– окончательная формулировка новых результатов, свойств, закономерностей;

– определение места найденного решения поставленной проблемы в системе имеющихся знаний.

Более детальное представление компонентов поисково-исследовательской деятельности приводит к такой последовательности действий: постановка проблемы исследования; постановка задач, адекватных проблеме исследования; предварительный анализ имеющейся информации, условий и методов решения задач исследования; формулировка исходных гипотез; теоретический анализ гипотез; планирование и организация эксперимента; проведение эксперимента; анализ и обобщение полученных в ходе исследования результатов; проверка исходных гипотез на основе полученных фактов; окончательная формулировка новых фактов, закономерностей, свойств; получение объяснений и научных предсказаний; определение места найденного решения поставленной проблемы в системе имеющихся знаний.

Список литературы

1. Далингер В.А. О тематике учебных исследований // Математика в школе. – 2000. – № 9. – С. 7-10.

2. Далингер В.А. Поисково-исследовательская деятельность учащихся по математике: учебное пособие. – Омск: Изд-во ОмГПУ, 2005. – 456 с.

3. Далингер В.А. Учебно-исследовательская деятельность учащихся в процессе изучения дробей и действий над ними: учебное пособие. – Омск: Изд-во ОмГПУ, 2007. – 191 с.

4. Далингер В.А. Математические задачи для любознательных: учебное пособие. – Омск: Изд-во ООО «Амфора», 2011. – 80 с.

5. Далингер В.А., Толпекина Н.В. Организация и содержание поисково-исследовательской деятельности учащихся по математике: учебное пособие. – Омск: Изд-во ОмГПУ, 2004. – 253 с.

Технические науки

ЗАЩИЩЕННАЯ ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА ПРЕДПРИЯТИЯ НА БАЗЕ ВИРТУАЛЬНЫХ АБОНЕНТСКИХ КАНАЛОВ

Котенко В.В., Румянцев К.Е., Панфилов С.В.

Южный федеральный университет, Таганрог, e-mail: virtsecurity@mail.ru

Целью исследования являлась разработка защищенной телекоммуникационной системы предприятия на базе виртуальных абонентских каналов. Основу исследования составила предложенная Котенко В.В. методика формирования виртуальных каналов компьютерных сетей. К базовым принципам реализации методики относятся:

1) образование виртуальных абонентских каналов локальной телекоммуникационной сети на базе радиомодемов, подключённых к звуковым платам компьютеров;

2) применение аудиостеганографии для решения задачи защиты информации. Виртуальный канал образуется непосредственно между конечными абонентами локальной телекоммуникационной системы предприятия.

Разработка системы включала два этапа:

1) этап программной реализации;

2) этап аппаратной реализации.

Основу программной реализации составил комплекс программ включающий:

1) программу Steganos Security Suite 7 для реализации аудиостеганографических функций, в результате чего данные, которые необходимо передать, прошиваются в файл-контейнер и передаются на выход звуковой платы;

2) программы Recorder для автоматической записи файла в формате WAV при появлении сигнала на входе звуковой карты и запуска программы расшифрования;

3) программы WavKompand для сверки исходного файла с файлом записанным после передачи по радиоканалу.

Аппаратная реализация системы базируется на реализации виртуальных абонентских каналов. Реализация виртуального канала осуществляется при помощи радио модемов и компьютеров. Радиомодемы соединяются с компьютером через звуковую плату. Виртуальный абонентский канал (АК) позволяет скрытно передавать информацию между абонентами с высокой степенью защиты, а также создавать независимый от общей сети канал связи. Это является основной особенностью и основным достоинством защищенного виртуального АК для любой топологии. Ввод виртуального абонентского канала обеспечивает возможность мобильного соединения и подключения абонентов телекоммуникационной системы. Еще одним преимуществом виртуального АК является его автономность и независимость от основной сети, что позволяет надежно и эффективно с точки зрения безопасности передавать информацию. Защищенный виртуальный АК может быть реализован так же в отсутствии основной компьютерной сети на базе двух компьютеров. К основной функции разработанной системы относится обеспечение безопасности передаваемой информации между абонентами. Безопасность обеспечивается с помощью аудиостеганографии. Стеганография реализуется на звуковых файлах в которые прошивается дискретная информация. Звуковые файлы передаются на заданной для каждого АК радиочастоте. В ходе экспериментальных исследований установлено, что глубина ошибки 11 разрядов составляет 2047 (3,12%). Отсюда следует, что наиболее подходящим разрядом для стеганографического кодирования является 12-й разряд.

Список литературы

1. Котенко В.В., Румянцев К.Е., Юханов Ю.В., Евсеев А.С. Технологии виртуализации процессов защиты информации в компьютерных сетях // Вестник компьютерных и информационных технологий. Науч.-практ. журн. – М., 2007. – №9 (39). – С. 46-56.

2. Котенко В.В. Оптимизация стратегии шифрования на основе виртуализации информационных потоков // Информационное противодействие угрозам терроризма. Науч.–практ. журн. – 2005. – №5. – С. 57-58.

3. Котенко В.В. Принципы кодирования для канала с позиций виртуального представления выборочных пространств ансамблей сообщений и кодовых комбинаций // Информационное противодействие угрозам терроризма. Науч.-практ. журн. – 2004. – №3. – С. 65-71.

4. Котенко В.В. Новый взгляд на условия обеспечения абсолютной недешифруемости с позиции теории информации // Информационное противодействие угрозам терроризма.: Науч.-практ. журн. – 2004. – №2. – С. 36-43.

5. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование с последовательным усложнением виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 98–98.

6. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование с параллельным усложнением виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 97–98.

7. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование на основе многомерного представления виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 97–97.

КОМПЛЕКС ЗАЩИТЫ ИНТЕРНЕТ РЕСУРСОВ

Котенко В.В., Румянцев К.Е., Миргородский С.В., Шаповалов А.В.

Южный федеральный университет, Таганрог, e-mail: virtsecurity@mail.ru, rke2004@mail.ru

Исследовалась возможность повышения эффективности защиты информации в компьютерных сетях путем применения разработанного Котенко В.В. подхода, состоящего в виртуализации сообщений и криптограмм в процессе защиты информации. В результате программной и схемной реализации решений, полученных на основе данного подхода, был создан программный комплекс защиты интернет ресурсов, обеспечивающий комплексное решение задач шифрования, аутентификации, помехоустойчивости и имитозащиты.

Функционирование передающей части комплекса разделяется на три основных этапа:

1) формирование виртуальных сообщений;

2) формирование виртуальных ключей и шифрование;

3) формирование виртуальных криптограмм.

Основной функциональной задачей первого этапа является преобразование различных видов сообщений, поступающих на вход комплекса, к единому виду, определяемому принятой моделью сообщения. Этот вид сообщений определяется как виртуальные сообщения, т.е. сообщения возможные при условии принятой модели сообщения. Для формирования виртуальных сообщений применяются псевдослучайные последовательности. Основной функциональной задачей второго этапа является формирование виртуальных ключей и их применение для преобразования сообщений в криптограммы. Для формирования виртуальных ключей применяются псевдослучайные последовательности. Основной функциональной задачей третьего этапа является преобразование криптограмм к виду, определяемому принятой моделью наблюдения. Этот вид криптограмм определяется как виртуальные криптограммы, т.е. криптограммы возможные при условии принятой модели наблюдения. Модель наблюдения задается принятыми механизмами защиты в компьютерной сети. Для формирования виртуальных криптограмм применяются псевдослучайные последовательности. Функционирование приемной части комплекса разделяется на следующие этапы:

1) девиртуализация криптограмм;

2) формирование виртуальных ключей и базовое дешифрование;

3) разделение каналов дешифрования;

4) двухканальное формирование сообщений (дешифрование);

5) оценка сообщений.

Для обеспечения защищенности процесса выполнения преобразований разработанного программного комплекса и невозможности доступа со стороны аппаратно-программной среды предусмотрена аппаратная реализация комплекса. Конструктивно программный комплекс может выполняться в виде автономного модуля с интерфейсом USB для подключения к ЭВМ. Экспериментальная проверка комплекса показала его высокую эффективность.

Список литературы

1. Котенко В.В. Оптимизация стратегии шифрования на основе виртуализации информационных потоков // Информационное противодействие угрозам терроризма. Науч.–практ. журн. – 2005. – №5. – С. 57-58.

2. Котенко В.В. Принципы кодирования для канала с позиций виртуального представления выборочных пространств ансамблей сообщений и кодовых комбинаций. // Информационное противодействие угрозам терроризма. Науч.-практ. журн. – 2004. – №3. – С. 65-71.

3. Котенко В.В. Новый взгляд на условия обеспечения абсолютной недешифруемости с позиции теории информации // Информационное противодействие угрозам терроризма. Науч.-практ. журн. – 2004. – №2. – С. 36-43.

4. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование с последовательным усложнением виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 98–98.

5. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование с параллельным усложнением виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 97–98.

6. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Шифрование на основе многомерного представления виртуальных выборочных пространств ансамблей ключа // Фундаментальные исследования. – 2004. – № 5. – С. 97–97.

7. Котенко В.В., Румянцев К.Е. Теория информации и защита телекоммуникаций: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2009. –369 с.

8. Котенко В.В. Теоретические основы виртуализации процесса защиты информации при полной априорной неопределенности источника // Прикладная радиоэлектроника. – 2011. – Т.10, №2. – С. 204-213.