также четырехугольники гласных при различных соотношениях сигнал/шум. На рис. 2 показано изменение зависимости формант F_1 и F_2 на примере фонем, произнесенных женским голосом.

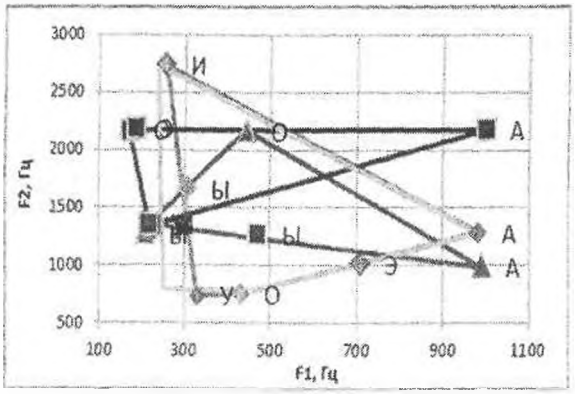

Рис. 2. Изменение расположения фонем при воздействии шумом

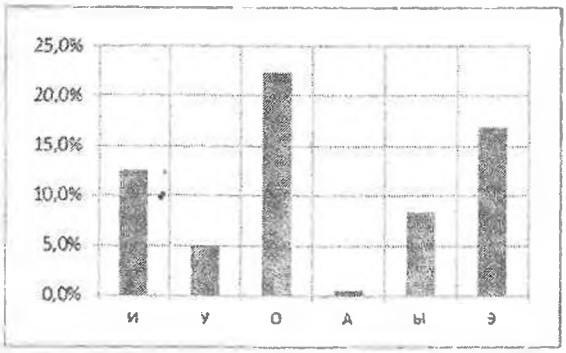

Рис. 3. Помехоустойчивость гласных фонем

По результатам исследований можно утверждать, что форманта F_1 фонемы *а* наиболее устойчива к шумам. А пока соотношение между расположением звуков остается, мы распознаем голос. Таким образом, по изменению соотношений между формантами и смещению вершин относительно друг от друга можно судить о величине искажений речевого сигнала, а по смещению форманты F_1 о разборчивости конкретной фонемы. Далее на рисунке 3 показана устойчивость определения формант различных фонем к помехам.

В результате, проведенных исследований предлагается комбинированное использование методов оценки первичных признаков речевого сигнала: метода АФК для частоты ОТ и кепстрального – для выделения основных формант (достаточно первых двух). Такой подход позволит достоверно определить наличие речи в шумах и провести оценку величины искажения сигнала.

В.К. ЖЕЛЕЗНЯК, А.В. БАРКОВ

МЕТОД МАСКИРОВАНИЯ СТАТИЧЕСКИХ И ДИНАМИЧЕСКИХ RGB-ВИДЕОКАДРОВ СИНХРОННЫМ И АДАПТИВНЫМ ШУМОВЫМ RGB-ВИДЕОКАДРОМ

Предложен метод формирования маскирующей помехи для защиты видеосигнала от утечки по техническим каналам. Видеосигнал обладает рядом характерных особенностей, которые надо учитывать при решении задачи защиты от утечки по техническим каналам. Целью является формирование маскирующей помехи видеосигнала. Задачей является разработать и предложить метод формирования маскирующей помехи с учетом особенностей видеосигнала. Исследования показали возможность синхронного накопления зашумленного статического видеокадра, которое значительно улучшает отношение сигнал/шум (ОСШ). В этой связи обоснована необходимость создания синхронной адаптивной помехи для маскирования статических видеокадров. Предложен способ формирования маскирующих видеокадров с учетом того, что видеокадры на экране могут быть статическими (неподвижными) и динамическими (подвижными), содержать крупномасштабные и мелкодетальные элементы.

Суть метода маскирования статического видеокадра состоит в том, что синхронным накоплением и запоминанием создают статический видеошумовой кадр.

В предложенном методе маскирования реализуется синхронность видеосигнала и маскирующего видеошума.

Метод маскирования статических видеокадров реализован в синхронных и адаптивных шумовых RGB-видеокадрах. Время накопления зашумленного видеокадра устанавливается выигрышем по отношению количества накоплен-

ных статических кадров к накопленным шумовым кадрам равным $n/\sqrt{n}=\sqrt{n}$, таким образом, ОСШ улучшается пропорционально $\sqrt{n}$, где n – количество накоплений, что соответсвует данным исследования в University of Cambridge Computer Laboratory автором Dr Markus Kuhn «Security Limits for Compromising Emanations». Статическое накопление исключает улучшение ОСШ по сравнению с динамическим пропорционально $\sqrt{n}\cdot\sqrt{k}$, где n – число видеокадров, k - количеством смен шумового видеокадра.

Из анализа видеосигналов для контроля каналов утечки предложен тестовый видеокадр черно-белого (рис. 1) и цветного (рис. 2) RGB-изображения в виде шахматного поля, шахматные клетки которого включают горизонтальные и вертикальные линии различной толщины, что позволяет определить тонкую структуру видеокадра, включающую крупномасштабные и мелкодетальные элементы.

Проведены экспериментальные исследования синхронного накопления зашумленного динамическим шумом и статическим шумовым RGB-кадром видеосигнала. Исследовано маскирование цветного и черно-белого тестового изображения.

Рис. 1. Кадр тестового черно-белого изображения (шахматное поле с горизонтальным и вертикальным заполнением линиями)

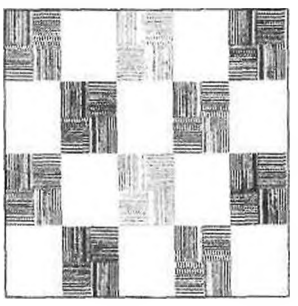

Рис. 2. Кадр тестового цветного изображения (шахматное поле с горизонтальным и вертикальным заполнением линиями)

Результаты эксперимента по синхронному накоплению видеосигнала длительностью 30 секунд динамически зашумленного тестового цветного изображения (рис. 3) показывают восстановление RGB-видеокадра, где различимы крупномасштабные элементы в виде клеток и мелкодетальные линии внутри клеток поля (рис. 4), а так же цветовые компоненты видеокадра. Результатом синхронного накопления статических видеокадров синхронно зашумленных адаптивным шумовым RGB-видеокадром (рис. 5) является невозможность восстановления изображения статических видеокадров.

Рис. 3. Зашумленный кадр цветного тестового изображения (длительность видеосигнала 30 секунд)

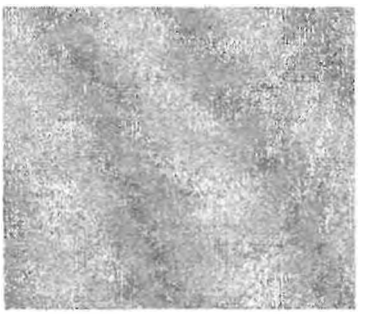

Рис. 4. Накопленный кадр цветного тестового изображения, зашумленного динамическим шумом

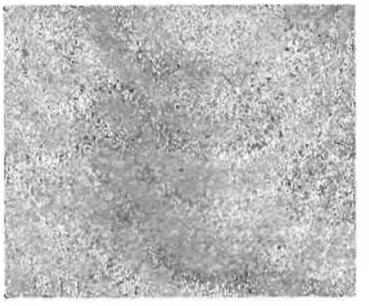

Рис. 5. Накопленный кадр цветного тестового изображения, зашумленного статическим адаптивным шумовым RGB-видеокадром

добные шифропоследовательности, устойчивы к вскрытию, и криптоаналитик не может предсказать ни следующий, ни предыдущий бит последовательности.

Криптографический анализ кодовых структур кривой Эрмита в поле $GF(16)$ выполнен с использованием спектральных преобразований. Кодированные вектора имеют высокую степень устойчивости к линейному криптоанализу, но требуют добалансировки для возможности противодействия прямым статистическим атакам. Высокая степень линейной сложности и близость к криптографическим стандартам *BBS* и *AES* обеспечивает устойчивость к вскрытию и приемлемость подобных структур для систем защиты информации.

ЛИТЕРАТУРА

1. Саломатин, С.Б. Поточные криптосистемы : учеб. пособие по курсам «Кодирование и защита информации», «Основы криптологии» / С. Б. Саломатин. – Минск: БГУИР, 2006. – 76 с.

2. Patrick J. Morandi. Lecture Notes for Mathematics 601. Error Correcting Codes and Algebraic Curves [Электронный ресурс] – Режим доступа: LectureNotes.pdf.

Д.С. РЯБЕНКО, В.К. ЖЕЛЕЗНЯК

ПРИМЕНЕНИЕ ХАОТИЧЕСКИХ ИМПУЛЬСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ МАСКИРОВАНИЯ АНАЛОГОВЫХ И ЦИФРОВЫХ РЕЧЕВЫХ СИГНАЛОВ

Высокая точность передачи цифровой информации определила приоритетность цели ее защиты. При взаимном преобразовании аналоговых и цифровых сигналов возникли новые каналы утечки информации, усложнились способы их защиты и разработки новых методов и средств оценки их защищенности [1]. Одним из способов маскирования применяются помехи в виде хаотических импульсных последовательностей (далее – ХИП).

В общем виде помехи указанного вида можно представить как последовательность импульсов с заданной частотой заполнения, амплитуды и длительности которых, а также интервалы между соседними импульсами изменяются случайным образом [2].

Актуальным является повышение степени защиты речевых сигналов в аналоговой и цифровой форме, видеосигналов и сигналов звукового сопровождения, сигналов передачи данных путем расширения функциональных возможностей широкополосных маскирующих сигналов в виде ХИП по низкочастотным каналам утечки информации.

Для формирования ХИП предлагается устройство для получения сигнала маскирования каналов утечки информации, содержащее последовательно включенные источник шумового сигнала, фильтр нижних частот и усилитель, дополнительно включены последовательно соединенные блок формирования ХИП, сумматор, устройство масштабирования уровня совпадающих импульсных последовательностей и согласующий каскад, причем блок формирования ХИП содержит N формирователей ХИП положительного уровня и N формирователей ХИП отрицательного уровня, а также N-1 формирователей опорных уровней положительного уровня и N-1 формирователей опорных уровней отрицательного уровня, выход усилителя подключен на первые входы каждого из формирователей ХИП, второй вход двух формирователей ХИП первого уровня соединен с землей, второй вход каждого из остальных формирователей ХИП соединен с выходом предшествующего формирователя ХИП через последовательно включенный формирователь опорного уровня, выходы формирователей ХИП соединены со входами сумматора.

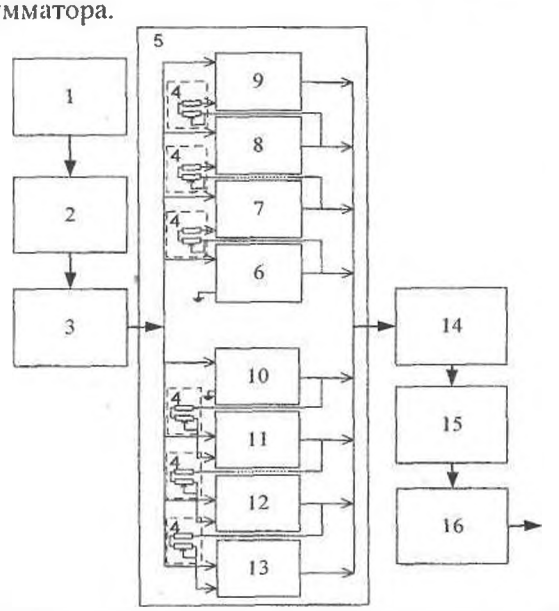

Рис.1. Схема устройства для получения сигнала маскирования каналов утечки информации