

УДК 371.3.001.8

В.К. Маригодов, профессор, д-р техн. наук*Севастопольский национальный технический университет**ул. Университетская, 33, г. Севастополь, Украина, 99053**E-mail: root@sevgtu.sebastopol.ua***ЗАЩИТА УЧЕБНОЙ ИНФОРМАЦИИ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ**

Рассматриваются методы защиты учебной информации в системах дистанционного обучения. Проведен сравнительный анализ эффективности методов и рассмотрена целесообразность их практического использования.

Ключевые слова: дистанционное обучение, защита учебной информации, анализ методов защиты

Постановка задачи. Системы дистанционного обучения (СДО) находят все большее применение в учебном процессе вузов и университетов Украины. Актуальной задачей при подготовке студентов заочной формы обучения является широкое использование компьютерных средств и систем контроля знаний. При разработке СДО особое внимание должно быть обращено на защиту информации и безопасность функционирования системы. СДО – сравнительно дорогое «удовольствие». В связи с этим, необходимо предотвратить возможность проникновения в эту систему несанкционированных пользователей. Это важно еще и потому, что СДО рассчитана на передачу абонентам материалов новейших электронных учебников и учебных пособий. В СДО должен быть предусмотрен сервис разграничения прав доступа, с помощью которого происходит прохождение передаваемой информации только для конкретного пользователя, а также определяются «границы видимости» уровней системы и безопасность, отделяющая СДО от внешнего мира.

Анализ публикаций и нерешенные задачи. Основные принципы построения СДО рассмотрены в [1 – 4], исследовано также моделирование СДО на основе систем массового обслуживания с различными видами приоритетов [5, 6]. Известны также способы надежной защиты СДО от несанкционированного доступа [7]. При этом используются следующие средства защиты: 1) *служба секретности данных* (защита от вскрытия учебной информации и от возможности проведения анализа интенсивности потоков информации между пользователями); 2) *служба аутентификации* (предназначена для подтверждения того, что в данный момент связи пользователь является действительно тем абонентом СДО, за которого себя выдает); 3) *служба целостности данных* (обеспечивает защиту информации от случайных и преднамеренных воздействий, направленных на изменение передаваемых сообщений); 4) *служба управления доступом* (обеспечивает защиту от несанкционированного доступа к передаваемой информации); 5) *служба сохранности информации* (обеспечивает доказательство целостности сообщения, принятого от источника и находящегося на хранении в терминале приемника); 6) *служба доставки* (обеспечивает защиту от попыток злоумышленника нарушить связь или задержать сообщение на время, превышающее время ценности передаваемой в сообщении информации).

Несмотря на многочисленные разновидности систем закрытия информации для СДО необходимо выбрать такую систему, которая обладает относительной простотой и не требует использования сложных алгоритмов зашифровывания и криптоанализа. Так, например, можно обойтись применением механизма *цифровой электронной подписи*, который подтверждает подлинность передаваемой информации и удостоверяет, что переданное сообщение получено реальным пользователем. Поэтому **целью статьи** является краткий анализ методов защиты учебной информации в СДО и выбор наиболее целесообразного метода, который удовлетворяет требованиям простоты реализации, надежности функционирования и достаточно высокой степени защиты от несанкционированного доступа.

Изложение основного материала. Схема закрытой сети связи, которая может быть использована в СДО, изображена на рисунке 1. Открытый текст x в шифраторе подвергается преобразованию $y = \lambda(x)$ и передается по каналу связи. На приемном конце с помощью ключа z осуществляется обратное преобразование и λ^{-1} в дешифраторе выполняется операция

$$\lambda^{-1}(y) = \lambda^{-1}[\lambda(x)] = x$$

Таким образом, получатель сообщения имеет дело с открытым текстом. Заметим, что под термином «текст» можно подразумевать речевые сообщения, факсимильные или малокадровые изображения.

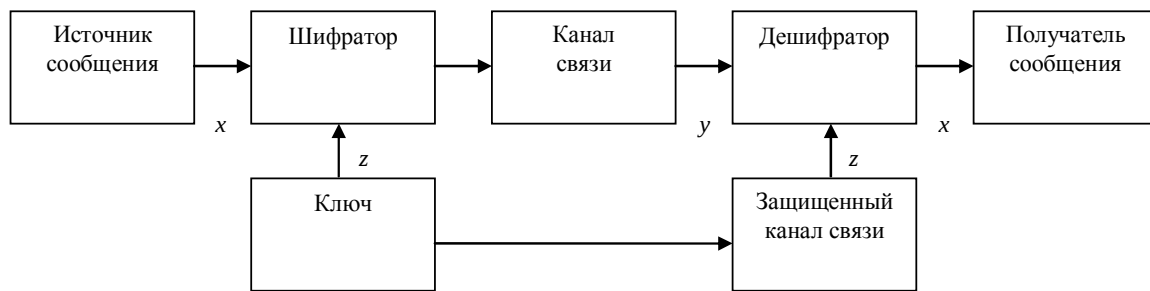


Рисунок 1 – Схема закрытой системы связи

Теоретическая (совершенная) и практическая стойкости шифра исследованы в работах [7, 8]. Как правило, потенциальные возможности этих параметров достигаются применением для их реализации чрезвычайно сложных и громоздких алгоритмов шифрования и криптоанализа.

Различают следующие разновидности шифрованной связи: «линия за линией» (link-by-link) и «из конца в конец» (end-to-end). Первая из них имеет более сложную структуру, поскольку необходимо предусмотреть в ней объединение разнородных алгоритмов шифрования, при которых нет необходимости каждой паре пользователей иметь общие ключи [9]. Вторая система гарантирует закрытие передаваемой информации на всем протяжении линии связи, однако в ней все пользователи (абоненты) должны иметь одинаковые алгоритмы шифрования. Для СДО последняя система представляется более предпочтительной вследствие простоты схемной реализации.

Рассмотрим простейшие методы шифрования и дешифрования учебной информации, которые можно рекомендовать к использованию в СДО. При передаче речевых и факсимильных сообщений в простейшем случае целесообразно при использовании в системе метода амплитудной модуляции применять принцип *полосового инвертирования*, как показано на рисунке 2.

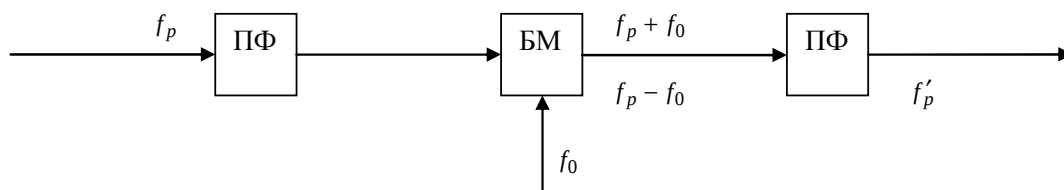


Рисунок 2 – Схема, поясняющая принцип полосового инвертирования:

f_p – мгновенное значение речевого или факсимильного сообщения;

f_0 – частота опорного генератора; БМ – балансный модулятор;

ПФ – полосовой фильтр (300 ... 3400) Гц;

f'_p – сигнал с инвертированными спектрами боковых полос модуляции

Полосовой инвертор, реализуемый с помощью балансного модулятора и полосовых фильтров, преобразует исходный спектр амплитудно-модулированного сигнала таким образом, что частота 300 Гц передается как 3400 Гц и наоборот. При этом частотные составляющие вблизи опорной частоты $f_0 = 1875 \text{ Гц}$ имеют незначительный сдвиг. Таким образом осуществляется режим, при котором инвертированные речевой или факсимильный сигналы становятся совершенно неразборчивы. Дальнейшим развитием полосового инвертирования явилось использование *метода частотной перестановки нескольких боковых полос спектра*. При этом каждая полоса может передаваться в прямом или инвертированном виде. В такой системе применяется множество полосовых фильтров и балансных модуляторов, ключ, управляющий работой коммутатора каналов (полос сигналов), коммутатор и сумматор. Для СДО целесообразно использовать небольшое количество переставляемых полос спектра сигнала, практически 5...7. При перестановке полос можно также применить прямую и обратную инверсию.

В качестве еще одного метода закрытия учебной информации можно использовать так называемую *временную перестановку*. При этом исходный речевой сигнал разбивается на ряд сегментов длительностью порядка 50 мс. Каждый из таких сегментов задерживается во времени на некоторое количество тактов по отношению к другим сегментам, как показано на рисунке 3.

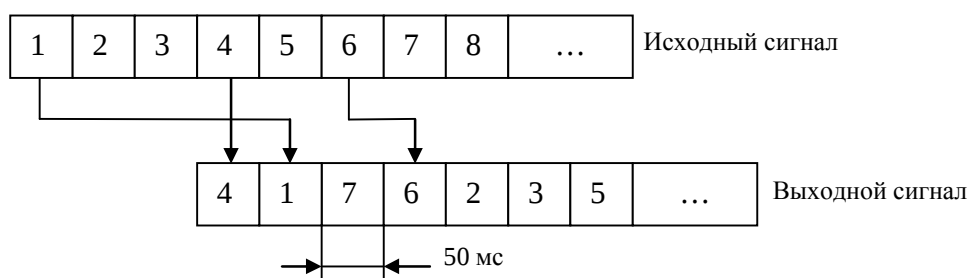
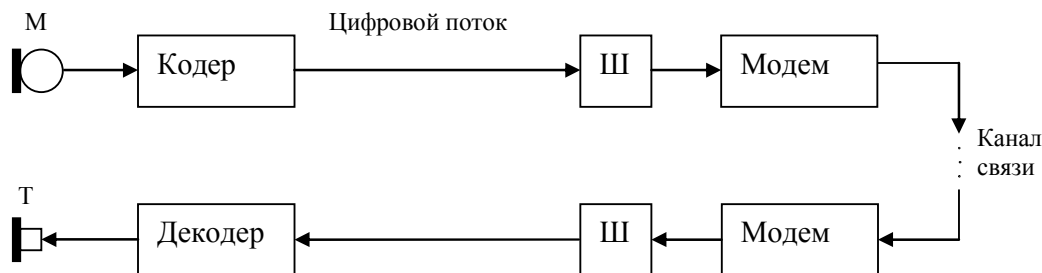


Рисунок 3 – Схема временной перестановки сегментов

Схема, изображенная на рисунке 3, обеспечивает отсутствие чувствительности к низкому качеству канала связи, но приводит к «затягиванию» речи и появлению эффекта «эхо».

Дальнейшим развитием метода перестановок явились смешанные системы, в которых используется комбинация частотных и временных перестановок спектра исходного речевого сигнала. Внедрение микроэлектроники дало возможность повысить эффективность таких систем и значительно уменьшить их вес и габариты.

В настоящее время широкое применение находят цифровые системы закрытия информации, как представлено на рисунке 4. В них исходный аналоговый сигнал представляется в виде цифрового потока данных. Этот поток шифруется и с помощью модема передается по каналу связи.

Рисунок 4 – Цифровая система закрытия информации:
М – микрофон; Т – телефон; Ш – шифратор

Цифровая система закрытия аналогового (речевого) сигнала включает в качестве основных блоков кодер, который преобразует речевой сигнал в цифровой поток символов; цифровой шифратор данных и модем, обеспечивающий передачу цифровой информации по каналу связи. На приемном конце расположен модем, шифратор и декодер, который служит для преобразования цифрового сигнала в аналоговый (речевой).

Самым простейшим способом предотвращения несанкционированного доступа к СДО может служить *электронная подпись* как электронный аналог рукописной подписи. При этом необходимо обеспечить трудность подделки подписи, а также простоту проверки ее подлинности. В связи с этим электронная подпись в отличие от физической представляет ряд символов, который сопровождает пакет учебной информации. При этом необходимо сделать подпись функцией определенного секретного ключа, который может время от времени меняться. Сама электронная подпись также должна периодически претерпевать изменения. Электронная подпись основана на использовании метода шифрования с «открытым ключом» [7].

Поскольку сеть СДО имеет разветвленную структуру, необходимо рассмотреть варианты практической ее реализации [9]. Компьютерная сеть СДО может быть построена по следующим принципам:

- коммутация пользователей (абонентов) осуществляется через центральный компьютер (сетевой сервер);
- коммутация абонентов выполняется при помощи четырехвыходовых мультиплексоров;
- коммутация пользователей, которая использует сетевой сервер и серию четырехвыходовых мультиплексоров.

Наиболее слабые места в смысле устойчивости сети – это сетевой сервер и мультиплексоры. Отказ сетевого сервера приводит к полной или частичной потере связи в сети, а отказ мультиплексоров – к полной изоляции станций, сгруппированных на базе мультиплексора. По таким параметрам, как относительная задержка в передаче информации, максимально возможное число пользователей,

устойчивость к отказам физических устройств наиболее целесообразной для применения в сети СДО является децентрализованная сеть, в которой отсутствует сетевой сервер (центральный компьютер).

Выводы и задачи дальнейших исследований. Таким образом, рассмотрены варианты методов закрытия учебной информации в сетях СДО. При этом не рассматривались такие способы шифрования и дешифрования, которые требуют применения сложных алгоритмов реализации, например система DES (США) или система ГОСТ 28147 – 89 (РФ) [7]. В связи с изложенным можно рекомендовать систему закрытой связи типа «из конца в конец», а также систему, в которой применяется полосовое инвертирование полос амплитудной модуляции с перестановкой 3...5 полос. В принципе можно с успехом использовать метод временной перестановки сегментов спектра при условии их ограниченного количества, а также цифровую систему закрытия учебной информации и электронную подпись.

К задачам дальнейших исследований в данном направлении можно отнести, например, следующие: применение в каналах связи СДО методов передачи сообщений с использованием амплитудно-частотной модуляции несущей (вначале по частоте, а потом по амплитуде); использование амплитудного или фазового предсказания модулирующих сигналов.

Библиографический список использованной литературы

1. Умрик М.А. Дистанційне навчання і професійна освіта / М.А. Умрик // Матер. докл. Междунар. конф. памяти проф. И.И. Мархеля «Новые информационные технологии в учебных заведениях Украины», Одесса, 21 – 26 июня 2005 г. — Одесса: Астропринт, 2005. — С. 170–173.
2. Давыдов В.И. Защита информации в системах дистанционного обучения / В.И. Давыдов, А.А. Змиевский // Матер. докл. Междунар. конф. памяти проф. И.И. Мархеля «Новые информационные технологии в учебных заведениях Украины», Одесса, 21 – 26 июня 2005 г. — Одесса: Астропринт, 2005. — С. 58 – 59.
3. Вербицкий В.В. Криптографическая защита электронной информации с MS CRYPTOAPI / В.В. Вербицкий, В.В. Пленский // Матер. докл. Междунар. конф. памяти проф. И.И. Мархеля «Новые информационные технологии в учебных заведениях Украины», Одесса, 21 – 26 июня 2005 г. — Одесса: Астропринт, 2005. — С. 55 – 56.
4. Десятов Т.М. Дистанційне навчання в системі неперервної освіти / Т.М. Десятов // Педагогіка і психологія. — 2003. — № 1. — С. 75 – 80.
5. Маригодов В.К. Дистанционное обучение как система массового обслуживания со смешанными приоритетами / В.К. Маригодов // Вестник СевГТУ. Сер. Педагогика: сб. науч. тр. — Севастополь, 2009. — Вып. 96. — С. 118–121.
6. Маригодов В.К. Дистанційне навчання як система масового обслуговування / В.К. Маригодов, Ю.М. Кравченко // Проблеми освіти. — 2010. — № 62. — С. 49–54.
7. Защита информации в системах телекоммуникации: учеб. пособие для вузов / В.Л. Банкет, Н.В. Захарченко, А.В. Дырда, Г.Н. Гулак и др.; под ред. В.Л. Банкета. — Одесса: Изд-во Украинский госуд. академ. связи им. А.С.Попова, 1997. — 95 с.
8. Маригодов В.К. Энтропийная оценка совершенной стойкости шифра с позиции теории игр / В.К. Маригодов, В.Л. Хайков // Вестник СевГТУ. Сер. Информатика, электроника, связь: сб. науч. тр. — Севастополь, 2003. — Вып. 47 — С. 20–25.
9. Маригодов В.К. Анализ эффективности работы компьютерных сетей экологического мониторинга / В.К. Маригодов, О.В. Слободнюк // Вестник СевГТУ. Сер. Механика, энергетика, экология: сб. науч. тр. — Севастополь, 1999. — Вып. 16. — С. 96–103.

Поступила в редакцию 30.11.2011 г.

Марігодов В.К. Захист навчальної інформації в системах дистанційної освіти

Розглядаються методи захисту навчальної інформації в системах дистанційної освіти. Наведено порівняльний аналіз ефективності методів і розглянута доцільність їх практичного використання.

Ключові слова: дистанційна освіта, захист навчальної інформації, аналіз методів захисту

Marigodov V.K. Defense of Educational Information in Distance Learning Systems

It has been demonstrated methods defense of educational information in distance learning systems. Comparative analysis efficiency of methods and has been discern expediency utilization in practice is conducted.

Keywords: distance learning, defense of educational information, defense of methods analysis.