ческие методы атаки против алгоритма и лишь незначительно снижает скорость шифрования.

Преимуществами предложенного метода шифрования данных являются малый объем необходимой памяти (менее 1 Кбайт) и высокая скорость кодирования информации. Аналитические методы атаки против данного алгоритма не дают результата, а поиск ключа прямым перебором неэффективен ввиду его большой длины $((256!)^3 \tilde{n} 2^N$, где 256 - количество байт в каждом массиве, 3 - число массивов, N - разрядность LFSR).

Таким образом, предлагаемая криптосистема представляет собой удачное сочетание высокой степени защиты данных с хорошей производительностью при потреблении незначительных ресурсов.

СОЗДАНИЕ ЭЛЕКТРОННОГО УЧЕБНИКА С ОТСЛЕЖИВАНИЕМ ОШИБОК ОБУЧЕНИЯ В СРЕДЕ MULTIMEDIA

Матюшков Л.П., Зудина Г.С.

Анализ литературных источников, статей и отчетов стажеров позволяет сделать вывод,что использование ПК в учебном процессе развивается в двух направлениях: использование промышленных систем производства работ (типа P-CAD, Auto CAD и других)и создания учебников в среде MULTIMEDIA.

Улучшение эргономических показателей экранов, нарастающая мощность компьютеров и ресурсов памяти позволяют создать электронный учебник со средствами контроля усвоения материала и возможностями корректировки усваивания. Обычно ошибки классифицируются по трем видам: нарушение принципа постепенности, отсутствие связи предмета с реальным физическим миром(отсутствие массы) и непроясненные слова.

При создании такого учебника автор строго определяет последовательность изучения материала, первое вхождение ключевых слов, которые должны быть прояснены в соответствии со спецификой предмета, и область действия мультипликационной вставки ,для обретения обучающимся массы.

Операционная система WINDOWS, с возможностью наложения окон и графическим экраном имеет эффективные средства для решения поставленной задачи.

Создание электронного учебника делится на несколько этапов:

-создание структурной схемы учебника с включением приложений;

-создание гипертекста учебника;

-создание библиотеки графических иллюстраций;

-создание интерактивной среды чтения учебника.

Каждый электронный учебник должен иметь доступ к толковому словарю языка на котором он написан.

Техническая реализация методом объектно-ориентированного программирования в среде WINDOWS.

ОБ ОДНОМ ПОДХОДЕ К МЕХАНИЗМУ СОЗДАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ ДОКУМЕНТОВ В ЛВС

Матюшкова Г.Л., Матюшков Л.П.

В задачах по автоматизации научных исследований, проектирования, а также обработки различной рыночной и конъюктурной информации является важным не только защита информации, но и ответственность лиц и организаций, внесших ее непосредственно в базу данных. В таких случаях говорить о мере ответственности лиц и организаций за качество работы относительно их доли труда, зафиксированного в соответствующей базе данных, можно лишь при наличии электронной подписи под результатами работы.

Изложим концепцию возможной реализации таких подписей. Как и во всех принятых в мире моделях подписи, за основу возьмем в широком смысле слова текст (в виде нулей и единиц, букв и цифр или в других формах представления, позволяющих, например, вычислять от них некоторые целочисленные функции). Чтобы считать такой текст документом, необходима подпись под ним. Поэтому второй посылкой является обеспечение неотделимости подписи от документа. Это достигается тем, что подпись является функцией от рассматриваемого нами текста. Результат вычисления функции от данного текста должен быть воспроизводимым третьим лицом (нотариусом, арбитражным органом или администратором сети) после вскрытия секретного пакета, касающего процедуры, связанной с передаваемым текстом, временем суток, с фиксацией некоторого обязательного соотношения для всего переданного текста и его подписи.

Для простоты рассмотрим случай, когда подпись является некоторым вектором V (y 41 0(x),y 42 0(x),...,y 4i 0(x),...,y 4n 0(x), y 4n+1 0(y 41, 0y 42, 0..., y 4n 0)), где y 4i 0(x) - значение простой легко вычисляемой от x (текста) функции, а y 4n+1 0(y 41,..., 0y 4n 0) - контрольная функция. Суть вопроса состоит в том, что функции выбирает человек, который ставит электронную подпись и они известны только ему. В частности, вычисление вектора (всех y 4i 0(x)) может обеспечиваться процедурой, которую он хранит на дискете в своем сейфе, а точно такая же копия дискеты может лежать в ячейке арбитра. Функция y 4n+1 0 играет роль контрольного разряда. Отдельно могут вычисляться некоторые функции, которые связаны с фактом общения пользователя с машиной или с другим человеком в данной ЛВС, смысл которых - подтвердить факт общения, время, дату и номер рабочего листа.