ЗАЩИЩЕННЫЙ РАДИОКАНАЛ ДЛЯ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ АВТОМАТИЗИРОВАННЫМИ ОБЪЕКТАМИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Григоришин В.А.

Лихачев Д.С. – к.т.н., доцент

На сегодняшний момент существует множество объектов, как промышленного, так и бытового назначения, в которых присутствует в той или иной степени автоматизация различных процессов. При удаленном контроле и управлении такими автоматизированными объектами используется пакетная передача данных, по радиоканалу или другим системам телекоммуникации, непосредственно с самого автоматизированного объекта на централизованный пульт оператора.

Применение системы автоматизированного контроля и управления объектами с зашифрованным радиоканалом особенно актуально в нефтегазовой промышленности, в системах газораспределения, в газовых котельных, на газовых распределительных подстанциях, в системах контроля и учета электроэнергии, в системах дистанционного управления стратегически важными объектами, узлами, оборудованием, т.е. там, где скорость и последствия принятия решения имеют существенное значение. По этой причине необходимо предусмотреть надежную защиту радиоканала от несанкционированного доступа на любом этапе взаимодействия оператора централизованного пульта управления и удаленного автоматизированного объекта.

Отталкиваясь от сферы применения, радиоканал должен иметь следующие характеристики защиты передаваемой информации:

- надежную защиту от несанкционированного подключения и доступа к удаленному объекту, а также к централизованному пульту оператора [3];
- надежную защиту от несанкционированного перехвата передаваемой информации и дальнейшего использования перехваченной информации для управления и контроля автоматизированным объектом;
- зашифрованный радиоканал должен иметь устойчивую и надежную криптозащиту информации, передаваемой на большие расстояния [2].

В настоящее время распространены следующие методы защиты информации, передаваемой по радиоканалу:

1. Препятствие. Этот метод не удовлетворяет поставленным задачам, так как на физическом уровне ограничить доступ к радиоканалу невозможно.
2. Метод управления доступом. Опираясь на этот метод, можно реализовать одно из предъявленных требований для защищенного радиоканала – обеспечить защиту от несанкционированного подключения, но передаваемая информация вовсе не будет защищена.
3. Маскировка, т.е. защита информации посредством ее криптографического закрытия. Используя этот метод можно реализовать все ранее перечисленные характеристики, которыми должен обладать защищенный радиоканал. Используя секретные алгоритмы шифрования и дешифрования информации, можно обеспечить минимальный риск несанкционированного подключения и перехвата информации, передаваемой по радиоканалу, и сделать невозможным дальнейшее использование перехваченной информации.
4. Регламентация. Этот метод защиты информации не применим к цифровой технике, осуществляющей автоматизированное управление объектами различного назначения.
5. Принуждение. Метод может быть применим к персоналу и сотрудникам обслуживающих систему.
6. Побуждение. Этот метод защиты информации не применим к цифровой техники, осуществляющей автоматизированное управление объектами различного назначения.

Для обеспечения безопасности информации от несанкционированного доступа, передаваемой по радиоканалу, предлагается использовать метод маскирования, так как он в наиболее полном объеме удовлетворяет требованиям поставленной задачи [1].

В методе маскирования предлагается использовать симметричные и асимметричные алгоритмы шифрования информации. В асимметричных системах необходимо применять длинные ключи (512 битов и больше). Длинный ключ хотя и резко увеличивает время шифрования, но позволяет распределять ключи по незащищенным каналам. В симметричных алгоритмах, в которых используются более короткие ключи, шифрование происходит быстрее, но в таких системах сложно обеспечить надежное распределение ключей.

Совместное использование симметричного и ассиметричного алгоритмов позволит с минимальными аппаратными затратами реализовать защиту радиоканала и передавать информацию по защищенному радиоканалу в режиме реального времени.

Протокол обмена информацией между автоматизированным объектом и центральным пультом оператора можно описать следующим образом:

- получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным;
- отправитель, используя открытый ключ получателя, зашифровывает сеансовый ключ, который пересылается получателю по незащищенному каналу;
- получатель получает сеансовый ключ и расшифровывает его, используя свой секретный ключ;

отправитель зашифровывает сообщение сеансовым ключом и пересылает получателю;

– получатель получает сообщение и расшифровывает его.

Список использованных источников:
1. Водолазский В. Коммерческие системы шифрования: основные алгоритмы и их реализация. Часть 1. – М.: Монитор, 1992. – 14с.
2. Ковалевский В., Максимов В. Криптографические методы. – СПБ.: КомпьютерПресс, 1993. – 31с.
3. Мафтик С. Механизмы защиты в сетях ЭВМ. – М.: Мир, 1993.

СИСТЕМА КОРРЕКЦИИ РЕЧИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Демидович В.С.

Лихачев Д.С. – к.т.н., доцент

Важнейшим достижением человека, позволяющее ему использовать общечеловеческий опыт, является речевое общение, которое развивалось на основе трудовой деятельности. Речь – один из важнейших элементов человеческой деятельности, позволяющий человеку узнавать мир, делиться знанием и опытом с другими людьми.

В настоящее время большое количество людей страдает теми или иными расстройствами нарушения речи (нарушение звукопроизношения, темпа речи и др.), и их количество постепенно увеличивается. В логопедии и медицине на сегодняшний день существует большое количество разнообразных методик по коррекции дефектов речи: от лекарственных препаратов, физических и дыхательных упражнений до хирургических операций.

У людей с дефектами устной речи может наблюдаться как одно расстройство речи, так и несколько одновременно, поэтому к данным пациентам необходимо применять комплексное лечение. В настоящее время существуют тренажеры для коррекции речи. Например, АКР «Монолог» для коррекции при заикании. В основном данные тренажеры узконаправленные и используются для коррекции одного расстройства и под контролем специалистов. Поэтому актуальным является вопрос создания комплексной системы коррекции речи.

К нарушениям устной речи относятся:

1) *брадилалия* и *тахилалия* (нарушение темпа речи);
2) *заикание*;
3) *дислалия* (нарушение звукопроизношения);
4) *ринолалия* (нарушение тембра голоса);
5) *алалия* (отсутствие или недоразвитие речи вследствие органического поражения речевых зон коры головного мозга);
6) *афазия* (полная или частичная утрата речи, обусловленная локальными поражениями головного мозга);

При нарушении темпа речи коррекционная работа строится на различных речевых упражнениях. Основные упражнения: *произношение речевого материала различной сложности* (слогов, слов, коротких фраз, скороговорок и т. п.), *чтение под отбиваемый рукой такт, под метроном с постепенным ускорением темпа говорения и чтения*; *прослушивание и воспроизведение речевого материала, записанного в ускоренном темпе*; *запись слогов, слов* и т. п.

При заикании используются следующие виды коррекции*: прямое торможение речевого центра* (замедление речи, ритмизация речи, длительное молчание), *включение двигательной сферы в процесс речеобразования* (синхронизация речи с движением пальцев рук, артикуляционный контроль).

Основные этапы коррекции при дислалии: 1) *формирование первичных произносительных умений и навыков* (подражание, с механической помощью, смешанные); 2) *автоматизация звука и включение его в речь*.

При ринолалии осуществляются следующие виды корректировок: активизация работы артикуляционного аппарата (способы активизации зависят от состояния дефекта); развитие артикуляции звуков; разделение звуков с целью предотвращения нарушения звукового анализа; устранение назальных звуков; нормализация просодики речи.

При алалии упор в корректировке направляется в первую очередь на создание речевой системы: формирование коммуникативного намерения, формирование внутренней программы высказывания, лексическая развёрстка, отбор и организация системы лексико-грамматических средств, грамматическое структурирование.

При афазии методика коррекционной работы подбирается, учитывая, какие участки головного мозга пострадали, а какие функционируют в нормальном режиме. Необходимо учитывать, что восстановление речевого механизма сильно отличается от его формирования, поскольку высшие корковые функции говорящего и пишущего человека организованы иначе, чем у человека, начинающего говорить.

Проанализировав данные заболевания и логопедические методы коррекции речи, для включения в систему коррекции речи были выбраны следующие дефекты речи: нарушение темпа речи, заикание, дислалия. Выбор данных дефектов был обусловлен возможностью автоматизации некоторых методов коррекционной работы.

При нарушениях темпа речи в тренажере планируется использовать речевые упражнения с использованием корректоров темпа. Пользователю будет предложено прослушать фрагмент звукового