Рассматривается многопользовательский канал с подслушиванием (МКП). Используется два кодера с когнитивной связью, в том смысле, что одному кодеру априори известно некоторое сообщение другого кодера.

Предполагается, что в МКП передаются с разными скоростями два независимых сообщения.

Кодирование сообщений осуществляется двумя пользователями с использованием независимых случайных переменных с произвольной энтропией. Один из пользователей работает в режиме когнитивного кодирования и кодирует два сообщения. Второй пользователь кодирует только одно из двух сообщений.

Декодеры легитимного и подслушивающего приемников работают в разных условиях приема.

Когнитивная модель передачи информации создает для подслушивающего узла сети режим приема на фоне помехи, что снижает эффективность подслушивания и обеспечивает в топологии сети области с надежной связью.

Метод позволяет создать защищенный регион сети, в котором скорости передачи, удовлетворяют требуемым неравенствам.

КОДОВАЯ ЗАЩИТА В СЕТЕВЫХ СТРУКТУРАХ С ОШИБКАМИ И ПЕРЕХВАТОМ ИНФОРМАЦИИ

Т.А. АНДРИЯНОВА, С.Б. САЛОМАТИН

В сетевых структурах, использующих элементы с разным уровнем защиты, возможен перехват информации скрытыми агентами, а также возникновение разного рода ошибок в процессе передачи информации по каналам связи. Информация в таких сетевых объектах может быть защищена путем внесение кодовой избыточности и разнесение путей передачи информации.

Одними из механизмов сетевого кодирования являются коды, которые представляются в виде упорядоченных пар подпространств расширенного конечного поля.

Модель направленной сети связи имеет вид графа $G=(V, E)$, где V — множество узлов сети, а E — множество ребер — коммуникационных линий. Предполагается, что порядок E ассоциирован с частичным порядком G. Возможно мультиплексирование ребер между парами узлов. Через каждое ребро графа может быть передан один символ поля. Для сети G линейный код сетевого кодирования определяется как множество локально кодированных ядер вейвлет-функций.

Источник информации имеет M узлов сети, обеспеченных кодовыми фильтрами избыточного кода A. Доверенные узлы используют фильтрами избыточного кода B.

За один сеанс связи узел-получатель получает множество пакетов, прошедшие через узлы сети с кодированием фильтровой системой. Процесс декодирования основан на возможности восстановления информации с помощью вейвлет-преобразования в конечных полях.

Эффективность кодирования оценивается по скорости, с которой информация может быть надежно и безопасно доставлена требуемым узлам сети.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЛАТЕЖЕЙ В СИСТЕМАХ ЭЛЕКТРОННОЙ КОММЕРЦИИ

О.Б. ЗЕЛЬМАНСКИЙ, С.М.М. ГОНДАГ, Ш.М.Г. МОЗДУРАНИ

Современные информационные системы активно внедряются в банковской сфере, что позволяет банкам предоставить клиентам широкий спектр услуг, в том числе обеспечить возможность проведения удаленных транзакций. Несомненные удобства таких взаимодействий, с одной стороны, порождают проблему аутентификации и авторизации

клиента, обеспечения банковской тайны и защищенного информационного обмена, — с другой. Поэтому проблема обеспечения безопасности в электронных платежных системах является весьма актуальной.

Наиболее существенна такая проблема в системах электронной коммерции B2C типа, где покупатель или плательщик (физическое лицо) и продавец или получатель денежных средств (юридическое лицо) лично не знают друг друга, сделки, как правило, разовые, что обуславливает высокую степень недоверия. В настоящее время для обеспечения безопасности подобных платежей используются следующие подходы: взаимная аутентификация участников (покупатель, продавец, банк-эквайер, банк-эмитент) системы электронной коммерции и их оборудования, обеспечение конфиденциальности и целостности передаваемых сведений в такой системе, что реализуется применением широко спектра соответствующих средств защиты. Существенной проблемой на сегодняшний день является то, что использование одного и того же персонального компьютера покупателем, как для проведения платежа, так и для получения информации в сети Интернет, не связанной с оплатой товаров или услуг, приводит, как правило, к внедрению на персональный компьютер вредоносных программ и в конечном итоге потерям финансовым — со стороны покупателя и репутации — со стороны продавца. Таким образом, для обеспечения безопасности платежей в системах электронной коммерции B2C типа, наряду с используемыми средствами защиты платежа, обязательным является выполнение банковских транзакций с выделенного персонального компьютера, оснащенного необходимым программным обеспечением, который должен использоваться исключительно для платежей.

МАЛОГАБАРИТНАЯ УСТАНОВКА ДЛЯ ИЗМЕРЕНИЯ ЗВУКОИЗОЛЯЦИИ

Д.Э. ОКОДЖИ, С.Н. ПЕТРОВ, А.М. ПРУДНИК

Разработана стендовая установка для измерения звукоизоляции плоских образцов, которая позволяет за малое время провести оценку собственной звукоизоляции образца и произвести отбор образцов с наилучшими показателями звукоизоляции из некоторого числа исследованных.

Для определения величины звукоизоляции с высокой точностью необходимо выявить отдельные элементы установки, вносящие погрешности в процесс измерений и скомпенсировать эти погрешности. Такими элементами является приемо-передающий тракт установки, корпус и способ фиксации образца. Источник звука и усилитель не должен иметь существенных завалов формы АЧХ, это же касается и микрофонного предусилителя. Корпус установки, в силу своих геометрических размеров, обладает рядом собственных резонансных частот. Фиксация образца между фланцами установки осуществляется с помощью червячной передачи. Для обеспечения одинаковых условий измерений прижимная сила, прикладываемая к образцу должна быть постоянной для каждого проведенного измерения.

МЕТОД МОДИФИЦИРОВАННОГО СИНГУЛЯРНОГО СПЕКТРАЛЬНОГО АНАЛИЗА ДЛЯ ЗАШИФРОВАННОЙ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА ИНФОРМАЦИИ

А.В. СИДОРЕНКО, И.В. ШАКИНКО

Широкое распространение телекоммуникационных систем в повседневной жизни приводит к появлению задач для обеспечения защиты информации различного характера. Использование динамического хаоса для хаотических систем защиты информации обусловлено способностью хаотических отображений реализовать скрытость передачи зашифрованной информации.