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

устройств. Внимание также уделяется контролю сетевых протоколов, портов и служб для ограничения возможностей подключения к сети организации.

Во-вторых, применение активных средств управления защитой сети, таких как непрерывный анализ и устранение уязвимостей, организация защиты от вредоносного кода, обеспечение безопасности прикладного ПО и возможности восстановления данных, а также ведение, мониторинг и анализ журналов регистрации событий безопасности.

В-третьих, все стандарты большое значение придают квалификация персонала — как отдела ИБ, так и остальных сотрудников, поскольку их осведомленность в области ИБ играет большую роль в защищенности сети. Для этого предлагается периодически проводить обучение, повышение осведомленности, а затем и оценку навыков по безопасности и проведение тренингов по ИБ. Эффективность работы персонала отдела ИБ оценивается в том числе и по возможности реагирования на инциденты информационной безопасности и результатам тестирования на проникновение, упражнений и учений.

В-четвертых, важным аспектом ИБ организации является безопасно построенная сеть, что предполагает определенную архитектуру сети, защиту ее периметра и контроль входящих и исходящих потоков данных, предотвращение утечки данных.

В-пятых, для защиты информации в локальной сети необходим мониторинг и контроль учетных записей — как привилегированных аккаунтов администраторов, так и обычных пользователей. использования административных привилегий, контроль и управление их доступом.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ПЛАТФОРМ

А.Р. ОКОЛОВ, В.В. ХОДЬКО, А.В. ДРОЗД

Облачные платформы — это модель предоставления вычислительных ресурсов по требованию, охватывающая всё — от конкретных приложений до центров обработки данных, через Интернет. Такой подход к организации вычислений дает небывалые возможности клиентам, независимо от мощности их компьютеров и при этом обеспечивает доступ к облаку миллионам пользователей в каждый момент. Однако, при такой заманчивости использования облачных сервисов, пользователи предъявляют к ним и высокие требования, связанные с аутентификацией, сохранностью данных и их защищенностью.

Аутентификация. Самым распространенным способом аутентификации является защита паролем. Однако некоторые провайдеры, для обеспечения более высокой надежности, прибегают к помощи таких средств, как сертификаты и токены. Желательно, что бы провайдеры имели возможность работы с такими стандартами как LDAP и SAML. Это важно для обеспечения прозрачного взаимодействия провайдера с системой идентификации пользователей клиента при авторизации и определении выдаваемых пользователю полномочий.

Сохранность данных. Лучший способ защиты расположенных в хранилище данных — использование шифрования. С целью предотвращения случаев неправомерного доступа, провайдер должен шифровать хранящуюся на своих серверах информацию клиента, безвозвратно удалять данные, когда они больше не нужны и не потребуются в будущем.

Защита данных при передаче. Передаваемые данные должны быть зашифрованы и доступны пользователю только после аутентификации. Это является гарантией того, что эти данные не сможет изменить или прочитать ни одно лицо, даже если оно получит к ним доступ посредством ненадежных узлов сети. Для этих целей созданы и эффективно используются надежные протоколы и алгоритмы, такие как TLS, IPsec и AES.