответствующих им пиктограмм на панели инструментов.
- Операции обработки применяются к данным, содержащимся в активной вкладке.
- После выбора всех параметров для запуска процесса обработки следует нажать кнопку Применить.
- Чтобы закрыть окно с параметрами без выполнения операции обработки сигнала, нажмите кнопку Закрыть в правом верхнем углу диалогового окна.

### 2.5 Нормализация амплитуды

Под нормализацией понимается умножение на константу и сдвиг сигнала в каждой точке таким

образом, что максимум амплитуды сигнала становится равным заданному, либо все значения сигнала попадают в заданный интервал.

Нормализация может использоваться:

- перед прослушиванием – для приведения сигнала к разрядной сетке цифро-аналогового преобразователя или для того, чтобы повысить громкость;
- перед фильтрацией – чтобы уменьшить погрешность округления.

Чтобы выполнить нормализацию амплитуды, необходимо выбрать в меню Обработка Нормализация на горизонтальной панели инструментов.

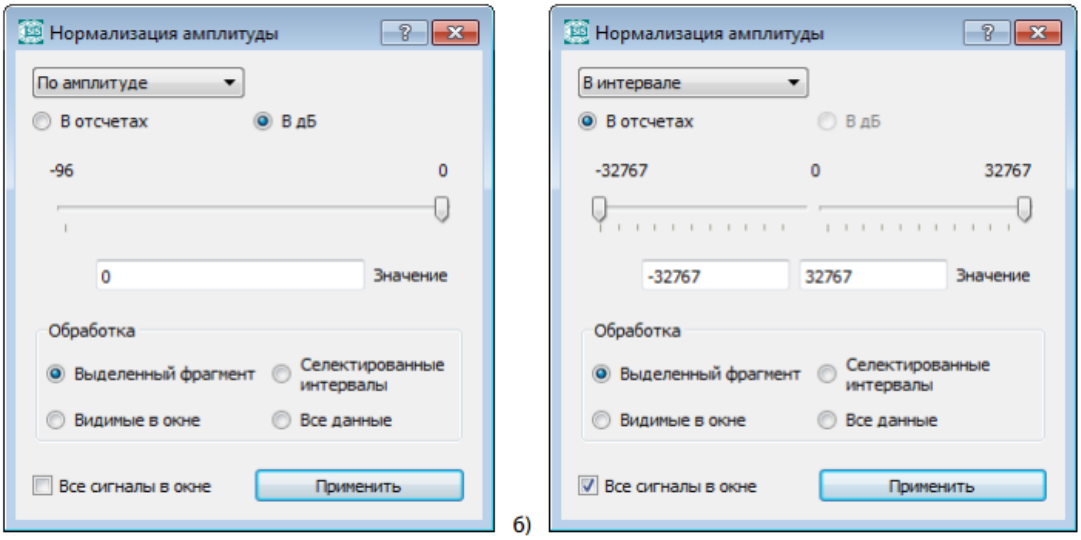



Рисунок 8 – Диалоговое окно «Нормализация амплитуды»

В диалоговом окне Нормализация амплитуды (рис. 8) задайте следующие параметры:

1) Выберите в выпадающем списке выполнять обработку По амплитуде (рис. 8, а) или В интервале (рис. 8, б).

2) Выберите единицу измерения амплитуды или интервала: в отсчётах или в децибелах. При выборе в дБ максимальное значение на ползунке, соответствующее 32 767 отсчётам, устанавливается как 0 дБ;

3) Используя ползунок, укажите конкретное значение амплитуды или интервала в выбранных

единицах измерения. Значения также можно задавать с клавиатуры в соответствующих окнах.

4) В поле Обработка выберите область обработки данных:

– выделенный фрагмент;

– селектированные интервалы;

– видимые в окне;

– все данные.

Если окно содержит данные нескольких сигналов, то при установке флажка перед пунктом

Все сигналы в окне заданные параметры будут применены ко всем сигналам.

## 2.6 Линейное преобразование

В том случае, если громкость речи на протяжении фонограммы монотонно возрастает или затухает можно использовать операцию линейного преобразования.

Под линейным преобразованием понимается умножение сигнала на линейную функцию, которая

задается двумя значениями: на левом и правом концах.

Чтобы выполнить линейное преобразование амплитуды, выберите команду в меню Обработка Линейное преобразование.

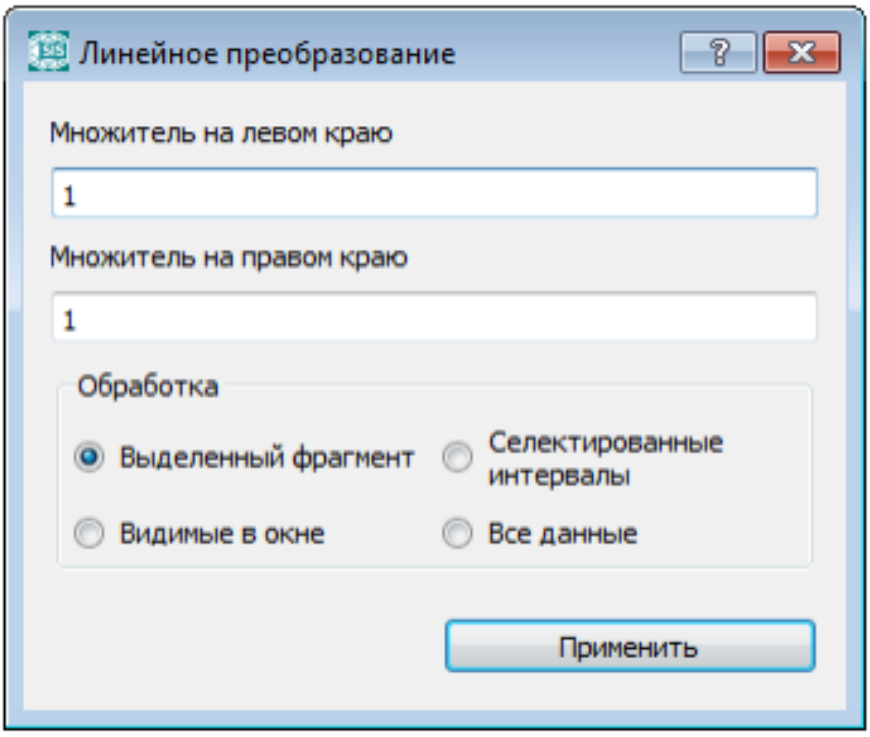



Рисунок 9– Диалоговое окно «Линейное преобразование»

В диалоговом окне Линейное преобразование (рис. 9) задайте следующие параметры:

1) Множитель на левом краю.

2) Множитель на правом краю.

3) В поле Обработка выберите область обработки данных:

– выделенный фрагмент;

– селектированные интервалы;

– видимые в окне;

– все данные.

Если при обработке 16-разрядных сигналов значение одного из множителей таково, что результат

операции в одной из точек сигнала может выйти за разрядную сетку целого числа (минус 32 768,

плюс 32 767), в левом углу строки информации появится предупреждение «Переполнение» и

операция выполняться не будет.

**2.7 Передискретизация**

Данная операция заключается в изменении частоты дискретизации исходного сигнала.

Деление частоты дискретизации обычно применяется, чтобы повысить спектральное разрешение в низкочастотной области. Это бывает необходимо, чтобы проверить фонограмму на перезапись и отсутствие склеек. В обычном речевом сигнале с частотой дискретизации, например, 10 000 Гц можно при помощи среднего спектра мощности увидеть отдельно два спектральных пика, если между ними не менее 10 Гц (размер кадра – 2048 отсчётов, окно Хэнна).

Если понизить частоту дискретизации примерно в 80 раз (до 125 Гц), то можно разделить пики, отстоящие на 0,12 Гц. Такого разрешения достаточно, чтобы увидеть, как двоится и разрывается пик сетевой частоты (50 Гц).

Изменение частоты дискретизации применяется, когда сигнал был неудачно записан. Для произвольной частоты это длительная, но иногда необходимая процедура.

Чтобы выполнить передискретизацию, выберите команду в меню Обработка Передискретизация на горизонтальной панели инструментов.

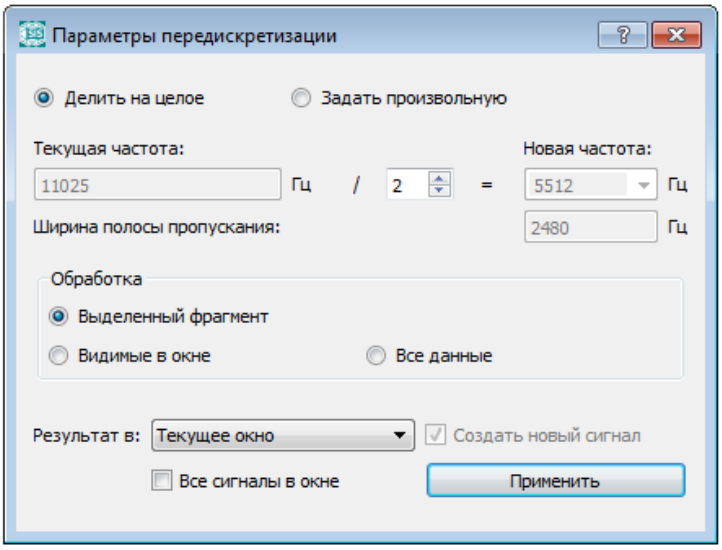



Рисунок 10 – Диалоговое окно «Параметры передискретизации»

В диалоговом окне Параметры передискретизации (рис. 10) задайте следующие параметры:

1. Делитель частоты для варианта Делить на целое или новую частоту дискретизации для варианта Задать произвольную. Произвольную частоту дискретизации можно выбрать из выпадающего списка или используя клавиатуру задать любое её значение в поле Новая частота.

2. Размещение результата в текущем или новом окне.

3. Необходимость создания нового сигнала: установкой флажка Создать новый сигнал.

4. В поле Обработка выберите область обработки данных:

– выделенный фрагмент;

– видимые в окне;

– все данные.

Если окно содержит данные нескольких осциллограмм, то при установке флажка перед пунктом Все сигналы в окне заданные параметры обработки будут применены ко всем осциллограммам

## 2.8 Темпокоррекция

Темпокоррекция позволяет получить сигнал, скорректированный по темпу воспроизведения, но с прежней высотой основного тона. Пользоваться данной функцией рекомендуется только для речи, причем относительно низкочастотной по сравнению с частотой дискретизации. Не рекомендуется замедлять высокий поющий женский голос, записанный на частоте дискретизации 8 кГц. Необходимо учитывать, что при замедлении в 3 раза белый шум превращается в тональный, а голос становится «пьяным».

Чтобы выполнить темпокоррекцию, выберите команду в меню Обработка Темпокоррекция на горизонтальной панели инструментов.

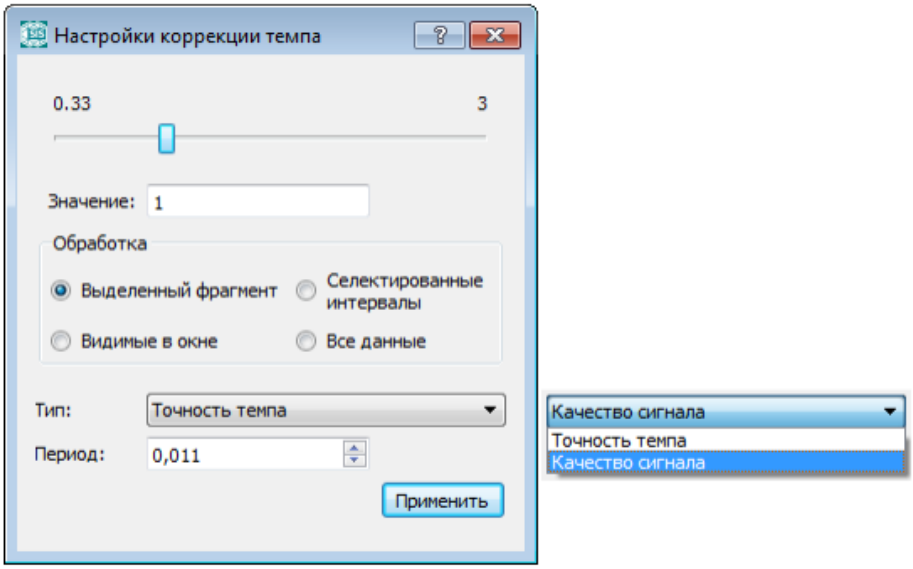



Рисунок 11 – Диалоговое окно «Настройки коррекции темпа»

В диалоговом окне Настройки коррекции темпа (рис. 11) задайте следующие параметры:

1) Значение скорости воспроизведения от 0,33 до 3 с использованием ползунка или поля Значение. Значение будет выдерживаться с относительной погрешностью 10-14 (если выбран тип Точность темпа).

2) Тип: Качество сигнала или Точность темпа. Для сохранения высокого качества выходного сигнала некоторые участки речи нельзя размножать

или удалять. Если выбрать пункт Качество сигнала, то такие участки будут сохраняться. Однако их сохранение приводит к тому, что заданный коэффициент

коррекции темпа соблюдается неточно (примерно с точностью до 0,01). Коррекция темпа отклоняется от заданной ещё и потому, что размножаемые (или удаляемые) участки все имеют разную длину. Если выбрать пункт Качество сигнала, данный эффект будет корректироваться.

Если выбрать пункт Точность темпа, то программа будет поддерживать точное значение коэффициента коррекции темпа даже в ущерб качеству.

3) Период – предполагаемый период основного тона в секундах. При увеличении этого параметра огибающая выходного сигнала становится пилообразной, и возникают специфические призвуки; при уменьшении возникают пощёлкивания.

4) В поле Обработка выберите область обработки данных:

– выделенный фрагмент;

– селектированные интервалы;

– видимые в окне;

– все данные.

### 2.9 Шумоочистка

Операция шумоочистки позволяет удалить из сигнала широкополосные и тональные помехи. Чтобы выполнить шумоочистку, выберите команду в меню Обработка Шумоочистка.

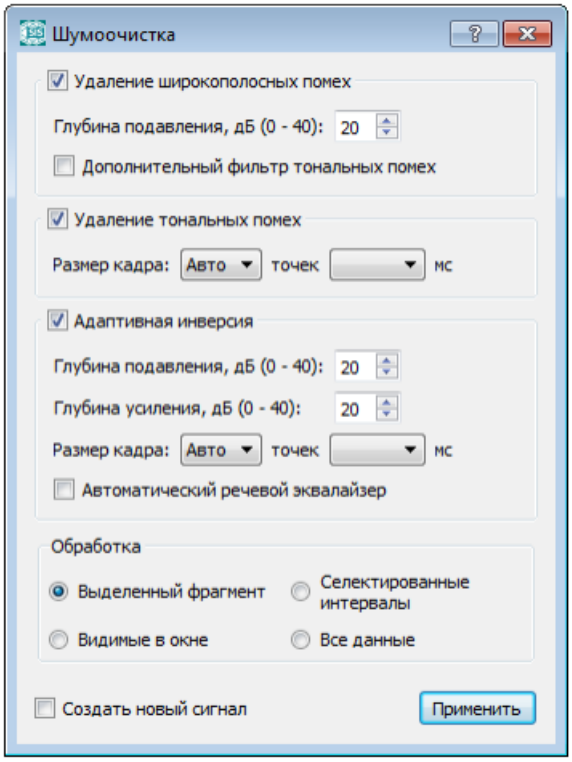



Рисунок 12 – Диалоговое окно «Шумоочистка»

В диалоговом окне Шумоочистка (рис. 12) задайте следующие параметры.

1) Для удаления широкополосных помех:

– установите флажок Удаление широкополосных помех;

– выберите глубину подавления от 0 до 40 дБ;

– установите или снимите флажок Дополнительный фильтр тональных помех.

2) Для удаления тональных помех:

– установите флажок Удаление тональных помех;

– выберите размер кадра в точках (Авто, 256, 512, 1024 или 2048) или в миллисекундах (их количество зависит от частоты дискретизации).

3) Установите флажок Адаптивная инверсия (инверсный фильтр), чтобы применить следующие параметры:

– Глубина подавления задает предельное ослабление спектральных компонент исходного сигнала, например, подавление гармоник помехи.

– Глубина усиления задает предельное усиление спектральных компонент исходного сигнала, например, подъема сигнала в области высоких частот.

– Размер кадра (то есть, порядок размера окна БПФ) определяет степень гладкости/селективности фильтра. Увеличение порядка приводит к увеличению частотного разрешения фильтра, улучшению подавления тональных помех. Уменьшение порядка делает частотную характеристику фильтра более гладкой.

– Установите флажок Автоматический речевой эквалайзер для автоматического приведения среднего спектра сигнала к модельному речевому спектру. В противном случае выполняется функция спектрального инверсного фильтра. Модельный средний спектр речи имеет плоский участок в интервале частот 400–1000 Гц и спадающую характеристику вне этого интервала. В низкочастотной области крутизна спада составляет 6 дБ на октаву относительно 400 Гц, в высокочастотной области крутизна спада составляет 6 дБ на октаву относительно 1000 Гц.

4) В поле Обработка выберите область обработки данных:

– выделенный фрагмент;

– селектированные интервалы;

– видимые в окне;

– все данные.

Чтобы очищенный от шумов сигнал сохранился как новый, установите флажок Создать новый сигнал.

**Задание на практическую часть**

1. Ознакомится с теоретической частью работы.
2. Произвести разделение речи дикторов.
3. Сделать автоматическое сравнение
4. Сделать обработку сигнала всеми представленными методами.
5. Составьте отчёт о выполнении лабораторной работы, выполнив все действия, описанные в практической части, представив скриншоты. Оформите отчёт согласно шаблона, представленного на последних страницах.

**Контрольные вопросы:**

1. Какие методы сравнения использует модуль «Автоматическое сравнение»?
2. На чем основан спектрально-формантный метод идентификации дикторов?
3. Каким образом строится модель голоса при использовании метода полной изменчивости?
4. Для чего следует проводить нормализацию амплитуды?
5. В каких случаях целесообразно использование линейного преобразования?
6. Что такое передискретизация?
7. Что остается неизменным при темпокоррекции?

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1,2

*Дополнительная:* 1-34

*Методическая:*1

*Программное обеспечение:* 1-4

## Практическое занятие № 5-9

**Тема:** Исследование модулей «Сравнение формант» и «Сравнение основного тона» комплекса криминалистического исследования фонограмм речи «ИКАР Лаб»

**Цель занятия:**

Ознакомиться с теоретическим материалом предназначенным для формирования у обучающегося базовых знаний для дальнейшего изучения комплекса криминалистического исследования фонограмм речи «ИКАР Лаб».

**Формируемые компетенции:** ПК-1

**Структура лабораторной работы**

**Вводная часть**

| | |
|---|---|
| Проверка готовности студентов к лабораторной работе | 10 мин |
| Вступительная часть | 10 мин |

**Вопросы (задачи), подлежащие исследованию**

| | |
|---|---|
| Изучение теоретических данных | 40 мин |

**Заключительная часть**

| | |
|---|---|
| Защита отчетов по лабораторной работе | 20 мин |
| Подведение итогов | 5 мин |
| Задание студентам для самостоятельной работы | 5 мин |

# 1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Аппаратно-программный комплекс ИКАР Лаб предназначен для решения широкого круга задач анализа звуковой информации, востребованного в специализированных подразделениях правоохранительных органов, лабораториях и центрах судебной экспертизы, службах расследования летных происшествий, исследовательских и учебных центрах. Первая версия продукта была выпущена в 1993 году и явилась результатом совместной работы ведущих аудиоэкспертов и разработчиков программного обеспечения. Входящие в состав комплекса специализированные программные средства обеспечивают высокое качество визуального представления фонограмм речи. Современные алгоритмы голосовой биометрии и мощные инструменты автоматизации всех видов исследования фонограмм речи позволяют экспертам существенно повысить надежность и эффективность экспертиз. Входящая в комплекс программа SIS II обладает уникальными инструментами для идентификационного исследования: сравнительное исследование диктора, записи голоса и речи которого предоставлены на экспертизу и образцов голоса и речи подозреваемого. Идентификационная фоноскопическая экспертиза основывается на теории уникальности голоса и речи каждого человека. Анатомическое факторы: строение органов артикуляции, форма речевого тракта и ротовой полости, а также внешние факторы: навыки речи, региональные особенности, дефекты и др.

Набор включает следующие программные модули, входящие в состав **SIS II**:

1) Модуль «Методика», представляющий собой совокупность всех модулей.

2) Модуль оценки качества фонограммы «Характеристики сигнала» позволяет автоматически вычислить основные параметры звукового сигнала фонограммы в целом и оценить ее пригодность для дальнейших исследований.

3) Модуль разделения речи дикторов «Разделение дикторов в диалоге» позволяет выполнять автоматическую маркировку речевых сегментов по дикторам на записях естественной речи.

4) Модуль поиска речевых участков «Детектирование речи» позволяет автоматически выделять в фонограмме речевые, шумовые участки и паузы.

5) Модуль «Автоматическое сравнение» выполняет автоматическую идентификацию личности по голосу тремя методами с использованием обобщающего решения.

6) Модуль «Сравнение формант» позволяет автоматизировать процесс идентификации личности по голосу на основе метода сравнения формант.

7) Модуль «Сравнение основного тона» позволяет автоматизировать процесс идентификации личности по голосу на основе сравнения параметров мелодических контуров голоса сравниваемых дикторов.

8) Модуль «Сравнение речевых признаков» позволяет автоматизировать процесс идентификации личности по голосу на основе экспертного сравнения лингвистических характеристик речи сравниваемых дикторов.

9) Модуль «Общее решение» позволяет принять общее решение относительно идентификации личности по голосу на основе результатов работы каждого из использованных модулей идентификации дикторов.

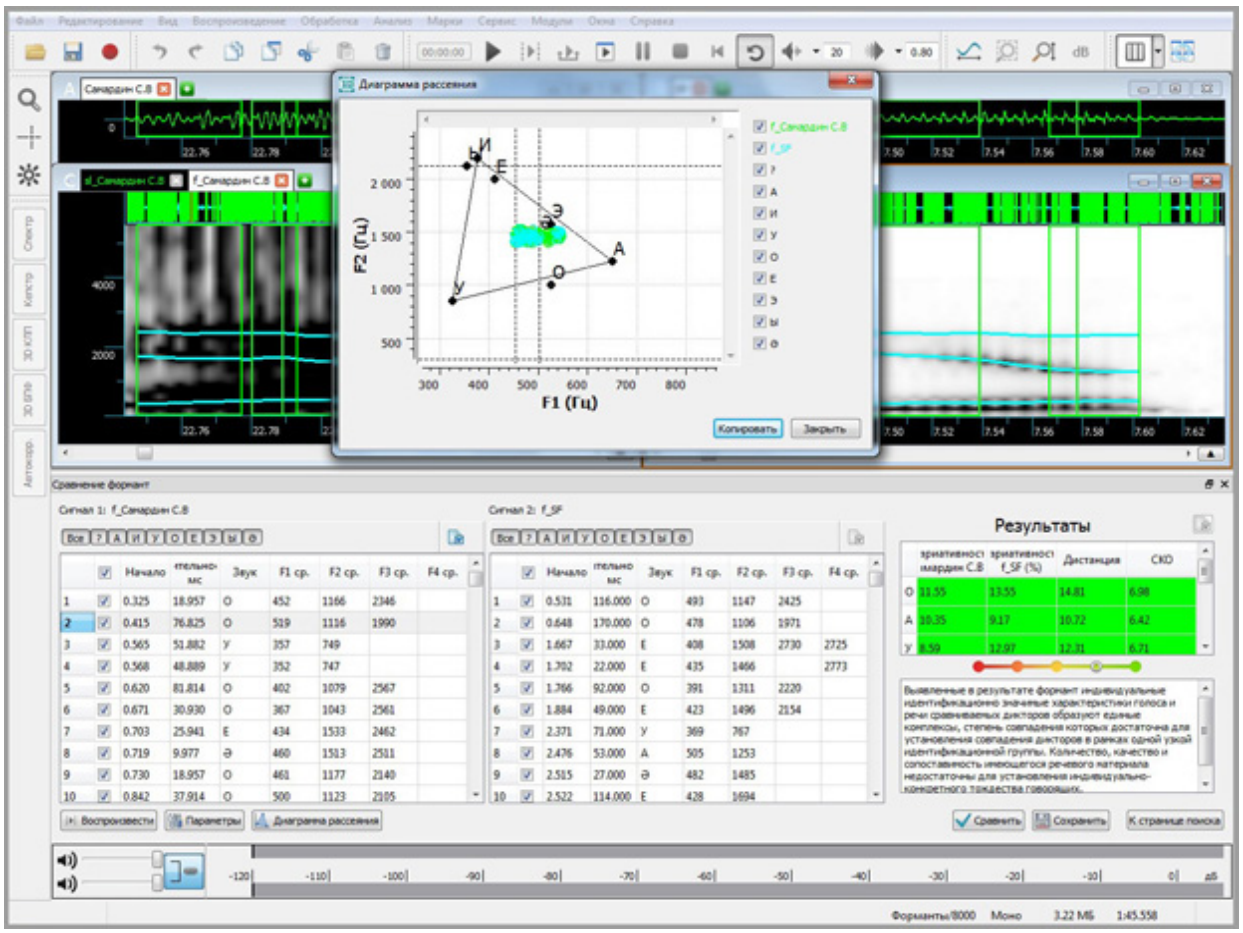



Рисунок 1 – Интерфейс программы SIS II

## 1.1 Модуль «Сравнение формант»

Модуль «Сравнение формант» позволяет автоматизировать различные методы сравнения формантных характеристик речевого сигнала. Возможно сравнение формантных частот как для совпадающих фонем (фонетико-спектральный подход, микроанализ гласных в сопоставимых трезвучиях) так и для одинаковых мгновенных артикуляций (конфигураций речевого тракта) в рамках произвольного фонетического контекста. Анализ соотношений формантных частот на сопоставимых опорных фрагментах речевого сигнала может применяться для идентификации диктора, говорящего на языке, не знакомом эксперту, а также для сравнения разноязычных фонограмм.

Надёжность метода сравнения формант в существенной степени зависит от того, насколько корректно построены формантные траектории. Автоматическое определение формантных траекторий осуществляется в **SIS II** путём применения

модуля «Выделение формант методом БПФ». Имеется возможность поправить вычисленные форманты вручную, а также обозначить траектории формант самостоятельно, без включения модуля выделения формант.

Стандартно процедура построения формант и их коррекции состоит из следующих шагов:

– Вычисление среднего спектра исследуемого сигнала.

– При наличии существенных неоднородностей среднего спектра, в частности, «завалов» на низких (<500Гц) и высоких (>3400Гц) частотах, – выравнивание спектра путем построения в окне спектра инверсного фильтра.

### 1.2 Модуль «Сравнение основного тона»

Модуль «Сравнение основного тона» позволяет автоматизировать процесс идентификационного исследования речевых сигналов на основе структурного анализа мелодических контуров речевого сигнала сравниваемых фонограмм. Модуль предназначен для сравнения речевых образцов на основе параметров реализации однотипных элементов структуры мелодического контура. Для анализа предусмотрено 18 типов фрагментов контура и 15 параметров их описания. Для разных типов используются разные наборы параметров.

Параметры выделяемых экспертом на графике основного тона однотипных участков контура, сопоставимых с точки зрения реализационной специфики, коммуникативной и эмоционально - стилистической нагрузки, вычисляются автоматически, данные заносятся в таблицу.

Сравнение осуществляется по каждому из используемых типов на основе пороговых значений, рассчитанных для параметров каждого типа элемента контура. Далее результаты сравнения отдельных типов суммируются для получения общего решения относительно тождества либо различия голосов. При вычислении общего результата учитываются весовые коэффициенты, приписанные каждому параметру и типу фрагмента мелодического контура.

Если показатель оценки сходства существенно превышает показатель различий, то высока вероятность тождества голосов. При высокой степени различий

между фонограммами формулируется решение о различии голосов. При незначительных различиях в оценках (менее 10 %) выдаётся сообщение о том, что решение принять невозможно.

Предварительная подготовка фонограмм для сравнения данным методом заключается в получении корректных графиков основного тона (ОТ) голоса. Получение данных графиков осуществляется в **SIS II** автоматически путём применения модуля «Выделение основного тона».

Для достижения заявленной надёжности идентификации по каждому из типов фрагментов мелодического контура должны быть соблюдены определённые условия, которые излагаются ниже:

1. Метод предназначен для сравнительного анализа фонограмм, содержащих речь нейтрального стиля, без ярко выраженной эмоционально-модальной окраски.

2. Заявленная надёжность метода достигается при сравнении фрагментов утвердительных высказываний одного стиля (спонтанная речь сравнивается со спонтанной речью, чтение – с чтением).

Результат сравнения типа «спонтанная речь – чтение» зависит от индивидуальных особенностей чтения конкретного диктора.

3. Ограничения по длительности имеются только для длительных речевых фрагментов – в стандартном случае не менее 60 секунд; в отдельных случаях возможно использование фонограмм длительностью 30–60 секунд.

Для остальных типов фрагментов контура важна не длительность сама по себе, а представленность в фонограмме целевых структур для анализа – ядерных тонов, предшкал, шкал, пауз хезитации и т. д. В зависимости от темпа речи, от акцентно-ритмической структуры и сегментного состава достаточная длительность фонограммы может варьироваться от 15–20 секунд до нескольких минут.

Рекомендуемое число фрагментов каждого типа для анализа составляет 7–10. При низкой степени вариативности параметров возможно использование 5–7 фрагментов, однако дальнейшее сокращение числа измерений ведёт к существенному снижению надёжности метода.

4. Поскольку основой получения данных для анализа является кривая ОТ, с

технической точки зрения метод имеет те же ограничения, что и автоматический метод сравнения статистики ОТ: желательное соотношение сигнал/шум не менее 10–15 дБ, отсутствие реверберации на обеих фонограммах.

# 2. ПРАКТИЧЕСКАЯ ЧАСТЬ

## 2.1 Исследование модуля «Сравнение формант»

Чтобы применить метод сравнения формант, выберите меню **Модули Сравнение формант**.

В диалоговом окне (рис. 2) укажите пару сравниваемых сигналов с уже вычисленными формантами. Если их в программе всего два, модуль выбирает их автоматически. Если сигналов больше двух, то сравниваемые сигналы выбираются оператором из выпадающих списков.

Окна, в которых находятся выбранные сигналы, будут автоматически связаны по вертикали.

Кроме того, если ранее в данном проекте уже выполнялись сравнения с выбранным сигналом, то таблицы фрагментов для этого сигнала можно загрузить из ранее сохранённых сравнений, воспользовавшись выпадающим списком **загрузить из**.

Выберите один из предустановленных профилей обработки с помощью выпадающего списка. Профиль представляет собой готовую таблицу значений границ форматных частот для разных типовых случаев: мужские и женские голоса для русского языка, таблицы для английского и испанского языков, а также параметры принятия решения о сходстве/различия дикторов.

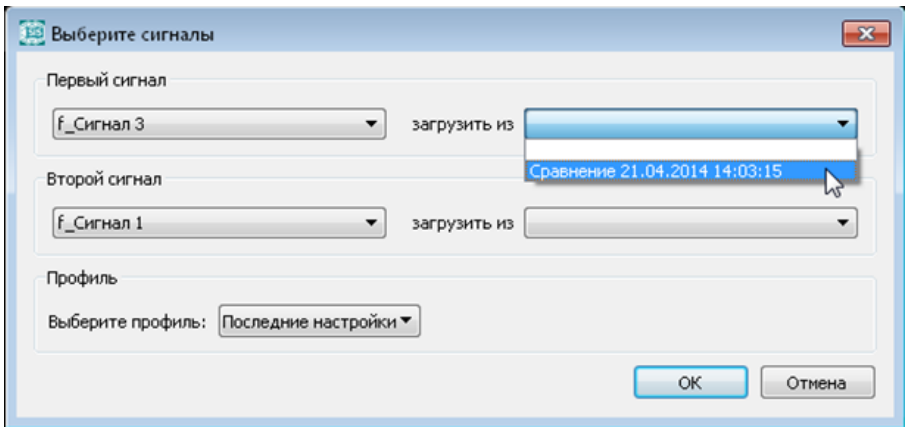



Рисунок 2 - Выбор сравниваемых сигналов

После выбора сравниваемых сигналов нажмите кнопку **ок**.

Откроется панель работы с модулем. Панель прикрепляется к нижней части главного окна **SIS II**, при этом открытые внутри него окна с данными, панели управления или окно спектра пропорционально меняют свой размер (рис. 3).

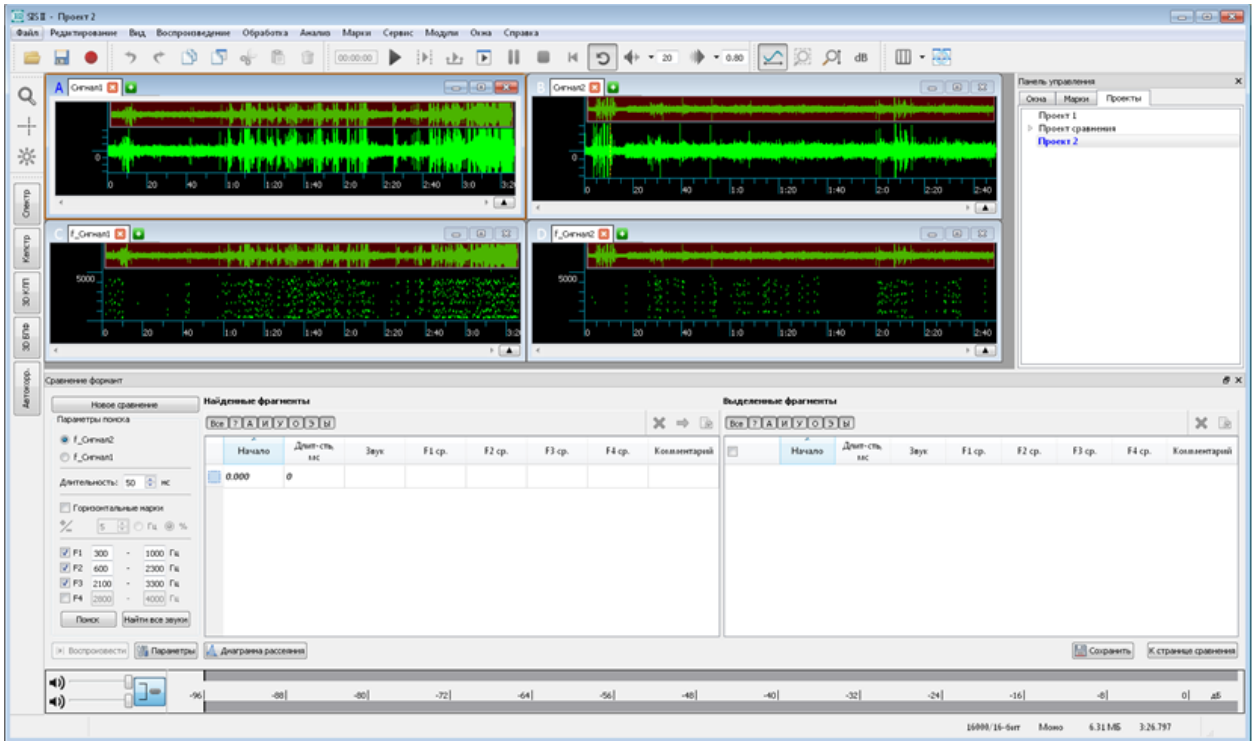


Рисунок 3 – Панель модуля формантного выравнивания внутри главного окна звукового редактора

Чтобы сделать панель модуля независимой от главного окна SIS II (рис. 4), следует нажать на значок в правом верхнем углу панели или дважды щёлкнуть левой кнопкой мыши на заголовке панели. Панель можно перемещать в любое место на экране монитора, удерживая нажатой на заголовке левую кнопку мыши.

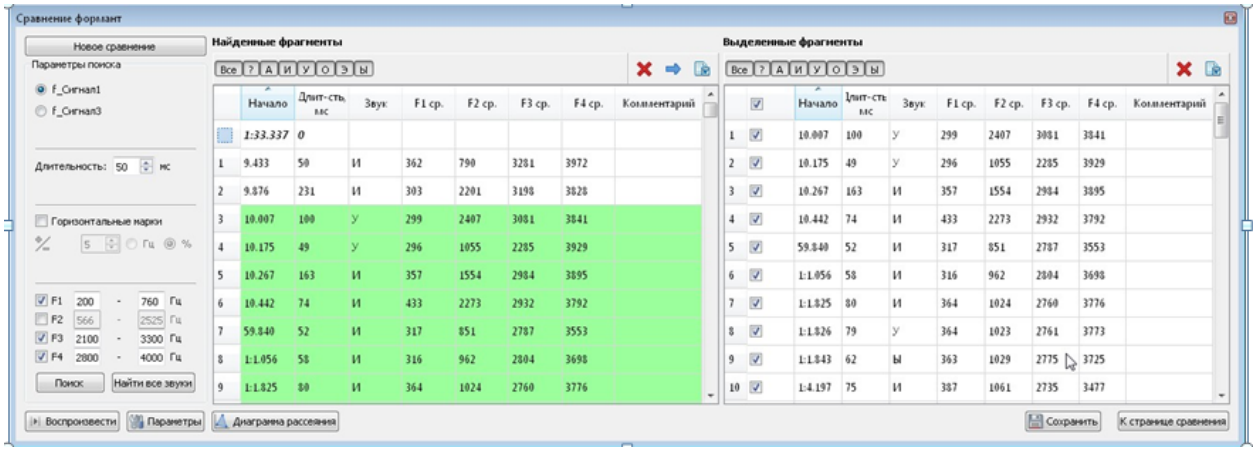



Рисунок 4 – Панель модуля в качестве отдельного независимого окна

При последующих запусках модуля предыдущее положение панели сохраняется. Чтобы прикрепить панель обратно к нижней части главного окна **SIS II**, следует снова дважды щёлкнуть на заголовке панели.

Чтобы выбрать другие сигналы (форманты) для сравнения, нажмите кнопку Новое сравнение и в диалоговом окне **Выберите сигналы** (см. рис. 2) осуществите выбор.

Для работы с данным модулем целесообразно использовать два монитора или монитор с большим экраном.

Во время работы с модулем может потребоваться задать отдельные параметры. Чтобы открыть окно параметров сравнения формант (рис. 29), нажмите кнопку Параметры.

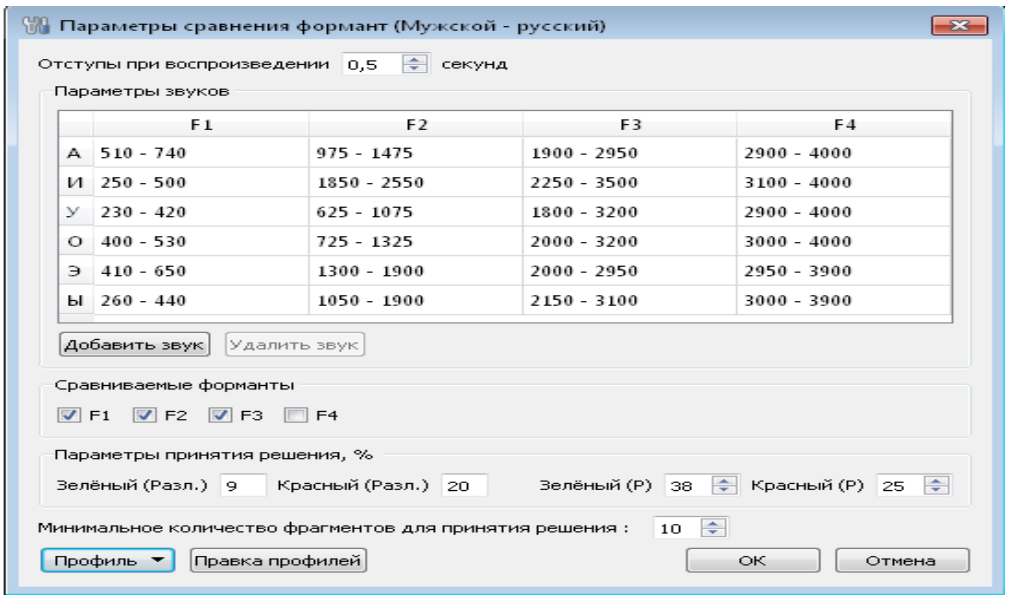



Рисунок 5 - Параметры сравнения формант

Окно позволяет задавать следующие параметры работы модуля:

1. Продолжительность проигрывания фонограммы в секундах до начала фрагмента и после него при прослушивании выбранного фрагмента. По умолчанию выставлено 0,5 секунды.

Воспроизведение выделенного в левой или правой половине таблицы фрагмента со сдвинутыми на заданную величину границами производится циклически при нажатии кнопки Воспроизвести. При повторном нажатии кнопки воспроизведение прекращается.

2. Любое сравнение формант в данном модуле производится только для занесенных в таблицу фрагментов, которым приписан один и тот же тип фонемы. Таким образом, до начала работы с модулем сравнения формант следует задать параметры типичных (обобщённых) формантных векторов для выбранных типов фонем. Диапазоны значений для образцов звуков приведены в таблице **Параметры звуков**. Например, при выборе профиля **Мужской > русский** для формант задаются диапазоны, показанные на рисунке 5. Необязательно задавать значения всех четырёх формант.

Оператор может убрать из таблицы отдельные звуки, если выделит соответствующую ячейку и нажмёт кнопку Удалить звук. Он также может добавить новые звуки. Для этого следует выполнить следующие действия:

а) Нажать на кнопку Добавить звук.

б) В поле **Название звука** диалогового окна **Новый звук** (рис. 6) указать название звука и нажать кнопку **ОК**.

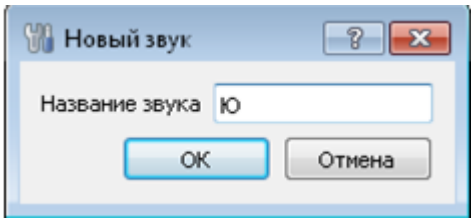



Рисунок 6– Диалоговое окно нового звука

в) Дважды щёлкнуть левой кнопкой мыши в ячейке соответствующей форманты добавленного звука и в появившихся полях ввести границы диапазона (рис. 7).

Рисунок 7 – Ввод значений диапазона форманты

г) Для сохранения введённых границ, щёлкнуть в любой соседней ячейке таблицы **Параметры звуков**.

Для исправления текущего значения той или иной формантной границы следует сделать двойной щелчок левой кнопки мыши, поместив указатель на выбранную в таблице ячейку. В появившемся окошке следует откорректировать желаемое значение частоты форманты и нажать **Enter**.

Можно задать минимальное количество фрагментов, участвующих в сравнении. Для этого укажите необходимое значение параметра **Минимальное количество фрагментов для принятия решения**.

Если количество участвующих в сравнении фрагментов для определенного звука меньше, чем указанное число, то решение по этому звуку не принимается и строчка со звуком в таблице результатов сравнения окрашивается серым.

Можно загрузить имеющиеся в программе готовые таблицы значений границ формантных частот для разных типовых случаев: мужские и женские голоса для русского языка, таблицы для английского и испанского языков. Для этого нужно в панели **Параметры** справа внизу нажать на надпись **Профиль** и выбрать желаемый профиль из выпадающего списка.

Чтобы создать и сохранить собственный профиль сначала необходимо задать в таблице **Параметры звуков** необходимые значения границ формант и наименования звуков. Границы диапазонов можно задать для одной или более формант. Затем следует нажать на надпись **Правка профилей** и затем **Сохранить текущий как.** Далее необходимо задать имя нового профиля. Записанный ранее профиль можно вызвать через кнопку **Профиль пользовательские**.

Для визуального представления использован особый вид графика, на котором отмечены все индивидуальные значения, принимаемые переменными – диаграмма рассеяния.

Чтобы открыть окно диаграммы рассеяния (рис. 8), нажмите кнопку Диаграмма рассеяния в нижней части панели модуля СФ.

В координатах частот первой и второй форманты на диаграмме рассеяния изображён треугольник гласных, построенный по средним значениям формант образцов наиболее удаленных друг от друга звуков: А, У, И.

По умолчанию на треугольник накладываются отображения формантных векторов всех выбранных фрагментов обоих анализируемых сигналов (для каждого сигнала своим цветом). Опции «Показывать область СКО» и «Показывать положение звуков» также по умолчанию отмечены. Для каждого звука рисуется закрашенный его цветом эллипс с центром в точке координат со средним значением формант и размерами, пропорциональными СКО по данной оси координат.

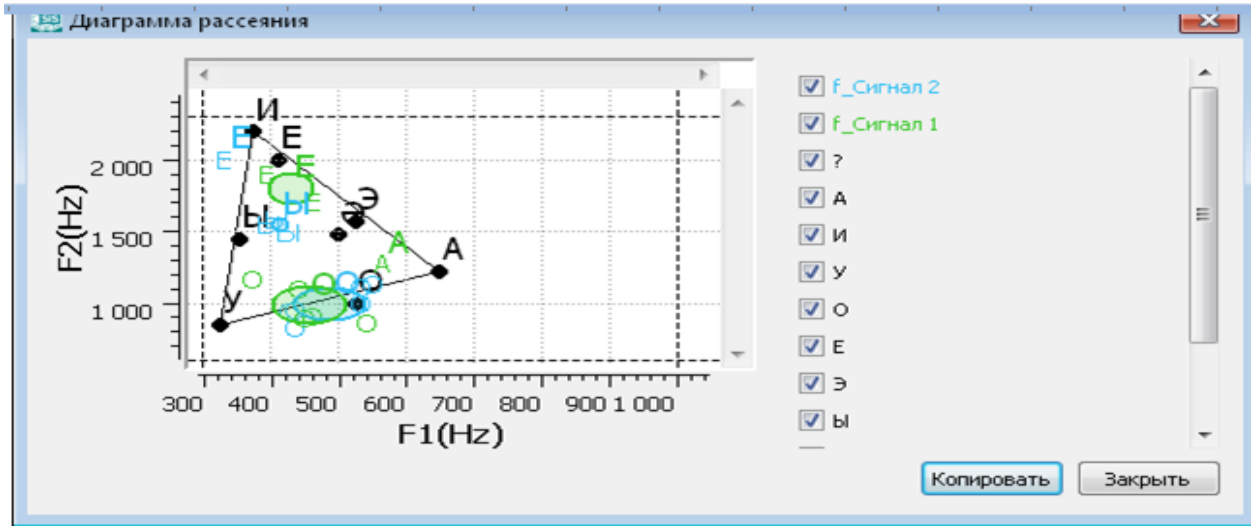



Рисунок 8 - Окно диаграммы рассеяния

Убирая те или иные флаги, оператор имеет возможность удалять с изображения диаграммы рассеяния отдельные звуки и области СКО, а также все звуки и области СКО, принадлежащие тому или иному диктору.

Размеры окна диаграммы рассеяния можно менять при помощи мыши так же, как любого окна операционной системы.

Имеется возможность, удерживая нажатой левую кнопку мыши, выделить для детального рассмотрения определённый фрагмент диаграммы рассеяния. При отпускании кнопки в окне отобразится только выделенный фрагмент (рис. 9).

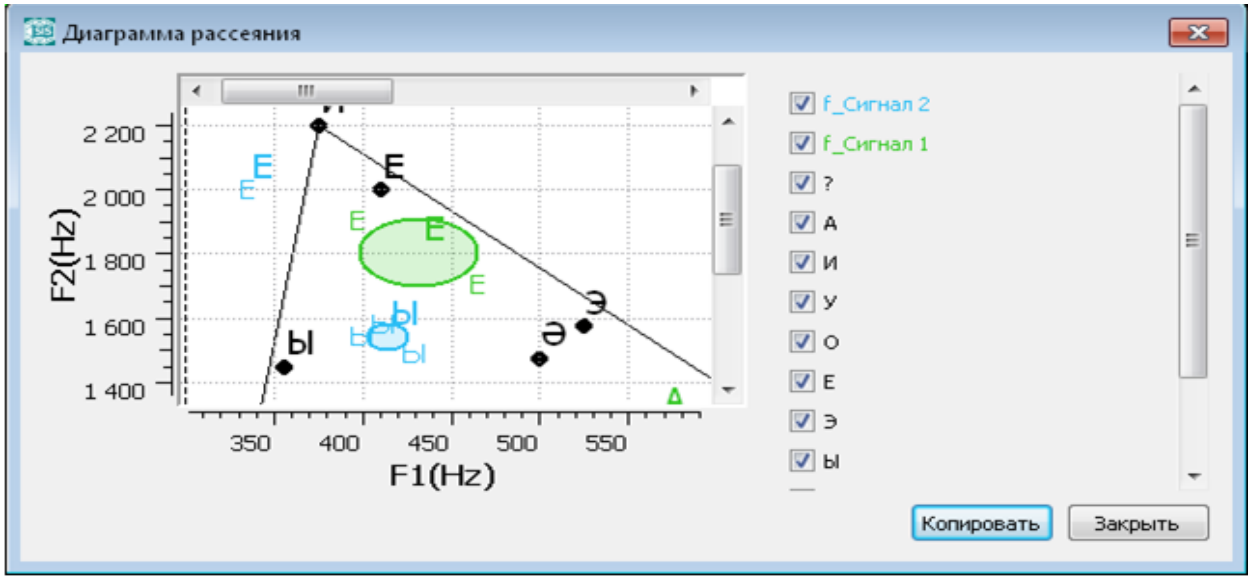



Рисунок 9 – Отображение выделенной части окна диаграммы рассеяния

В данном случае перемещение по диаграмме рассеяния становится возможным при помощи полос горизонтальной и вертикальной прокрутки. Для возвращения к полному изображению следует щелкнуть правой кнопкой мыши при положении курсора в окне диаграммы. В появившемся контекстном меню диаграммы рассеяния выбрать пункт **Показать целиком**.

Чтобы скопировать изображение диаграммы рассеяния в буфер обмена, воспользуйтесь пунктом контекстного меню **Копировать в буфер** или нажмите кнопку Копировать. Чтобы закрыть окно скатерограммы, нажмите кнопку Закрыть.

Имеется возможность поменять оси отображения диаграммы рассеяния на любую пару осей с 1 по 4 формант. Для этого следует щелчком правой кнопки мыши вызвать контекстное меню, а в нем выбрать пункт **Изменить оси**, а затем выбрать нужную пару формант для построения новой диаграммы (рис. 10).

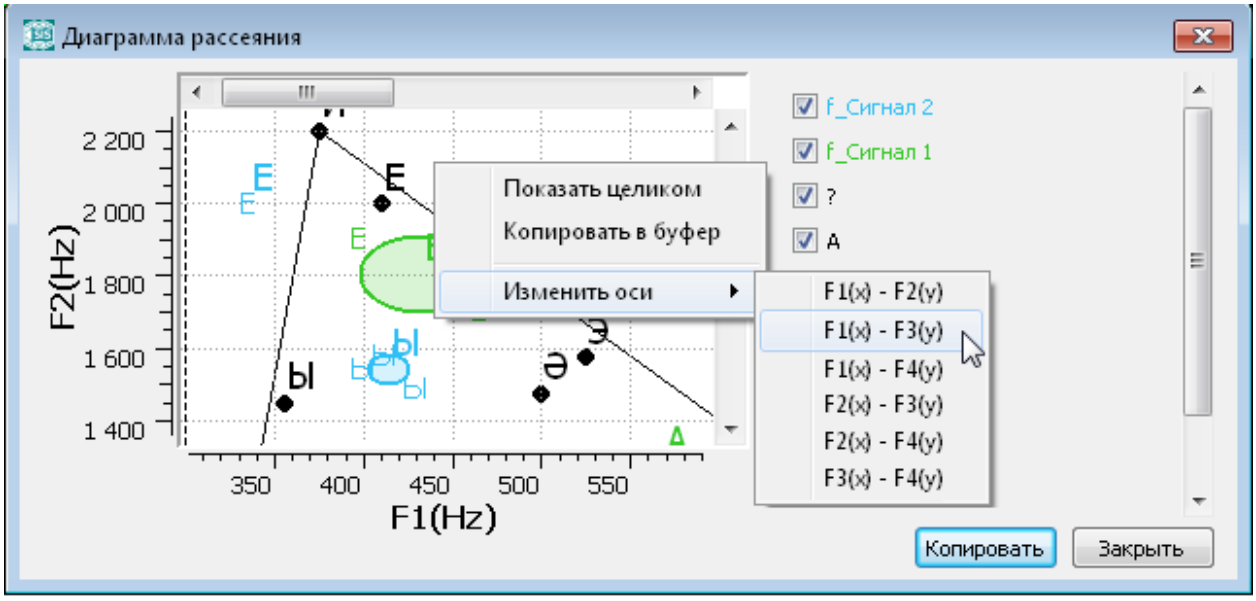



Рисунок 10 - Выбор новой пары осей для построения другой диаграммы рассеяния.

Новое изображение тех же фрагментов будет построено на формантной плоскости для выбранной пары осей.

Просмотр исследуемого речевого материала с помощью диаграммы рассеяния позволяет визуально определить степень совпадения/различия форматных структур в речи дикторов, уточнить положение оптимальных границ типов звуков в таблице параметров сравнения, выбрать для численного сравнения формант наиболее представительные фрагменты. График диаграммы рассеяния, помещенный в отчет, может служить наглядной и убедительной иллюстрацией выводов эксперта.

Именно использование диаграммы рассеяния позволяет легко установить и проиллюстрировать существенное различие в реализации дикторами того или иного типа звука.

## 2.2 Исследование модуля «Сравнение основного тона»

Чтобы применить метод анализа мелодического контура, выберите меню **Модули Сравнение основного тона**.

В диалоговом окне (рис. 11) укажите пару сравниваемых сигналов (с определённым основным тоном). Если их в программе всего два, модуль выбирает их автоматически. Если сигналов больше двух, то сравниваемые сигналы выбираются оператором из выпадающих списков.

Кроме того, если ранее в данном проекте уже выполнялись сравнения с выбранным сигналом, то таблицы фрагментов для этого сигнала можно загрузить из ранее сохранённых сравнений, воспользовавшись выпадающим списком **загрузить из**.

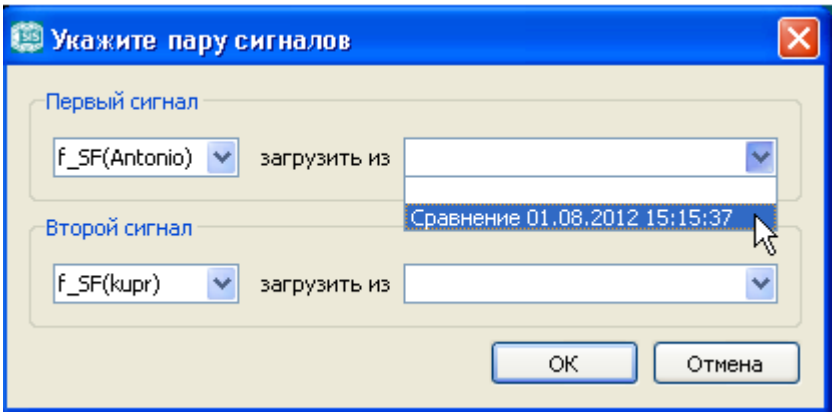



Рисунок 11 – Выбор сравниваемых сигналов

После выбора сравниваемых сигналов нажмите кнопку **ок**. Откроется панель работы с модулем. Панель прикрепляется к нижней части главного окна **SIS II**, при этом открытые внутри него окна с данными, панели управления или окно спектра пропорционально меняют свой размер (рис. 12).

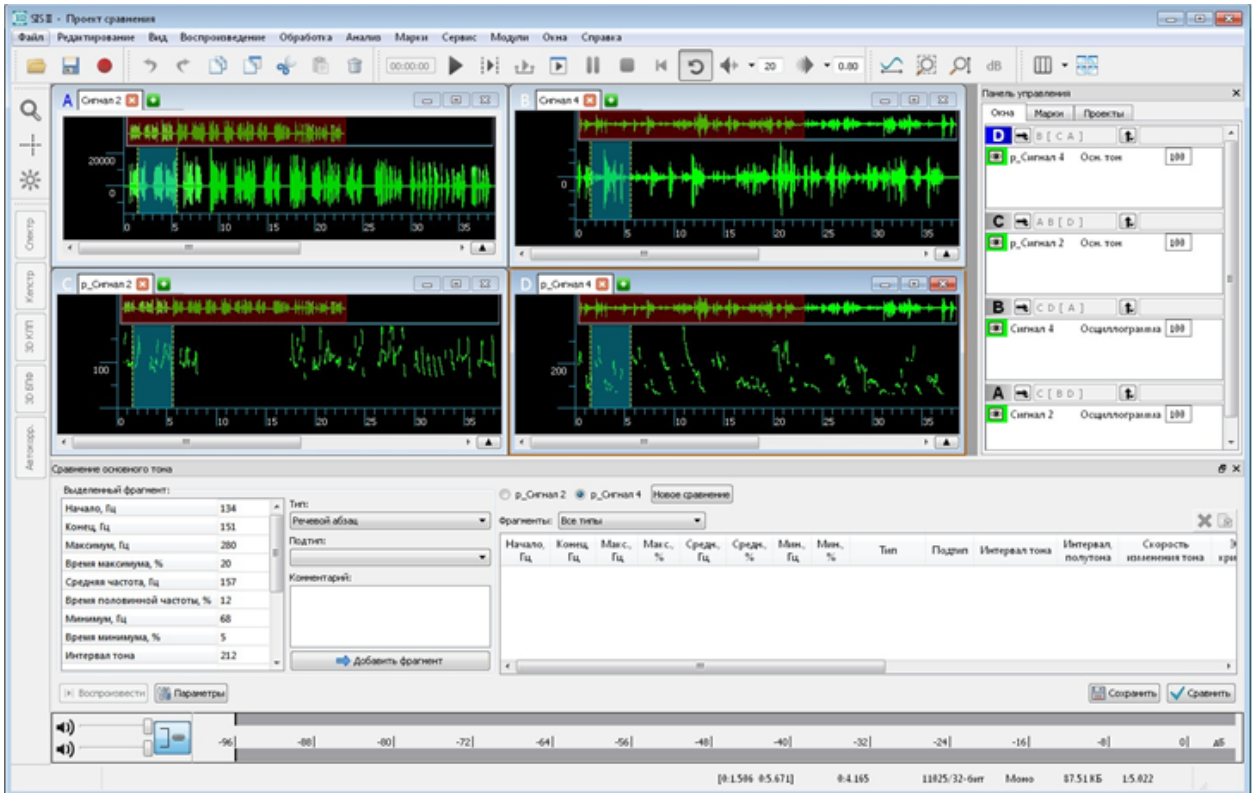


Рисунок 12 – Панель модуля внутри главного окна звукового редактора

Чтобы сделать панель модуля независимой от главного окна SIS II (рис. 13), следует нажать на значок в правом верхнем углу панели или дважды щёлкнуть левой кнопкой мыши на заголовке панели. Панель можно перемещать в любое место на экране монитора, удерживая нажатой на заголовке левую кнопку мыши.

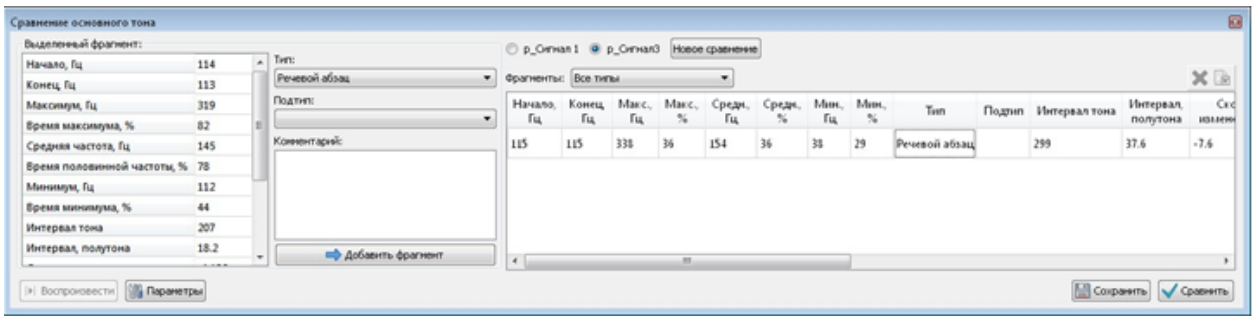


Рисунок 13 - Панель модуля в качестве отдельного независимого окна

При последующих запусках модуля предыдущее положение панели сохраняется. Чтобы прикрепить панель обратно к нижней части главного окна **SIS II**, следует снова дважды щёлкнуть на заголовке панели.

Чтобы выбрать другие сигналы (форманты) для сравнения, нажмите кнопку Новое сравнение и в диалоговом окне **Укажите пару сигналов** (см. рис. 11) осуществите выбор.

Перед началом работы с модулем может потребоваться задать отдельные параметры. Чтобы открыть окно параметров (рис. 14), нажмите кнопку Параметры.

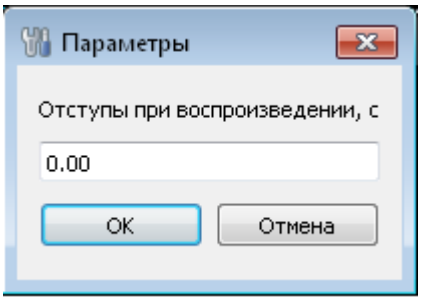



Рисунок 14 – Отступы при воспроизведении

Окно позволяет задавать продолжительность проигрывания фонограммы в секундах до начала опорного фрагмента и после него при прослушивании выбранного опорного фрагмента. По умолчанию выставлено 0,5 секунды.

Воспроизведение выбранного фрагмента производится циклически при нажатии кнопки Воспроизвести. При повторном нажатии кнопки воспроизведение прекращается.

Настройки текущего мелодического контура выставляются автоматически.

### 2.2.1 Формирование фрагментов

Текущий сигнал выбирается либо на панели модуля (рис. 53), либо в соответствующем окне данных главного окна программы. В последнем случае выбор также дублируется на панели модуля.

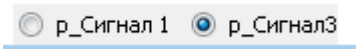


Рисунок 15 – Выбор текущего сигнала

Для выделенного в окне данных фрагмента основного тона рассчитывается и отображается в таблице

**Выбранный фрагмент** набор параметров, приведённый на рисунке 16

Далее оператор из выпадающих списков должен задать выбранному фрагменту **Тип** и **Подтип**, а также может дать комментарий (рис. 16).

После этого, чтобы добавить фрагмент в общую таблицу фрагментов, следует нажать кнопку Добавить фрагмент.

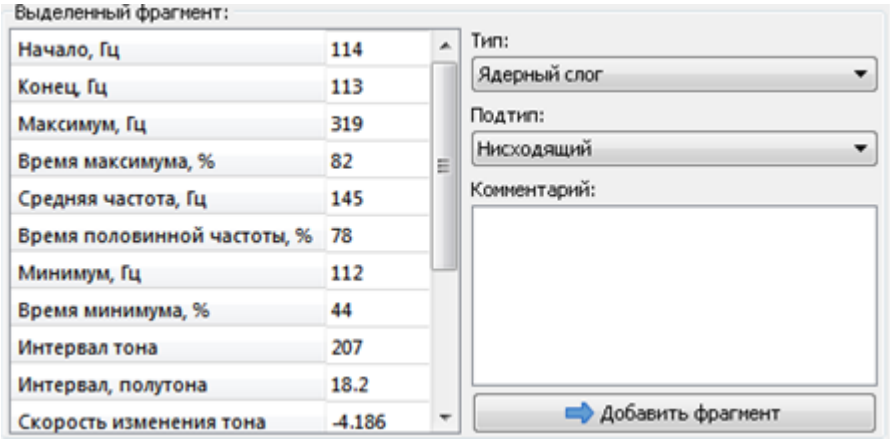



Рисунок 16 - Статистическая информация, тип, подтип и комментарий к фрагменту

В таблице отображается статистическая информация для фрагмента с указанием типа и подтипа, а также комментария оператора. Оператор может отобразить фрагменты только определённого типа: для этого над таблицей есть выпадающий список с возможностью выбрать тип фрагмента.

Оптимальное число однотипных опорных фрагментов для получения статистики составляет 10–15.

На основе данного набора статистических параметров эксперт может оценить степень представительности и однородности выборок, предназначенных для обобщения и сравнения, и при необходимости скорректировать наборы элементов.

Выделенный в таблице фрагмент можно удалить, нажав на значок ✖, или скопировать в буфер обмена, нажав на значок . Предусмотрена возможность изменить тип и/или подтип, а также комментарий у фрагмента, добавленного в таблицу.

Чтобы сохранить в проекте сформированную таблицу фрагментов, нажмите кнопку. Сохранить

### 2.2.2. Сравнение фрагментов

После завершения выбора фрагментов для двух фонограмм нажмите кнопку Сравнить.

Модуль автоматически выполняет сравнение выбранных оператором фрагментов и выдаёт результат, представленный на рисунке 55.

В таблице результатов сравнения отображается информация о количестве сравниваемых фрагментов для каждого типа/подтипа. Отображается разброс значений для каждого из статистических параметров сравниваемых фонограмм и процент совпадения.

Сравнение фонограмм производится по следующему алгоритму:

– усреднение нескольких фрагментов единой комбинации «тип/подтип/источник»;

– циклический поиск фрагментов одного типа/подтипа в двух источниках и проверка достаточности числа фрагментов (по умолчанию не менее 5) нужного типа/подтипа для каждого из сигналов;

– циклическая проверка использования сочетания «тип/подтип и параметр» для пороговых значений; расчёт процента сходства/различия двух дикторов по одному признаку; считывание весовых коэффициентов в зависимости от факта сходства или различия, а также проверка использования сочетания «тип/подтип и параметр» для весовых коэффициентов;

– расчёт значений «за» и «против» как результирующих характеристик по всем параметрам одного варианта типа/подтипа;

– статистическая проверка данных;

– расчёт единого для источника значения «за» и «против»;

– расчёт степени сходства/различия дикторов в зависимости от достаточного числа длительных фрагментов;

– определение значений FR/FA по степени сходства/различия и качественный вывод о сходстве/различии дикторов;

– проверка данных на высокую типичность и окончательное формирование всех выходных данных.

В окне **Результат:** отображаются FR и FA, общее количество сравниваемых типов (подтипов), число совпавших и не совпавших типов (подтипов), формулировка заключения.

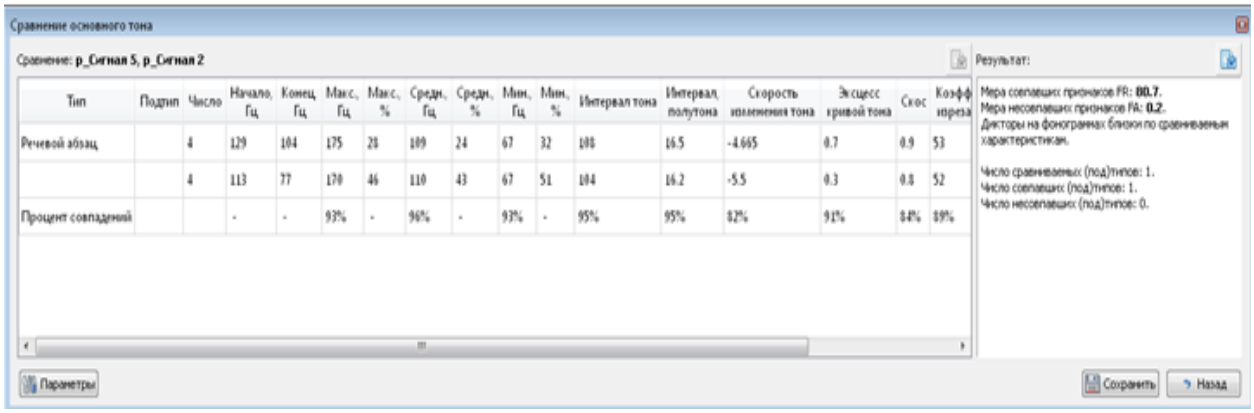



Рисунок 17 – Результат сравнения основного тона

Выделенную в таблице результатов строку, а также содержание окна **Результат:** можно скопировать в буфер обмена, нажав на значок .

Чтобы вернуться к выбору фрагментов, нажмите кнопку Назад.

Чтобы сохранить в проекте сформированную таблицу фрагментов, нажмите кнопку Сохранить.

Чтобы запустить модуль и открыть таблицы фрагментов из ранее сохранённых сравнений, следует левой кнопкой мыши дважды щёлкнуть на пункте **Сравнение…** в активном проекте (рис. 18).

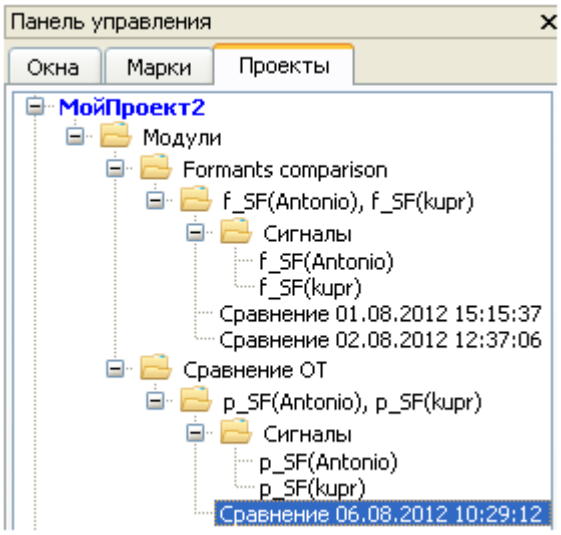



Рисунок 18– Сохранённые в проекте сравнения основного тона

Чтобы завершить работу с модулем и закрыть панель, нажмите на значок **x** или ☒ в правом верхнем углу панели.

**Задание на практическую часть**

1. Ознакомится с теоретической частью работы.
2. Провести исследование модуля «Сравнение формант».
3. Провести исследование модуля «Сравнение основного тона».
4. Составить отчет о проделанной работе, в котором указать выводы, рисунки, таблицы, графики.

**Контрольные вопросы.**

1. Назначение аппаратно-программного комплекса «ИКАР Лаб».
2. Основные функциональные возможности аппаратно-программного комплекса «ИКАР Лаб».
3. Основные модули аппаратно-программного комплекса «ИКАР Лаб».
4. Характеристика модуля «Сравнение формант».
5. Характеристика модуля «Сравнение основного тона».

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1,2

*Дополнительная:* 1-34

*Методическая:*1

*Программное обеспечение:* 1-4

## Практическое занятие № 10-18

**Тема:** Исследование модулей «Сравнение речевых признаков» и «Сравнение основного тона» комплекса криминалистического исследования фонограмм речи «ИКАР Лаб»

**Цель занятия:**

Ознакомиться с теоретическим материалом предназначенным для формирования у обучающегося базовых знаний для дальнейшего изучения комплекса криминалистического исследования фонограмм речи «ИКАР Лаб».

**Формируемые компетенции:** ПК-1

**Структура лабораторной работы**

**Вводная часть**

| | |
|---|---|
| Проверка готовности студентов к лабораторной работе | 10 мин |
| Вступительная часть | 10 мин |

**Вопросы (задачи), подлежащие исследованию**

| | |
|---|---|
| Изучение теоретических данных | 40 мин |

**Заключительная часть**

| | |
|---|---|
| Защита отчетов по лабораторной работе | 20 мин |
| Подведение итогов | 5 мин |
| Задание студентам для самостоятельной работы | 5 мин |

# 1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Аппаратно-программный комплекс ИКАР Лаб предназначен для решения широкого круга задач анализа звуковой информации, востребованного в специализированных подразделениях правоохранительных органов, лабораториях и центрах судебной экспертизы, службах расследования летных происшествий, исследовательских и учебных центрах. Первая версия продукта была выпущена в 1993 году и явилась результатом совместной работы ведущих аудиоэкспертов и разработчиков программного обеспечения. Входящие в состав комплекса специализированные программные средства обеспечивают высокое качество визуального представления фонограмм речи. Современные алгоритмы голосовой биометрии и мощные инструменты автоматизации всех видов исследования фонограмм речи позволяют экспертам существенно повысить надежность и эффективность экспертиз. Входящая в комплекс программа SIS II обладает уникальными инструментами для идентификационного исследования: сравнительное исследование диктора, записи голоса и речи которого предоставлены на экспертизу и образцов голоса и речи подозреваемого. Идентификационная фоноскопическая экспертиза основывается на теории уникальности голоса и речи каждого человека. Анатомическое факторы: строение органов артикуляции, форма речевого тракта и ротовой полости, а также внешние факторы: навыки речи, региональные особенности, дефекты и др.

Набор включает следующие программные модули, входящие в состав **SIS II**:

1) Модуль «Методика», представляющий собой совокупность всех модулей.

2) Модуль оценки качества фонограммы «Характеристики сигнала» позволяет автоматически вычислить основные параметры звукового сигнала фонограммы в целом и оценить ее пригодность для дальнейших исследований.

3) Модуль разделения речи дикторов «Разделение дикторов в диалоге» позволяет выполнять автоматическую маркировку речевых сегментов по дикторам на записях естественной речи.

4) Модуль поиска речевых участков «Детектирование речи» позволяет автоматически выделять в фонограмме речевые, шумовые участки и паузы.

5) Модуль «Автоматическое сравнение» выполняет автоматическую идентификацию личности по голосу тремя методами с использованием обобщающего решения.

6) Модуль «Сравнение формант» позволяет автоматизировать процесс идентификации личности по голосу на основе метода сравнения формант.

7) Модуль «Сравнение основного тона» позволяет автоматизировать процесс идентификации личности по голосу на основе сравнения параметров мелодических контуров голоса сравниваемых дикторов.

8) Модуль «Сравнение речевых признаков» позволяет автоматизировать процесс идентификации личности по голосу на основе экспертного сравнения лингвистических характеристик речи сравниваемых дикторов.

9) Модуль «Общее решение» позволяет принять общее решение относительно идентификации личности по голосу на основе результатов работы каждого из использованных модулей идентификации дикторов.

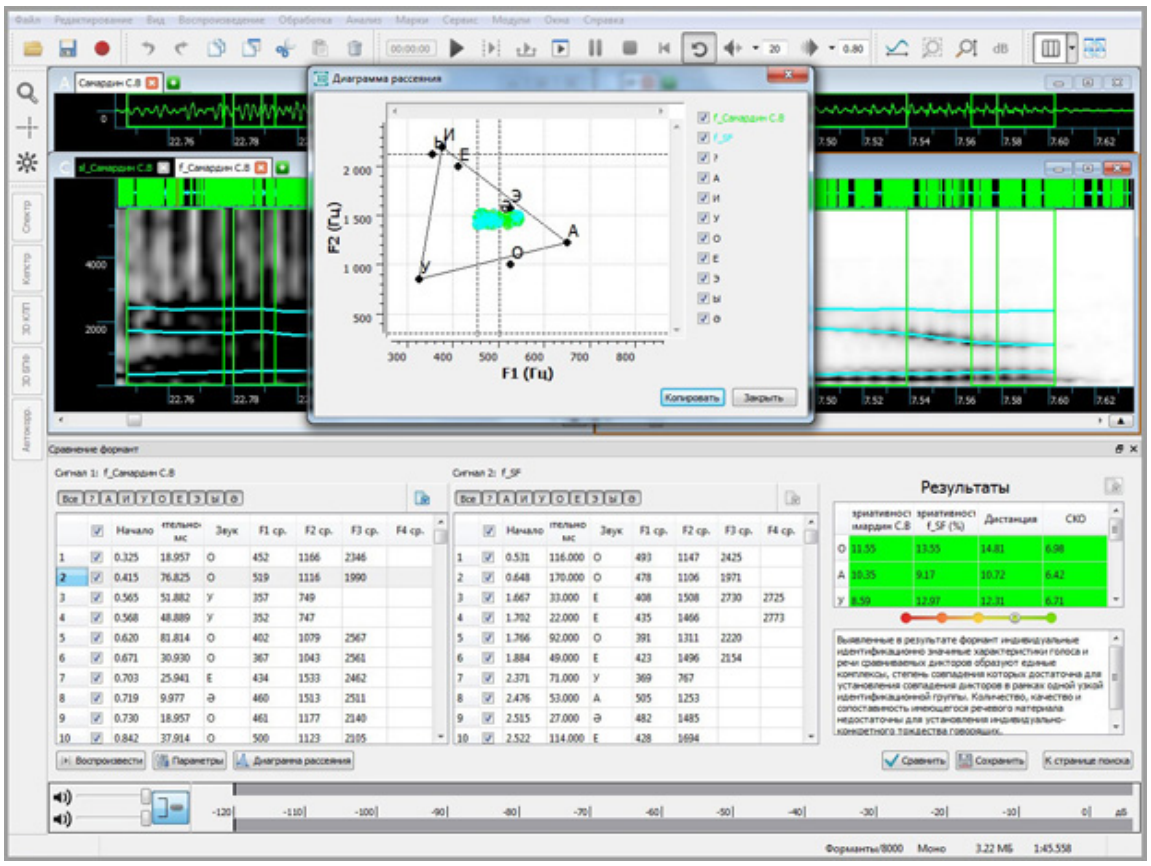



Рисунок 1 – Интерфейс программы SIS II

### 1.1 Модуль «Сравнение речевых признаков»

Метод речевого анализа лишь частично автоматизирован. Всю подготовительную работу по отбору материала, оценке его приемлемости для анализа, выделению признаков и оценке их выраженности в сравниваемых фонограммах выполняет эксперт. Поэтому следует помнить, что надёжность конечного результата речевой идентификации в значительной мере определяется квалификацией эксперта и правильностью оценки им речевых признаков.

Фонограммы, предназначенные для сравнения методом речевого анализа, должны быть приемлемого качества, т. е. обеспечивать адекватное восприятие на слух существенных для речевого анализа характеристик гласных исогласных.

Затруднению речевого анализа (вплоть до невозможности его применения) способствует высокий уровень фонового шума на фонограмме, перегрузка сигнала, высокая реверберированность, различия в канале записи (телефон и микрофон) и/или звукозаписывающей аппаратуре. Кроме того, снизить надёжность идентификационного сравнения могут различия в речевом стиле (чтение/спонтанная

речь), в манере произнесения (аккуратная или небрежная, энергичная или вялая), в темпе речи. Наличие или отсутствие визуального контакта между собеседниками, принимающими участие в разговорах на сравниваемых фонограммах (разговор по телефону или при личной встрече собеседников) также может играть роль.

Одно из основных требований правильной идентификации – одинаковый канал записи спорной и образцовой фонограммы и схожее качество записи. Для сравнения слуховым методом микрофонных и телефонных фонограмм рекомендуется предварительно обработать микрофонные фонограммы эквалайзером с полосой пропускания, аналогичной полосе фонограммы телефонного канала.

Кроме требований к качеству записи, важно учитывать и другие факторы, влияющие на степень надёжности идентификационных выводов, в частности, на наличие и степень выраженности отдельных групп слуховых признаков. Важно учитывать влияние разных ситуативных факторов, таких как жанр, время и место разговора, наличие требований и ограничений на поведение дикторов. Одним из главных факторов является эмоциональное состояние диктора.

Данные факторы могут повлиять на следующие группы признаков:

– громкость;

– интонация (в т. ч. темп речи);

– речевые сбои; – манера речи;

– частотность и долгота хезитационных пауз.

В случае качественной и стилистической сопоставимости фонограмм ведущим фактором, определяющим надёжность сравнения, является их фонетико-лингвистическая представительность. Под представительностью понимается наличие в обеих сравниваемых фонограммах контекстов реализации речевых признаков в количестве, достаточном для получения надёжных данных для сравнения. При этом важную роль играет длительность исследуемых фонограмм, поскольку короткие фонограммы (менее 20 секунд), как правило, не обеспечивают должной фонетической представительности.

При длине фонограммы более одной минуты проведение идентификации слуховым методом возможно по всем группам признаков.

При фонограммах меньшей длины (от 10 секунд) идентификация также возможна, но её результат может быть менее точным из-за того, что для принятия экспертом более обоснованного решения о наличии или отсутствии большинства признаков в речи диктора требуется более длительный речевой отрезок. Например, на более длительном речевом отрезке может быть варьирование темпа, высоты и громкости речи диктора, которое не будет представлено на коротком отрезке.

Кроме того, выделение большинства признаков, характеризующих наличие либо отсутствие каких- либо особенностей речи диктора (хезитационные паузы, нарушения речи), может также требовать фонограмм большей длины.

Для получения решения могут остаться незаполненными не более 3 признаков основного списка. При большем количестве незаполненных полей получить решение невозможно.

### 1.2 Модуль «Общее решение»

Основываясь на результатах работы каждого из описанных выше модулей, программа позволяет принять общее идентификационное решение. При этом эксперт имеет возможность настраивать применимость каждого из отдельных методов исследования, изменяя таким образом, его вес в общем решении. Применимость также может быть выставлена автоматически по результатам расчёта качественных и количественных характеристик сравниваемых фонограмм.

Модуль просматривает сохранённые результаты сравнений по всем модулям в активном проекте. Если для исследуемой пары фонограмм имеются результаты нескольких сравнений по какому-либо из модулей, пользователь может выбрать из списка сравнение, результаты которого должны учитываться для принятия общего решения.

## 2. ПРАКТИЧЕСКАЯ ЧАСТЬ

## 2.1 Исследование модуля «Сравнение речевых признаков»

Чтобы применить метод анализа слуховых характеристик, выберите меню **Модули Сравнение речевых признаков.**

В диалоговом окне (рис. 2) выберите сравниваемые сигналы. Если их в программе всего два, модуль выбирает их автоматически. Если сигналов больше двух, то сравниваемые сигналы выбираются оператором из выпадающих списков.

Кроме того, если ранее в данном проекте уже выполнялись сравнения с выбранным сигналом, то таблицы фрагментов для этого сигнала можно загрузить из ранее сохранённых сравнений, воспользовавшись выпадающим списком **загрузить из.**

Можно также указать один из двух возможных источников записи фонограммы (микрофон либо телефон) и, если у диктора наблюдается явный иностранный акцент, выбрать акцент.

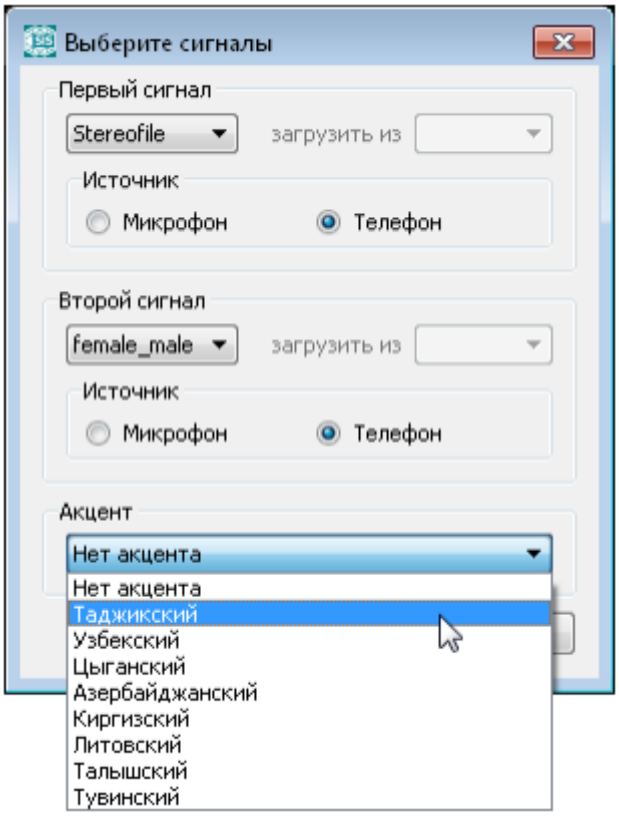



Рисунок 2 - Выбор сравниваемых сигналов

После выбора сравниваемых сигналов, источника и, если необходимо, нужного акцента нажмите кнопку OK. Откроется панель работы с модулем. Панель прикрепляется к нижней части главного окна SIS II, при этом открытые внутри него окна с данными, панели управления или окно спектра пропорционально меняют свой размер (рис. 3).

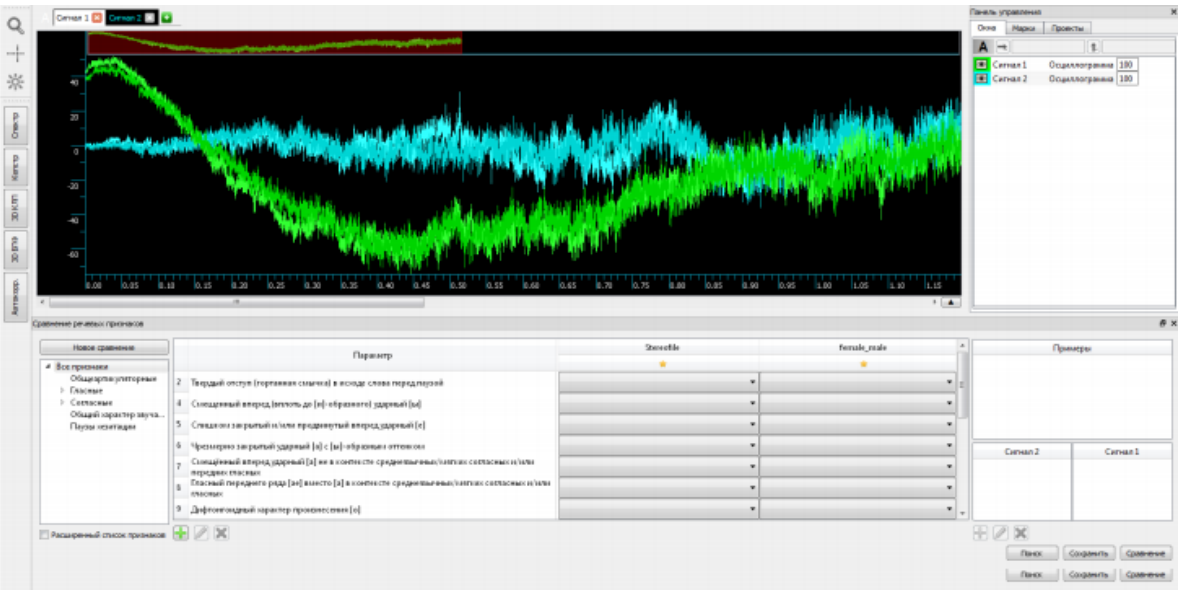


Рисунок 3 - Панель модуля внутри главного окна программы

Чтобы сделать панель модуля независимой от главного окна SIS II (рис. 4), следует нажать на значок в правом верхнем углу панели или дважды щёлкнуть левой кнопкой мыши на заголовке панели. Панель можно перемещать в любое место на экране монитора, удерживая нажатой на заголовке левую кнопку мыши.

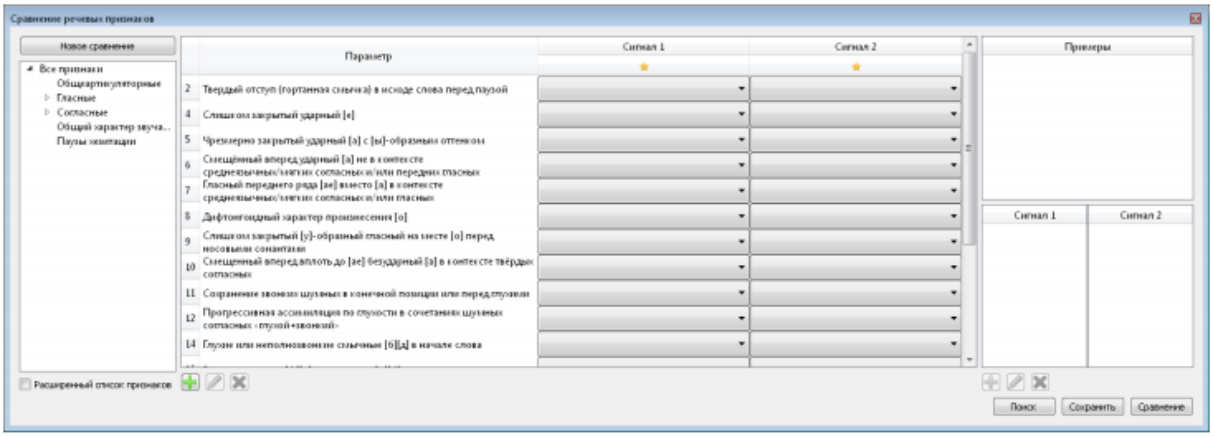



Рисунок 4 - Панель модуля в качестве отдельного независимого окна

При последующих запусках модуля предыдущее положение панели сохраняется. Чтобы прикрепить панель обратно к нижней части главного окна SIS II, следует снова дважды щёлкнуть на заголовке панели. Чтобы выбрать другие сигналы для сравнения, нажмите кнопку и в диалоговом окне Выберите сигналы (см. рис. 2) осуществите выбор.

### 2.2 Исследование модуля «Общее решение»

Чтобы открыть модуль «Общее решение», выберите меню **Модули Общее решение.**

Откроется диалоговое окно модуля (рис. 5). Окно модуля «Общее решение» содержит таблицу сравнений фонограмм с помощью различных методов. Результаты сравнения по каждому из них отражены в столбце **LR** (отношение правдоподобия). Качественные характеристики фонограмм для сравнений по каждому из методов отображаются в левом столбце в виде индикатора зелёного, жёлтого или красного цвета, соответствующего хорошему, среднему или плохому качеству данных.

Эксперт может изменить выставленное по умолчанию значение применимости для различных методов. Например, если речевой анализ проводил не очень опытный эксперт, можно занизить вес его оценки. Для изменения

применимости передвиньте ползунок в нужное положение или задайте точное значение с помощью поля ввода.

Методы, в основе которых лежит анализ основного тона (**ОТ** и **Сравнение основного тона**), сильно зависят от эмоционального состояния диктора. Например, если человек возбуждён, то увеличивается не только среднее значение основного тона, но также могут сильно меняться и все остальные статистические характеристики ОТ. Поэтому если выставить или снять флажок **Различается эмоциональное состояние**, значения применимости названных методов будет пересчитываться в меньшую или большую сторону соответственно в зависимости от качества данных.

Если после ручной коррекции величин применимости нажать кнопку Установить по качеству, то её значения будут пересчитаны в зависимости от качества фонограммы (будут выставлены по умолчанию).

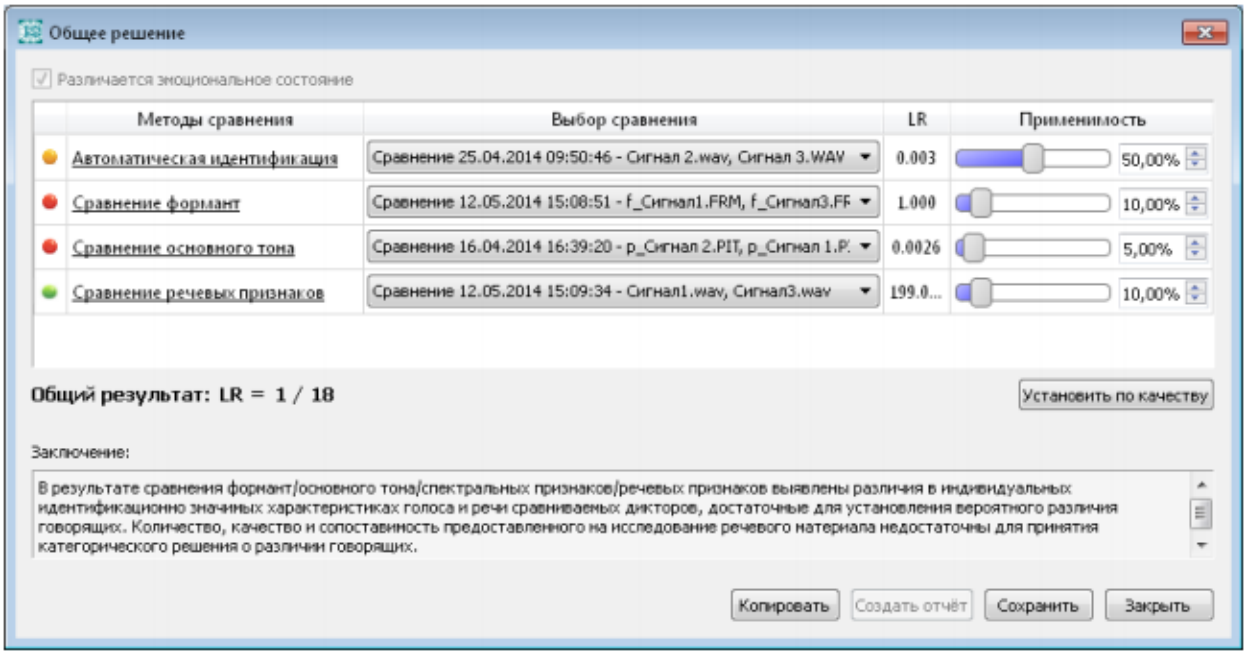



Рисунок 5 - Диалоговое окно модуля "Общее решение"

Под основной таблицей в окне модуля приводится общий результат – отношение подобия (LR) по всем использованным сравнениям – и даётся общее решение в виде экспертного заключения.

Чтобы скопировать полученные результаты в виде данных для включения в текстовый отчёт, нажмите кнопку Копировать.

Для сохранения результата сравнения фонограмм в проекте нажмите кнопку Сохранить.

Для генерирования отчета об исследовании в формате PDF нажмите кнопку Создать отчёт.

Чтобы запустить модуль и открыть данные из ранее сохранённых сравнений, следует сделать двойной щелчок мыши на пункте **Сравнение…** в активном проекте (рис. 6).

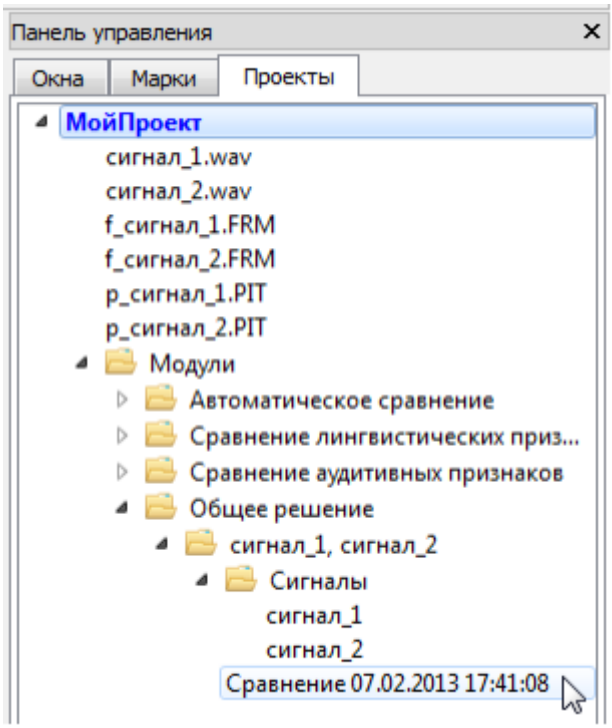



Рисунок 6 - Сохраненные в проекте общие идентификационные решения

Чтобы завершить работу с модулем, нажмите на значок в правом верхнем углу диалогового окна или на кнопку Закрыть.

**Задание на практическую часть**

1. Ознакомится с теоретической частью работы.
2. Провести исследование модуля «Сравнение речевых признаков».
3. Провести исследование модуля «Общее решение».
4. Составить отчет о проделанной работе, в котором указать выводы, рисунки, таблицы, графики.

**Контрольные вопросы.**

6. Назначение аппаратно-программного комплекса «ИКАР Лаб».

7. Основные функциональные возможности аппаратно-программного комплекса «ИКАР Лаб».

8. Основные модули аппаратно-программного комплекса «ИКАР Лаб».

4. Характеристика модуля «Сравнение речевых признаков».

5. Какие факторы влияют на степень надежности идентификационных выводов, и на какие группы признаков они могут повлиять?

6. Характеристика модуля «Общее решение».

7. От чего сильно зависят методы, в основе которых лежит анализ основного тона?

**Список литературы, рекомендуемый к использованию по данной теме:**

*Основная:* 1,2

*Дополнительная:* 1-34

*Методическая:*1

*Программное обеспечение:* 1-4

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Технологии аутентификации в информационных системах»
для студентов направления подготовки
10.03.01«Информационная безопасность»
Направленность (профиль):
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности»

Ставрополь,
2026

## СОДЕРЖАНИЕ

Введение
1. Общая характеристика самостоятельной работы студента
2. Технологическая карта самостоятельной работы студента
3. Самостоятельное изучение тем лекций
4. Паспорт фонда оценочных средств для проверки самостоятельной работы
5. Список рекомендуемой литературы

## Введение

Целью дисциплины «Технологии аутентификации в информационных системах» является рассмотрение теоретических основ и закономерностей построения и функционирования систем, в том числе и организационных, методологических принципов их анализа и синтеза, применение изученных закономерностей для формирования набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Основными задачами изучения дисциплины являются:

1. Изучение основных естественнонаучных законов для адекватного применения математического аппарата и выявления сущности проблем, возникающих в сфере защиты информации и информационной безопасности.

2. Формирование способностей применять методы теории систем и системного анализа при проведении предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.

3. Формирование способностей самостоятельно проводить эксперименты по заданной методике, обрабатывать результаты, оценивать погрешность и достоверность результатов.

## 1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные работы и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области математических основ теории систем. На лабораторных работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным работам и тестовые, завести новую тетрадь для конспектирования лекций и выполнения лабораторных работ.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих

конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

– самостоятельное изучение учебного материала по заданным темам;
– подготовка к лабораторным работам, оформление отчета по выполненному лабораторному занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:
– чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
– работа с нормативными документами;
– поиск информации в Интернет;
2) для закрепления и систематизации знаний:
– работа с конспектом лекции (обработка текста);
– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
– составление плана и тезисов ответа или графическое изображение структуры ответа;
– составление таблиц для систематизации учебного материала;
– изучение нормативных документов;
– ответы на контрольные вопросы;
3) для формирования умений:
– подготовка к лабораторным занятиям;
– решение задач и лабораторных заданий;
– подготовка отчетов по лабораторным занятиям;
– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, лабораторные занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям, а также варианты тестовых заданий.

## 2. Технологическая карта самостоятельной работы студента

| Коды реализуемых компетенций, индикатора(ов) | Вид деятельности студентов | Средства и технологии оценки | Обьем часов, в том числе | | |
|---|---|---|---|---|---|
| | | | СРС | Контактная работа с преподавателем | Всего |
| 4 семестр | | | | | |
| ПК-1 ИД-2 | Подготовка к лабораторной работе | Собеседование | 5.00 | 2.00 | 7.00 |
| ПК-1 ИД-2 | Подготовка к лекции | Конспект | 5.00 | 2.00 | 7.00 |
| ПК-1 ИД-2 | Подготовка доклада | Доклад | 5.00 | 2.00 | 7.00 |
| ПК-1 ИД-2 | Самостоятельное изучение литературы | Конспект | 5.00 | 2.00 | 7.00 |
| ПК-1 ИД-2 | Подготовка к практическому занятию | Собеседование | 6.00 | 2.00 | 8.00 |
| **Итого за 4 семестр** | | | 26.00 | 10.00 | 36.00 |
| **Итого** | | | 26.00 | 10.00 | 36.00 |

## 3. Порядок выполнения самостоятельной работы

*3.1 Методические рекомендации по изучению теоретического материала*

Комплексное изучение предлагаемой студентам учебной дисциплины «Технологии аутентификации в информационных системах» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения лабораторных работ, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к лабораторным занятиям.

***Работа с конспектом лекций***

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

***Выполнение лабораторных работ по дисциплине «Технологии аутентификации в информационных системах»*** На первом занятии получите у преподавателя задания по курсу, планы подготовки к лабораторным работам. Обзаведитесь всем необходимым методическим обеспечением.

Перед лабораторными работами изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью лабораторных работ является:

- закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

*3.2 Методические рекомендации по написанию и оформлению доклада*

1. Общие положения

1.1. Доклад, как вид самостоятельной работы в учебном процессе, способствует формированию навыков исследовательской работы, расширяет познавательные интересы, учит критически мыслить.

1.2. При написании доклада по заданной теме студент составляет план, подбирает основные источники.

1.3. В процессе работы с источниками систематизирует полученные сведения, делает выводы и обобщения.

1.4. К докладу по крупной теме могут привлекать несколько студентов, между которыми распределяются вопросы выступления.

2. Выбор темы доклада

2.1. Тематика доклада обычно определяется преподавателем, но в определении темы инициативу может проявить и студент.

2.2. Прежде чем выбрать тему доклада, автору необходимо выявить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

3. Этапы работы над докладом

3.1. Формулирование темы, причем она должна быть не только актуальной по своему

значению, но и оригинальной, интересной по содержанию.

3.2. Подбор и изучение основных источников по теме (как правильно, при разработке доклада используется не менее 8-10 различных источников).

3.3. Составление списка использованных источников.

3.4. Обработка и систематизация информации

3.5. Разработка плана доклада.

3.6. Написание доклада.

3.7. Публичное выступление с результатами исследования.

4. Структура доклада:

- титульный лист

- оглавление (в нем последовательно излагаются названия пунктов доклада, указываются страницы, с которых начинается каждый пункт);

- введение (формулирует суть исследуемой проблемы, обосновывается выбор темы, определяются ее значимость и актуальность, указываются цель и задачи доклада, дается характеристика используемой литературы);

- основная часть (каждый раздел ее, доказательно раскрывая отдельную проблему или одну из ее сторон, логически является продолжением предыдущего; в основной части могут быть представлены таблицы, графики, схемы);

- заключение (подводятся итоги или дается обобщенный вывод по теме доклада, предлагаются рекомендации);

- список использованных источников

5. Структура и содержание доклада

5.1. Введение - это вступительная часть научно-исследовательской работы. Автор должен приложить все усилия, чтобы в этом небольшом по объему разделе показать актуальность темы, раскрыть практическую значимость ее, определить цели и задачи эксперимента или его фрагмента.

5.2. Основная часть. В ней раскрывается содержание доклада.
Как правило, основная часть состоит из теоретического и практического разделов. В теоретическом разделе раскрываются история и теория исследуемой проблемы, дается критический анализ литературы и показываются позиции автора. В практическом разделе излагаются методы, ход, и результаты самостоятельно проведенного эксперимента или фрагмента.

В основной части могут быть также представлены схемы, диаграммы, таблицы, рисунки и т.д.

5.3. В заключении содержатся итоги работы, выводы, к которым пришел автор, и рекомендации. Заключение должно быть кратким, обязательным и соответствовать поставленным задачам.

5.4. Список использованных источников представляет собой перечень использованных книг, статей, фамилии авторов приводятся в алфавитном порядке, при этом все источники даются под общей нумерацией литературы. В исходных данных источника указываются фамилия и инициалы автора, название работы, место и год издания.

5.5. Приложение к докладу оформляются на отдельных листах, причем каждое должно иметь свой тематический заголовок и номер, который пишется в правом верхнем углу, например: «Приложение 1»

6. Требования к оформлению доклада

6.1. Объем доклада может колебаться в пределах 5-15 печатных страниц; все приложения к работе не входят в ее объем.

6.2. Доклад должен быть выполнен грамотно, с соблюдением культуры изложения.

6.3. Обязательно должны иметься ссылки на используемую литературу.

6.4. Должна быть соблюдена последовательность написания библиографического аппарата.

7. Критерии оценки доклада

- актуальность темы исследования;

- соответствие содержания теме;

- глубина проработки материала; правильность и полнота использования источников;

- соответствие оформления доклада стандартам.

По усмотрению преподавателя доклады могут быть представлены на семинарах, научно-практических конференциях, а также использоваться как зачетные работы по пройденным темам.

*3.3 Методические рекомендации по конспектированию первоисточников*

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта,

так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материал, одной из обязательных форм организации умственного труда.

**Планом** удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

**Тезисы** предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

**Конспектирование** – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

**По форме *конспекты подразделяются* на формализованные и графические.**

**1. Формализованные** (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

**2. Графические** (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

**Плановый** – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

**Текстуальный** – это конспект, созданный в основном из цитат.

**Сводный конспект** – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

**Тематический** – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

**Способы конспектирования.**

***- Тезисы*** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

***- Линейно-последовательная запись текста.*** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- С***пособ «вопросов – ответов».*** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- С***хема с фрагментами*** **–** способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- ***Простая схема*** **–** способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- ***Параллельный способ*** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

***Однако л***учше использовать разные способы конспектирования для записи одного и того же материала.

***Комбинированный конспект*** – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

**Принципы составления конспекта прочитанного.**

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

*1. Резюмирование.*

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

*2. Аннотация.*

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуется изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

· тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)

· задачи, поставленные автором аннотируемого документа

· метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)

· принадлежность автора к определенной научной школе или направлению

· структуру аннотируемого документа

· предмет и тему произведения, основные положения и выводы автора

· характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

**Перечень литературы необходимый для освоения дисциплины**

**Основная литература:**

Краковский Ю.М. Методы защиты информации: учебное пособие для вузов / Ю.М. Краковский. - 3-е изд., перераб. - Санкт-петербург: Лань, 2021. - 236 с.: ил. https://eJanbook.eom/reader/book/156401/#2

**Дополнительная литература:**

Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.

**Методическая литература:**

Конспект лекций по дисциплине «Технологии аутентификации в информационных системах».

Методические рекомендации по лабораторным работам.

Методические рекомендации по практическим занятиям.

**Интернет-ресурсы:**

Windows Server. Официальный сайт. http ://www.microsoft.com/Rus/windows-server/default.mspx

Oracle Database 10g Release 2 (10.2) Documentation

http://www.oracle.com/technology/documentation/database10gr2.html

Oracle E-Business Suite. Каталог. http://download.oracle.com/otndocs/ebs/oracle-ebs-catalogue-full.pdf