обработки вычисляются коэффициенты $C_{m,n}$. Оценка частоты f производится по параметру m, оценка длительность сигнала $\widehat{T}$ определяется как разность $\Delta n = n_2 - n_1$, где n_1, n_2 начало и конец i-го луча. Оценка задержки $\Delta \widehat{t}$ определяется параметром n. Точность оценки зависит от λ_{opt}, которое является оптимальным для каждого из параметров.

Литература

1. B. Porat, B. Friedlander, Detection of transient signals by the Gabor representation IEEE Trans. Acoust., Speech, signal processing, Vol. 37, No. 2. February 1989.

СТАТИСТИЧЕСКИЙ АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

С.Б. САЛОМАТИН

Стеганографические методы защиты объектов используют в качестве скрывающих спектральные и корреляционные широкополосные преобразования данных. При этом возникает задача оценка стойкости стегосистем к обнаружению факта передачи скрываемых сообщений [1].

Для анализа стойкости стеганографических систем удобно использовать статистические методы распознавания образов.

Модель стеганографического процесса. Стегосообщение y представляется в виде аддитивной суммы стегошума n и скрываемых данных x. Стегошум характеризуется вероятностной функцией:

$$v[n] = p(y - x = n),$$

гистограмма стегосообщения может быть вычислена через свертку гистограммы скрываемых данных и вероятностной функции стегошума.

В качестве характеристических функций используются дискретные преобразования Фурье от соответствующих гистограмм и вероятностных функций.

Схема обнаружения. В условиях априори известного метода стеганографических преобразований анализатор строится на основе многомерного Байесовского классификатора, использующего линейную разделяющую функцию.

Дискриминантная функция задается в виде [2]

$$S_{ll'}(\vec{k}) = -\frac{1}{2}\vec{k}^T \Sigma^{-1}\vec{k} - \frac{1}{2}\vec{\mu}^T \Sigma^{-1}\vec{\mu} + (\Sigma^{-1}\vec{\mu})^T \vec{k} - \frac{1}{2} ln|\Sigma|,$$

где Σ^{-1}-общая ковариационная матрица классов l и l', $\vec{\mu}$ — вектор средних значений.

В условиях априорной неопределенности типа стегопреобразования, но в рамках анализа классов с многомерным нормальным распределением, которые отличаются лишь средними значениями, критерий оценки адекватности набора признаков использует понятие расстояния Махаланобиса:

$$\varphi = (\vec{\mu}_l - \vec{\mu}_{l'})^T \Sigma^{-1} (\vec{\mu}_l - \vec{\mu}_{l'}).$$

Для снижения вычислительной сложности алгоритма используется метод выбора "лучшего признака" [3].

Литература

1. Грибунин, Оков И.Н., Туринцев И.В. Цифровая стеганография. М., 2002.
2. Harmsen J.J, Pearlman W.A. Stegaanalysis of additive noise modelable information hiding. Center for ImageProcessing Research, Troy, NY.
3. Верхаген К.,Дейн Р., Грун Ф., Йостен Й., Вербек П. Распознование образов: состояние и перспективы. М., 1985.

О ФОРМИРОВАНИИ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

О.А. КАЧАН, И.В. МИТЯНОВ, В.К. ФИСЕНКО

В общем случае модель нарушителя определяется совокупностью признаков, характеризующих квалификацию C, мотивацию M и ресурсы R нарушителя, представленные в виде множеств (подмножеств).

Элементы множеств C, M и R также могут задаваться в виде подмножеств. Это позволяет сформировать вложенную систему подмножеств признаков и элементов. Достаточность глубины детализации и полноты охвата оценивается экспертным путем.

Множества C, M и R характеризуют различные аспекты процесса НСД. При этом:

C={c_1, c_2, c_3}, где c_1 — способности нарушителя, определяемые уровнем его подготовки; c_2 — степень информированности нарушителя о характеристиках объекта информатизации (ОИ); c_3 — статус нарушителя;

M={m_1, m_2, m_3, m_4}, где m_1 — ошибочные действия; m_2 — любознательность; m_3 — попытка взлома; m_4 — корыстные цели;

$R=\{r_1, r_2, r_3\}$, где r_1 — вариант реализации средств; r_2 — расположение средств; r_3 — функции средств.

Предлагается в одном из подмножеств отразить социально-психологические качества потенциального нарушителя: замкнутость или общительность, воля или нерешительность, авантюризм, прагматизм, карьеризм и др. Это позволит создать гипотетическую модель наиболее опасного нарушителя и выделить так называемую "группу риска".

Синтез моделей проводится с использованием аппарата логики высказываний.

Расширение номенклатуры классифицирующих признаков позволит детализировать модель нарушителя и получить более достоверные оценки вероятного направления, характера и риска возможного несанкционированного доступа.

ЗАДАЧА ИДЕНТИФИКАЦИИ АТАК В СРЕДСТВАХ АУДИТА БЕЗОПАСНОСТИ

Е.П. МАКСИМОВИЧ

В соответствии со стандартом СТБ 34.101.2-2001 (ИСО/МЭК 15408-2) средства аудита безопасности должны обнаруживать возможные нарушения безопасности на основе идентификации определенных правил, знаковых событий; известных сценариев проникновения; несоответствия текущей деятельности пользователя ранее применяемому профилю использования системы. Правила, знаковые события и профили стандартного поведения представляют собой некоторые шаблоны или экспертные правила, каждому из которых соответствуют нечеткое слабо формализуемое множество возможных реализаций. В таких условиях возникает нетривиальная задача идентификации наблюдаемых действий, выраженных в некоторых низкоуровневых сигналах относительно заданных эталонных описаний.

Один из возможных подходов к решению указанной задачи идентификации состоит в использовании распознавания с обучением.

Каждая атака представляется выборкой возможных реализаций, которые образуют один или несколько кластеров близких (в смысле заданной функции) ситуаций. Идентификация ситуации сводится к оценке ее возможной принадлежности одному из полученных кластеров. Если расстояние ситуации до ближайшего кластера меньше заданного порогового значения, то принимается решение о реализации соответствующей атаки. Для определения значения порога можно использовать контрольную выборку. В качестве критерия близости предлагается использовать правило типа "ближайшего соседа" либо близость к эталону кластера, заданному, например, в виде дизъюнктивной нормальной формы.

РАНДОМИЗАЦИОННЫЕ ПРЕОБРАЗОВАНИЯ С АЛФАВИТОМ БОЛЬШОЙ МОЩНОСТИ

В.В. ЗАХАРОВ

Известно, что одним из приемов, разрушающих частотные свойства исходного текста является рандомизация. В процессе рандомизации буквам алфавита исходного текста случайным образом ставятся в соответствие буквы алфавита рандомизированного текста. При этом если мощность алфавита рандомизатора незначительно превышает мощность алфавита исходного текста, то такой шифр может быть легко вскрыт.

Доклад посвящен синтезу и анализу рандомизационных преобразований с большой мощностью алфавита рандомизатора.

Показано, что такие рандомизаторы при мощности алфавита рандомизации $L \to \infty$ обеспечивают бесконечную энтропию криптограммы и, соответственно, полную статистическую независимость криптограммы от исходного текста. При этом возможно получение различной степени приближения к полной статистической независимости исходного и зашифрованного текстов путем использования рандомизатора с ограниченным, достаточно большим полем рандомизации.

Дана численная оценка мощности алфавита рандомизатора, при которой достигается практическая статистическая независимость исходного текста и криптограммы.

Приведена методика синтеза рандомизаторов с большой мощностью алфавита рандомизации на основе кусочно-линейных разрывных функций. Показаны возможные подходы к анализу стойкости таких рандомизаторов.

МЕТОД МНОГОКАНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ДАННЫХ И ЕГО ПРИМЕНЕНИЕ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Ю.В. ВИЛАНСКИЙ

В 1999 году в заявке PCT /BY99/ 00005 был предложен метод преобразования данных, в котором исходный текст преобразуется в два или более выходных потока. Особенностью метода является циклический характер получения составляющих выходных потоков, что позволяет распределять их совокупности, каналам передачи или использовать как дополнительные степени свободы в различных системах. При этом, по крайней мере, один из выходных потоков можно сделать достаточно малым.