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.

9. 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.

КОМПЛЕКС АУТЕНТИФИКАЦИИ БАНКОВСКИХ СИСТЕМ

Румянцев К.Е., Котенко С.В., Паньков А.А.

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

Банк как структура наиболее требовательная к защите информации использует практически весь спектр механизмов защиты информации. Одним из основных механизмов защиты является аутентификация. Целью исследования являлась разработка комплекса, обеспечивающего абсолютную аутентификацию. Основу исследования составила методика аутентификации с позиций комплексного определения разборчивости и избыточности виртуальных идентификаторов, впервые предложенная Котенко В.В. Содержание предложенной методики состоит в использовании двух видов идентификаторов: виртуального и рабочего. Виртуальные идентификаторы находятся у корреспондентов и формируются ими. Особенностью методики является то, что выборочные пространства ансамблей виртуального идентификатора X* является непрерывным, в результате чего обеспечивается его бесконечная энтропия ($H[X^*] = \infty$) для несанкционированного пользователя. Основу функционирования комплекса составляет определение среднего количества информации и разборчивости X [1]. Численные значения комбинаций этих параметров используются в качестве рабочего идентификатора.

Разработанный комплекс аутентификации банковских систем последовательно выполняет следующие функции:

1) речевой сигнал преобразуется в электрический микрофоном;

2) с выхода микрофона сигнал поступает на устройство преобразования, предназначенное для введения идентификационных признаков;

3) с выхода устройства преобразования сигнал подается на вход звуковой карты компьютера, после чего осуществляется создание звукового файла;

4) программным комплексом аутентификации осуществляется определение среднего количества информации, разборчивости и избыточности, которые выступают в роли рабочих идентификаторов;

5) в результате сравнения полученных значений рабочих идентификаторов с хранящимся в базе данных, делается вывод о подлинности исходного идентификатора.

В зависимости от результатов проведенной аутентификации выводится решение об отказе в доступе или подтверждении такового.

Используется два режима работы комплекса:

1) режим формирования рабочего и виртуального идентификаторов;

2) режим аутентификации.

Главными особенностями комплекса являются:

1. Для санкционированного доступа корреспондента к системе непосредственно используется только виртуальный идентификатор, который формируется корреспондентом в аналоговом виде самостоятельно.

2. Рабочий идентификатор используется только в качестве эталона для сравнения, что снимает необходимость его специальной защиты.

3. При желании корреспондент может оперативно изменить виртуальный идентификатор, представляя соответствующий ему рабочий идентификатор в систему.

Исследование эффективности реализованного макета комплекса показало, что его применение обеспечивает абсолютную аутентификацию

Список литературы

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

2. Котенко В.В., Абушинов О.В. Оценка избыточности аудиоинформации в задачах контроля качества информационной безопасности обьектов информатизации // Фундаментальные исследования. – 2006. – № 1. – С. 74.

3. Котенко В.В., Румянцев К.Е., Евсеев А.С., Кравцов С.В., Дорджиев М.А. Система оценки эффективности защиты аудиоинформации на основе виртуализации комплексного определения разборчивости и избыточности // Свидетельство № 2010610039 РФ. 11.01.2010.

4. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Аутентификация корреспондентов информационных и банковских систем на основе формирования виртуальных идентификаторов // Современные наукоемкие технологии. – 2004. – № 2. – С. 10.

5. Котенко В.В. Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Информационная безопасность: материалы XI Международной научно-практической конференции. Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177-183.

6. Котенко В.В. Теоретические основы виртуализации информационных потоков // Информационное противодействие угрозам терроризма. Науч.–практ. журн. – 2011. – №17. – С. 69-80.

7. Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б. Совершенствование банковской системы на основе виртуальной характеристики корреспондентов // Финансовые проблемы РФ и пути их решения: сб. трудов 5-й международной научно-практической конференции. – СПб., 2004. – С. 230-232.