Amplification Attacks (TA14-017A), NTP Amplification Attacks Using (TA14-013A / CVE-2013-5211), Malware Targeting Point of Sale Systems (TA14-002A).

6. National Vulnerability Database NIST по состоянию на апрель 2014 г. включает 62020 актуальных уязвимостей.

Таким образом, своевременная оценка уязвимостей позволяет повысить эффективность реагирования на инциденты информационной безопасности, а также обеспечить гарантированную защиту объектов различных категорий.

ОЦЕНКА КРИПТОСТОЙКОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ

Н.В. МИНОВ

Криптографическая стойкость — свойство криптографического шифра противостоять криптоанализу, то есть анализу, направленному на изучение шифра с целью его дешифрования. Криптостойкость шифра есть его важнейшая характеристика, которая отражает меру устойчивости системы к атакам. Система называется стойкой, если злоумышленник не может взламывать ее слишком часто или слишком быстро. Для измерения стойкости алгоритма необходимо оценивать вероятность взлома и объем вычислительных задач [1].

Стойкость абсолютно стойких алгоритмов не зависит от того, какими вычислительными возможностями обладает криптоаналитик. Практическое применение систем, удовлетворяющих требованиям абсолютной стойкости, ограничено соображениями стоимости.

Определены следующие требования к такого рода шифрам: каждый ключ используется только один раз, все ключи равновероятны, длина ключа равна или больше длинны сообщения [2].

В основном в криптографических алгоритмах применяются вычислительно стойкие системы. Стойкость этих систем зависит от того, какими вычислительными возможностями обладает криптоаналитик. Практическая стойкость таких систем оценивается последовательно с двух позиций: вычислительная сложность полного перебора, известные уязвимости системы и их влияние на вычислительную сложность.

Литература

1. *Венбо М.* Современная криптография. Теория и практика. М., 2005.

2. *Шеннон К.* Теория связи в секретных системах. [Электронный ресурс]. — Режим доступа: http://www.enlight.ru/crypto/articles/shannon. — Дата доступа: 23.04.2014.

ЗАЩИТА ЧЕЛОВЕКА ОТ ВЛИЯНИЯ АКУСТИЧЕСКИХ ВОЛН РАЗЛИЧНЫХ ДИАПАЗОНОВ

В.В. МИРОНЧИК

В современном мире человек постоянно воспринимает информацию по акустическому каналу. Воздействовать на психоэмоциональное состояние человека можно с помощью звуковых волн различных частот.

При воздействии на человека частотами, относящимися к инфразвуку (область частот ниже 20 Гц) и ультразвуку (частоты свыше 20 кГц), человеческое ухо не воспринимает какую-либо информацию, но вызываются резонансные явления всего тела человека. Данные резонансные явления в зависимости от их интенсивности и продолжительности могут вызывать различные нарушения в организме человека. Для защиты от данного типа воздействий на различных производствах необходимо использовать звукопоглощающие камеры, не передающие вибрации, расположенные на определенном удалении от источника данных частот.

В слышимом диапазоне частот, который варьируется для каждого человека в зависимости от его личных физиологических данных, акустическое воздействие на психоэмоциональное состояние осуществляется путем речевого манипулирования. Внедрение в различные аудиофайлы дополнительной информации может быть осуществлено различными способами: внедрение путем использования разности времени между записями в файл событиями, кодирование информации двоичным кодом с последующим использованием последовательности в аудиозаписи и др. Данные способы внедрения информации позволяют передавать скрытые сообщения с помощью аудиофайлов, не оказывая влияния на качество исходной аудиозаписи, однако воздействуя на подсознание человека. Таким образом, важной проблемой является выявление скрытой информации в аудиофайлах для обеспечения защиты жизнедеятельности людей.

АЛГЕБРАИЧЕСКАЯ КОНСТРУКЦИЯ КОДА НА ОСНОВЕ ФУНКЦИИ МЁБИУСА

А.И. МИТЮХИН, Р.П. ГРИШЕЛЬ

В ряде специальных коммуникационных приложениях желательным требованием является не только контроль ошибок в каналах с шумами посредством применения помехоустойчивого кодирования информации, но и обеспечение определенной степени защиты информации от подслушивания. В таком случае необходимо иметь код с заданным минимальным расстоянием и наибольшей мощностью кодовых слов. Кроме того, для увеличения структурной скрытности сигналов необходимо достаточно часто изменять форму сигналов, чтобы усложнить распознавание формы сигнала, способа его кодирования и модуляции, т.е. увеличивать время на осуществление отождествления обнаруженного сигнала с одним из множества априорно известных сигналов. Названным требованиям могут удовлетворять нелинейные коды с компонентами из поля Галуа $GF(p)$, где p — характеристика поля. В работе предлагается алгебраическая конструкция нелинейного кода, получаемая с использованием функции Мёбиуса $\mu(m)$, $m \in \mathbf{Z}^+$ [1] над полем с множеством $p \in \{1,-1\}$. Значение параметра n определяется числом r различных простых чисел, образующих произведение m. Например, для значений m=30, r=3 и m=210, r=4 формируются уравновешенные бинарные коды длиной n=8 и n=14, соответственно с кодовым расстоянием d=4 и d=7. Структура (форма) кода зависит от простых делителей, на которые разлагается число m. Решение задачи разложения сравнительно большого целого составного числа на простые множители вычислительно трудоемко. Скрытность самой информации достигается с ростом числа m.

Литература

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки: пер. с англ. М., 1979.

ОСНОВНЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ЛОКАЛЬНЫХ СЕТЕЙ

Н.В. НАСОНОВА

На основе анализа рекомендаций основных международных стандартов в области информационной безопасности (ISO 2700x, NIST 800-53, BSI и др.) можно выделить несколько областей, наиболее важных для обеспечения защиты локальной сети организации от воздействия компьютерных атак, и составляющих основой базис безопасности.

Во-первых, это инвентаризация и контроль применения авторизованного оборудования, программного обеспечения, управление их конфигурацией с применением эталонных защищенных образов систем, а также контроль и защита беспроводных