8. Производится комплексная оценка степени соответствия значений W и μ эталонным идентификаторам.

Используется два режима работы программного комплекса: 1) режим формирования идентификаторов; 2) режим аутентификации.

Результаты исследования эффективности аутентификации реализованного макета комплекса показали, что его применение обеспечивает абсолютную аутентификацию. Основными отличительными 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.

Список литературы

1. Котенко В.В. Теория виртуализации и защита телекоммуникаций: – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 244 с.

2. Котенко С.В. Комплекс аурикулодиагностической идентификации // Информационное противодействие угрозам терроризма: науч.-практ. журн. – 2011. – №16. – С. 73-79.

3. Котенко С.В., Румянцев К.Е., Сторчак С.А., Паньков А.А., Бакулин К.И. Система формирования виртуального вербального образа личности // Свидетельство № 2010613972 РФ. 18.06.2010.

4. Котенко С.В., Румянцев К.Е. Оценка эффективности виртуальной аурикулодиагностической идентификации // Информационное противодействие угрозам терроризма: науч.-практ. журн. – 2011. – №16. – С. 73-79.

5. Котенко С.В. Новый подход к многофакторной персональной аутентификации: материалы Международной научно-практической конференции «Молодежь и Наука: модернизация и инновационное развитие страны». – Пенза: Изд-во ПГУ, 2011. – С.93-96.

6. Котенко В.В., Котенко В.В., Румянцев К.Е., Горбенко Ю.И. Оптимизация процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости // Прикладная радиоэлектроника. – 2013. – Т.12, №3. – С.265-273.

7. Котенко В.В., Котенко В.В., Румянцев К.Е., Горбенко Ю.И. Стратегия защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей // Прикладная радиоэлектроника. – 2013. – Т.12, №3. – С.308-313.

8. Котенко В.В., Иванков И.Н. Модель защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей // Информационное противодействие угрозам терроризма. Научно-практический журнал. – 2013. – №20. – С.196-201.

9. Котенко В.В., Румянцев К.Е., Поляков А.И., Ежов А.И. Модель оптимальной защиты непрерывной информации // Международный журнал прикладных и фундаментальных исследований. – 2013. – №8 (часть 3). – С.73-74.

10. Котенко В.В., Румянцев К.Е., Поляков А.И., Хмелев И.С., Ежов А.И. Алгоритм оптимизации декодирования на основе виртуализации информационных потоков // Международный журнал прикладных и фундаментальных исследований. – 2013. – №8 (часть 3). – С.73-74.

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ЗАЩИТЫ КОРПОРАТИВНЫХ ИНТЕРНЕТ РЕСУРСОВ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Котенко В.В., Румянцев К.Е.,
Хмелев И.С., Ермолаев А.Ю.

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

Важнейшей составляющей качества функционирования телекоммуникационных систем является качество защиты информации. Обеспечение этой составляющей в настоящее время сталкивается с целым рядом проблем, основной из которых выступает противоречие между потенциальными возможностями существующих подходов и постоянно возрастающими требованиями к защите информации. К одной из таких проблем относится проблема защиты интернет ресурсов. В значительной мере эта проблема проявляется в недостаточной эффективности комплексной защиты файловой системы в компьютерных сетях.

Исследовалась возможность повышения эффективности защиты информации в компьютерных сетях путем применения подхода [1], состоящего в виртуализации сообщений и криптограмм в процессе защиты информации. Разработанная на основании подхода методика [1] определяет область возможных схемных решений, которая включает три основных этапа: виртуализация сообщений; виртуализация цифровой обработки; виртуализация криптограмм. Основу реализации схемных решений составляет алгоритм виртуальных оценок:

$$\begin{cases} \mathbf{u}^*_{i-1} = \left(\tilde{\mathrm{e}}^*_i - \tilde{\mathbf{v}}_i\right)\mathrm{H}_i^{-1}\mathbf{G}_{i-1}^{-1} - \left(\mathbf{\Phi}_{i-1,i\text{-}2}\tilde{\mathbf{s}}^*_{i-2} - \left((\tilde{\mathbf{s}}^*_i - \tilde{\mathbf{s}}^*_{i-1}) - (\mathbf{w}_i - \mathbf{w}_{i-1})\right)\right)\mathbf{G}_{i-1}^{-1} - \mathbf{n}_{i-1}, \\ \mathbf{u}^*_i = \left(\tilde{\mathrm{e}}^*_i - \tilde{\mathbf{v}}_i\right)\mathrm{H}_i^{-1}\mathbf{G}_i^{-1} - \left(\mathbf{\Phi}_{i,i\text{-}1}\tilde{\mathbf{s}}^*_{i-1} - \left(\mathbf{w}_i - \mathbf{w}_{i-1}\right)\right)\mathbf{G}_i^{-1} - \mathbf{n}_i, \end{cases}$$

где $\mathbf{u}^*_i$ – оценка сообщения; $\mathbf{n}_i$ – формирующий шум, $\mathbf{\Phi}_{i,i\text{-}1}$ и $\mathbf{G}_i$ – матрицы модели виртуального сообщения; $\tilde{\mathrm{e}}^*_i$ и $\tilde{\mathrm{e}}^*_i$ – виртуальные криптограммы; $\tilde{\mathrm{v}}_i$ и H_i^{-1} – шум и матрица модели наблюдения; $\mathbf{w}_i$ – ключевые последовательности.

В результате программной и схемной реализации алгоритма 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) форми-

рование 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.

Созданный программный комплекс защиты интернет ресурсов обеспечивает комплексное решение задач шифрования, аутентификации, помехоустойчивости и имитозащиты. Дальнейшее развитие разработанной компьютерной технологии открывает возможность создания единой системы защиты информации, обеспечивающей новые классы стойкости шифрования. Полученные результаты являются новыми, не имеют аналогов и могут быть использованы при модернизации действующих и в процессе разработки перспективных телекоммуникационных систем и компьютерных сетей, а так же в учебном процессе при подготовке специалистов в области информационной безопасности..

Список литературы

1. Котенко В.В. Теория виртуализации и защита телекоммуникаций: – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 244 с.

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

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

6. Котенко В.В., Иванков И.Н. Модель защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей // Информационное противодействие угрозам терроризма: науч.-практ. журнал. – 2013. – №20. – С. 196-201.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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. – Москва. – 2007. – №9 (39). – С. 46-56.

«Наука и образование в современной России», Россия (Москва), 13-15 ноября 2014 г.

Географические науки

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ГЛУБОКОВОДНЫХ РЕСУРСОВ МОСКОВСКОГО РЕГИОНА

Семенова И.В.

Московский государственный машиностроительный университет, Москва, e-mail: vzpi_semenova@mail.ru

Московский регион является крупным промышленным центром России, в котором до 95% потребностей в воде для промышленных и бытовых целей обеспечивается за счет эксплуатации глубинных артезианских скважин. Геологической особенностью Московской области является наличие пяти глубоководных горизонтов, которые пересекают область с севера на юг. Состав подземных вод региона неоднозначен. Проведенные нами на протяжении нескольких лет исследования показали, что во многих районах региона воды загрязнены катионами тяжелых металлов, а также стронцием и кремнием [1,3].