3. Использовать потенциал компьютерных технологий для формирования учебной среды по курсу ТПР;
4. Организация учебной деятельности по теории и практике в условиях доступности учебного материала в новом временном режиме (24*7*17).

Новизна и достоверность предложенных методов и решений:
Организация индивидуальной траектории обучения с учетом потенциала учащегося (умение осваивать новый материал, умение встраивать в практическую деятельность, рефлексия и т.д.) на основе системы компьютерных моделей, используемых в процессе обучения.

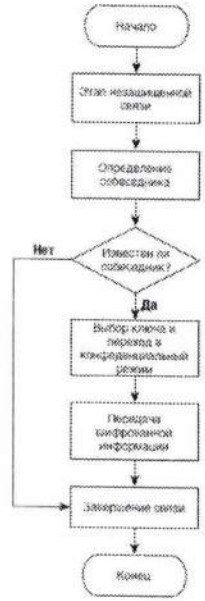
Библиографический список:

1. Васильева И.Б., Рыбаков А.В. Роль и место электронного учебника в модернизации образования // Вестник МГТУ «Станкин», 2012, № 2, С.102-107.
2. Васильева И.Б., Воеводина К.В., Рыбаков А.В. Влияние информационных технологий на процесс профессиональной подготовки специалистов по обслуживанию оборудования с ЧПУ // Информационно-аналитический PLM – журнал CAD/CAM/CAE Observer, 2012, №4, С.80-86.
3. Краснов А.А., Рыбаков А.В.,. Евдокимов С.А. Создание САПР технологической оснастки (на примере учебно – проектной САПР гладких калибров), - М.: ФГБОУ ВПО МГТУ СТАНКИН, 2015. – 167 с.
4. Гаврилова В.М. Применение системы моделей в ходе компьютерного обучения//Материалы студенческой научно-практической конференции «Автоматизация и информационные технологии (АИТ-2014). Первый тур,2014, С.88
5. Гаврилова В.М. Возможности создания интеллектуальных обучаемых систем на основе нечеткого деятельного подхода в обучение//Материалы студенческой научно-практической конференции «Автоматизация и информационные технологии (АИТ-2014). Первый тур,2014, С.122
6. Гаврилова В.М. Построение компьютерной среды обучения студентов на основе представления процесса деятельности в виде системы компьютерных моделей (на примере построения курса "Теория принятия решений") //Материалы университетского тура студенческой научно-практической конференции «Автоматизация и информационные технологии (АИТ-2014). Второй тур,2014, С.19

ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ В ОБЕСПЕЧЕНИЕ БЕЗОПАСНОЙ СВЯЗИ

Гордюк А.А.
Научный руководитель: Кабак И.С. – к.т.н., профессор
Кафедра «Компьютерные системы управления» ФГБОУ ВПО МГТУ «СТАНКИН»

Многочисленные выявленные случаи подслушивания телефонных переговоров, ставят задачу обеспечения надежной и защищенной связи с использованием мобильных устройств. Технической базой для решения этой задачи является разработка и повсеместное использование достаточно дешевых и простых в эксплуатации мобильных устройств, например, смартфонов с операционной системой Андроид.



Современные смартфоны имеют необходимые средства для решения достаточно ресурсоемких задач, но и ориентированы, в первую очередь, на последовательное выполнение задач операционной системой. Эти ограничения были учтены в данной разработке.

Процесс обмена информации представлен в виде нескольких последовательных этапов:

- Короткий этап незащищенной связи. На этом этапе система решает задачу распознавания собеседника при помощи биометрической информации (голоса).
- Определение открытого ключа для асимметричной шифрации данных
- Переход в конфиденциальный режим связи
- Потоковая шифрация/ дешифрация информации
- Завершение связи

Схема связи приведена на рис.1

Рис. 1. Предлагаемая блок-схема связи

На первом этапе, в самом начале разговора система пытается определить абонента на противоположной стороне. Определение диктора является основной проблемой в таких задачах как идентификация и верификация личности.

Для решения данной задачи можно использовать разные методы определения диктора, которые разделяются на две категории:

- Зависящие от текста – текстозависимые
- Не зависящие от текста – текстонезависимые

Первый способ основан на определённой фразе произнесенной диктором, которая сравнивается с эталоном хранящимся в базе. Основным минусом данного способа является невозможность надежного сокрытия парольной фразы.

Второй способ может использовать для идентификации пользователя любой фрагмент речи, для этого используются уникальные особенности голоса диктора, которые выделяются посредством различных алгоритмов.

Воспользуемся методами текстонезависимой идентификации, а именно методом мел-кепстральных коэффициентов (MFCC). Он позволяет существенно сократить количество параметров, которые требуются нейронной сети для принятия корректного решения.

На основе фрагмента записи голоса, определяется его спектр. Для этого можно например, использовать алгоритмы быстрого преобразования Фурье (БПФ). Затем распределим его по мел-шкале и вычислим энергию сигнала.

На полученные энергии применим дискретное косинусное преобразование, в результате чего получим последовательность мел-кепстральных коэффициентов. Это множество мел-кепстральных коэффициентов является входной информацией обученной искусственной нейронной сети, которая решает задачу классификации объекта. Процесс преобразования записи голоса в мел-кепстральные коэффициенты показан на рис.2.

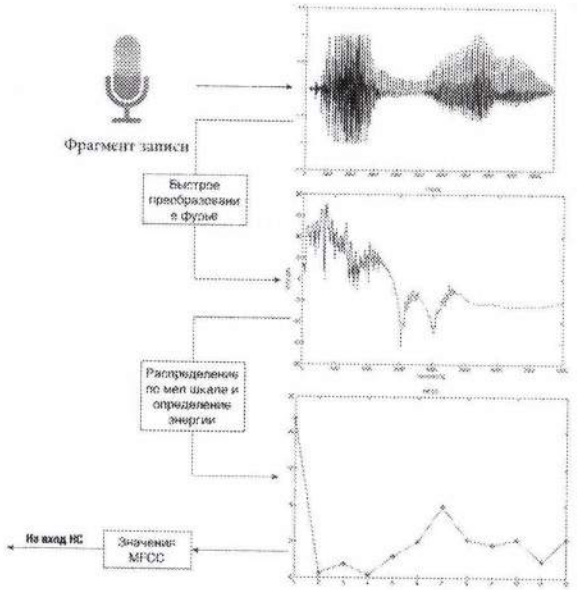


Рис. 2 Процесс преобразования записи голоса

После определения собеседника, переходим к процессу выбора ключа и шифрованию.

Вторым этапом задачи является определение открытого ключа шифрации.

Существуют две группы алгоритмов шифрования:

- с симметричным ключом (DES, AES, ГОСТ 28147-89)
- с открытым ключом – асимметричным (RSA, DSA, DSS)

В первом случае для шифрования и расшифровывания используется один криптографический ключ. При использование алгоритмов с открытым ключом, для расшифровки сообщения используется закрытый ключ.

Будем использовать криптосистему с открытым ключом, так как данная система имеет ряд преимуществ по сравнению с симметричными шифрами:

- Не нужно предварительно передавать секретный ключ по надёжному каналу.
- Только одной стороне известен ключ шифрования, который нужно держать в секрете.
- Пару ключей можно не менять значительное время (при симметричном шифровании необходимо обновлять ключ после каждого факта передачи).
- В больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

После получения информации о собеседнике от нейронной сети, выбираем открытый ключ из базы открытых ключей и используем его для шифрования сообщений.

Следующим этапом является шифрование.

На этом этапе при получение открытого ключа собеседника. Для шифрования используется операция возведения в степень по модулю большого числа. Данный алгоритм широко распространен и является частью многих стандартов(ISO 9796, SWIFT, ANSI X9.31 rDSA).

Приведенный в данной работе метод позволяет надежно защитить передаваемую информацию. Использование криптографической системы с открытым ключом и выбор ключа на основе решения нейронной сети придает системе повышенную надежность. Приведенный метод позволит осуществить передачу информации только в случае полного соответствия открытого ключа и биометрических данных собеседников, в ином случае, ключи у пользователей не будут совпадать, что приведет к невозможности расшифровки данных.

Библиографический список:

1. А.А. Гордюк Конфиденциальная телефонная связь на операционной системе «Андроид». Известия Кабардино-Балкарского государственного университета. 2014. Т. 4, № 5. С. 15–16.