37%) и νC-H аром (3058 см$^{-1}$, 39%, 3056 см$^{-1}$, 50%, 3060 см$^{-1}$, 54%).

Рассмотренные колебательные частоты являются отличительной спектральной характеристикой 4-бензоилоксикарбоновых кислот и могут быть использованы для идентификации и подтверждения структуры соединений этого класса.

Экспериментальный спектр КР соединения (**I**) в растворе бензол-хлороформ был зарегистрирован на спектрометре ДФС-24 с использованием линии 488 нм аргонового лазера ЛГН-503 мощностью 200 мВт на образце. Погрешность в определении положения полос КР не превышала ± 2 см$^{-1}$.

Список литературы

1. Деркач Л.Г., Теслюк О.И., Новикова Н.С., Дога П.Г., Яркова М.Ю., Мешкова С.Б. // ЖОХ. – 2014. – Т.84. – Вып. 7. – С.1095.

2. Binnemans K., Görlle-Walrand Ch. // Chem. Rev. – 2002. – V.102. – P.2303.

3. Новикова Н.С., Килименчук Е.Д., Кондратьева Р.В., Мешкова С.Б., Топилова З.М. // ЖПХ. – 2011. – Т.84. – Вып.6. – С.954.

4. Новикова Н.С., Килименчук Е.Д., Яркова М.Ю., Мешкова С.Б., Топилова З.М. // ЖПХ. – 2008. – Т.81. – Вып.8. – С.1528.

5. Gaussian 03, Revision B 03. Gaussian, Inc., Pittsburgh PA, 2003.

6. Scott P.A., Radom L. // J. Phys. Chem. – 1996. – V.100. – № 41. – P.16502.

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ МЕТОДИКИ АУТЕНТИФИКАЦИИ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ РЕЧЕВЫХ ИДЕНТИФИКАТОРОВ

Котенко В.В., Румянцев К.Е., Брагин И.А., Котенко С.В., Макаренко Я.А.

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

Целью исследования являлась разработка программного комплекса, обеспечивающего абсолютную аутентификацию. Основу исследования составила методика аутентификации с позиций комплексного определения разборчивости и избыточности виртуальных идентификаторов [1,2]. Содержание реализуемой 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*]=∞) для несанкционированного пользователя. Основу функционирования комплекса составляет определение среднего количества информации и разборчивости [1,2]. Численные значения комбинаций этих параметров используются в качестве рабочего идентификатора.

Введение идентификационных признаков осуществляется путем зашумления исходного речевого идентификатора пользователем. Основу математических моделей разборчивости W и избыточности μ составляют выражения:

$$I=0{,}01W\log_2 0{,}01W+(1-0{,}01W)\log_2\left(\frac{1-0{,}01W}{L-1}\right)-$$

$$-\sum_{l=1}^{L}\left\{0{,}01D_pP\left(x^{(l)}\right)+\frac{1-0{,}01D_p}{L-1}\left[1-P\left(x^{(l)}\right)\right]\right\}\times$$

$$\times\log_2\left\{0{,}01WP\left(x^{(l)}\right)+\frac{1-0{,}01W}{L-1}\left[1-P\left(x^{(l)}\right)\right]\right\},$$

$$\mu_{S_{ce}}\left[S_{cs}\right]=1-\left(1-\overset{o}{I}\left[S_{cs};S_{ce}\right]\right)\frac{H\left[S_{cs}\right]}{H_{max}\left[S_{cs}/S_{ce}\right]},$$

$$H\left[S_{cs}\right]=-W\cdot\log W-\frac{1-W}{M-1}\log\left(\frac{1-W}{M-1}\right),$$

$$H_{max}\left[S_{cs}/S_{ce}\right]=\frac{1-W}{M-1}\log\left(M-1\right)-$$

$$-\frac{1-W}{M-1}\log\left(\frac{1-W}{M-1}\right)-W\cdot\log W,$$

где W – разборчивость; M – количество логических элементов речевых сообщений в выборочном пространстве ансамбля сообщений; I – среднее количество информации.

Алгоритм аутентификации по разборчивости и избыточности на основе формирования виртуального идентификатора:

1. Задается N_i частот f_i, соответствующих средним частотам спектральных информационных каналов (N_i=20) с равным средним количеством информации: 0,1; 0,22; 0,32; 0,41; 0,475; 0,55; 0,65; 0,77; 0,88; 0,99; 1,43; 1,85; 2,24; 2,45; 3,23; 3,72; 4,22; 4,76; 5,60; 6,65 (кГц).

2. Формируется виртуальный идентификатор.

3. На основе спектров сигнала, соответствующего логическому элементу сообщения, и шума рассчитываются отношения сигнал/шум на средних частотах f_i спектральных каналов с равным средним количеством информации.

4. Для каждого спектрального канала определяется коэффициент восприятия.

5. По значениям коэффициентов восприятия рассчитывается среднее количество информации логического элемента аудиосообщения, выделяемое слухом.

6. Разборчивость W логического элемента аудиосообщения, выделяемого слухом, определяется из графика на основании (1).

7. Избыточность μ логического элемента аудиосообщения, выделяемого слухом, определяется из W.

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-