5. Erick Cantú-Paz A Survey of Parallel Genetic Algorithms // Department of Computer Science and Illinois Genetic Algorithms Laboratory University of Illinois at Urbana-Champaign, 2013. – С. 5.

6. Darrell Whitley Genetic Search for Feature Subset Selection: A Comparison Between CHC and GENESIS // Department of Computer Science Colorado State University Fort Collins, Colorado 80523 USA, 2012. – С. 7.

7. Dr. M.V. Siva Prasad An Intrusion Detection System Architecture Based on Neural Network and Genetic Algorithms // Principal Anurag Engineering College, 2013. – С. 6.

Л.Ф. Зиангирова, Т.И. Саттаров

СТЕГАНОАНАЛИТИЧЕСКИЕ МЕТОДЫ ДЛЯ ПЕРЕСЫЛАЕМЫХ КОНТЕЙНЕРОВ

(Башкирский государственный педагогический университет им. М. Акмуллы,
Уфимский государственный нефтяной технический университет)

Появление методов скрытой передачи данных посредством пересылаемых контейнеров привело к развитию стеганографического программного обеспечения. Пересылаемый контейнер – это объект в виде текста, архива, фотографии, звукового файла, видео файла и других объектов, пересылаемых через электронную почту, социальные сети, форумы, системы мгновенного обмена сообщениями, а также копирование на внешние носители.

Существуют различные решения для защиты сети предприятия от утечки из нее конфиденциальной информации. Данный класс решений получил название DLP (Data Leakage Prevention). DLP-система предназначена для контроля информационных потоков, защиты конфиденциальной информации от утечки и несанкционированного распространения. Известные представители DLP-систем: Websense DSS, InfoWatch, Symantec DLP, SearchInform и др. Данные системы перехватывают весь трафик, выходящий за пределы сети предприятия, и сканируют его на наличие в нем конфиденциальных данных. Также DLP-системы сканируют всю информацию, записываемую пользователями сети на съемные носители при помощи их рабочих станций. Они способны отследить конфиденциальную информацию, передаваемую в открытом или заархивированном виде, пресечь передачу зашифрованных данных.

Стеганографические программы предотвращают способность инсайдера передать конфиденциальные данные за пределы сети предприятия способом включения битов информации в мультимедийные контейнеры, которые не запрещены для передачи.

В зависимости от используемых исходных данных методы стеганоанализа можно разделить на следующие группы:

– Методы, предназначенные для работы с конкретными заранее известными стеганографическими алгоритмами.

– Методы, предназначенные для любых алгоритмов стеганографии.

К методам, предназначенным для работы с конкретными заранее известными стеганографическими алгоритмами, относят сигнатурные методы анализа. В сигнатурных методах рассматривается синтаксический анализ предъявленной на вход распознающего устройства последовательности терминальных символов, определяющих контейнер. В случае обнаружения принадлежности предъявленной на вход распознавателя цепочки терминальных символов языку, описывающему ту или иную стеганосистему, принимается решение об ее использовании для скрытия информации.

К методам, предназначенным для любых алгоритмов стеганографии, относят визуальные и статистические методы.

Визуальные методы базируются на способности зрительной системы человека анализировать зрительные образы и выявлять существенные различия в сопоставляемых изображениях. Например, рассмотрим метод визуального анализа битовых срезов. Основная идея метода заключается в сравнении изображения в целом с изображениями его битовых срезов [1]. С помощью программы изображение просматривают по слоям, т.е. по битовым срезам. Интенсивность каждого цвета определяется ровно одним байтом. Поэтому необходимо просмотреть восемь срезов. Для каждого из трех цветов первый срез – это изображение, построенное самыми младшими битами, второй срез – изображение, построенное вторыми битами и т.д. Полученное изображение битового среза просматривают и визуально сравнивают с анализируемым изображением.

Большинство методов стеганоанализа основано на обнаружении отклонения наблюдаемой мультимедийной информации от его ожидаемой модели. Статистические методы стеганоанализа используют множество статистических характеристик, таких как: коэффициенты корреляции, оценка числа переходов значений младших бит в соседних элементах изображения, анализ распределения пар значений на основе критерия Хи-квадрат, анализ гистограмм, построенных по частотам элементов изображения и др.

Известны методы стеганоанализа, направленные против конкретных стеганоалгоритмов. Например, методы стеганоанализа изображений, в которых производится внедрение в наименьший значащий бит, исследуют распределение этих битов, а также корреляционные связи между ними.

В настоящее время существует огромное количество свободно распространяемых программ стеганографии. Примеры программ для внедрения в изображения: S-Tools, EZStego, JPEG/JSteg, PGE, ScyTale; в музыкальные файлы: MP3Stego, Paranoid; в исполняемые коды: Smail; в текстовые файлы и e-mail: SNOW, Steganos, Spammimic и т.д.

Достаточно креативный способ воровства конфиденциальной информации долгое время оставался недоступным для противодействия инсайдерам. Появление программных средств сигнатурного и корреляционного анализов сканирования пересылаемых контейнеров практически перекрыло возможности сокрытия данных в мультимедийных файлах.

Литература

1. Алиев, А.Т. О применении стеганографического метода LSB к графическим файлам с большими областями монотонной заливки [Текст] / А.Т. Алиев // Вестник ДГТУ. – Ростов-на-Дону, 2004. – Т. 4, № 4 (22). – С. 454-460.

Д.В. Кириллов

НЕКОТОРЫЕ АСПЕКТЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ КОНТРОЛЕМ ДОСТУПА НА ОСНОВЕ РОЛЕЙ

(Самарский государственный университет)

Для достижения цели автоматизации управления контролем доступа на основе ролей в автоматизированных системах управления предприятием (АСУП) необходимо решить задачу замыкания компонентов и отношений подсистемы реализующей политику безопасности (ПБ) и объектов и отношений уровня бизнес-логики системы (БЛ), содержащей достаточно большой объем данных о субъектах необходимых для принятия решений о назначений или отзыве полномочий, либо для выполнения других операций [1].

В простейшем случае, когда в организации используется только одна система, и управление доступом реализуется в ней же, задача с формальной точки зрения является тривиальной - необходимо обогатить систему недостающими компонентами и отношениями [2]. Простая модель данных характерная для систем, использующих ролевую политику безопасности представлена на рис. 1.

Данная модель содержит минимальный набор идентифицирующих пользователя атрибутов и связей назначенных пользователю ролей. С другой стороны, на диаграмме представлен также минимальный набор идентифицирующих сотрудника атрибутов и связей с должностями, который сотрудник занимает в организации. Модель данных демонстрирует тот факт, что в обычной ситуации для автоматизированной системы, использующей контроль доступа на основе ролей для разграничения доступа в системе, формальная связь между компонентами подсистемы безопасности (в данном случае пользователи, роли и связи между ними) и соответствующими им объектам уровня бизнес-логики, отождествленными с субъектами и объектам реальной организации не существует. То есть, для выполнения операций связанных с изменением состояний объектов уровня бизнес-логики для отображения этих изменений на компоненты уровня подсистемы безопасности используются неформализованные механизмы, реализуемые непосредственно человеком, наделенным административными полномочиями на управление подсистемой безопасности.