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.

В работе проводится определение показателей выходных последовательностей зашифрованной на основе динамического хаоса информации. Для этого разработан метод модифицированного сингулярного спектрального анализа с применением непрерывного вейвлет-преобразования. Использование вейвлет-преобразования позволяет не только выявить детерминированную компоненту анализируемой последовательности, но и определить частоту, на которой проявляется детерминизм.

Проводится сравнительный анализ результатов, полученных при использовании для последовательностей сингулярного спектрального анализа и разработанного метода. Показано, что применение модифицированного метода позволяет выявить более чем на 20% различия в показателях уровня вклада вторых главных компонент входных и выходных (зашифрованных) последовательностях.

Определена зависимость уровня вклада главных компонент от числа итераций для информации, зашифрованной на основе динамического хаоса с применением режима CBC, в отличие от режима OFB, где подобная зависимость отсутствует.

Литература

1. *Сидоренко А.В., Мулярчик К.С. Шакинко И.В.* Вестник БГУ. Сер. 1 Физика, математика, информатика. 2012. № 4. С. 44–50.