

Второй способ заключается в создании собственного класса сообщений операционной системы. Процессы могут генерировать системное сообщение при необходимости, и если другие процессы «подписываются» на него путем установки стандартного простого обработчика, они получают уведомления о его происшествии. Такие сообщения широко используются операционной системой для управления приложениями, сервисами, отображением окон, файловой системой и составляют ядро Windows.

Недостаток первого способа проявляется в том, что моменты нажатия пользователем клавиш носят случайный характер. Пользователь может отойти от компьютера на длительное время, в течение которого управляющее приложение должно постоянно проверять разделяемую область памяти на появление новой информации от фильтрующих функций всех запущенных приложений. Если учесть, что объем информации, поступающей от функций, составляет 5–6 байт, то создание и поддержание отображаемой (общей) области памяти становится особенно неэффективно с точки зрения операционной системы. К тому же программисту необходимо самостоятельно реализовывать механизм временной целостности потоков от всех приложений.

В данном случае выгоднее использовать способ сообщений. Фильтрующие функции всех приложений при нажатии пользователем клавиши генерируют сообщение, которое поступает управляющему приложению. Операционная система обеспечивает временную целостность таких сообщений (т. е. сообщение о событии, произошедшем позже второго, не сможет прийти раньше его). Объем информации, передаваемой сообщениями, составляет 8 байт (два двойных слова), что достаточно для передачи информации о нажатой клавише.

УДК 621.391.16; 534

В.К. Железняк, Д.С. Рябенко, И.Б. Бураченок

ЗАЩИЩЕННОСТЬ РЕЧЕВЫХ СИГНАЛОВ ВЗАИМОКОРРЕЛЯЦИОННОЙ ЧАСТОТНО-ВРЕМЕННОЙ ОБРАБОТКОЙ СЛОЖНОГО ИЗМЕРИТЕЛЬНОГО СИГНАЛА С БОЛЬШОЙ БАЗОЙ

Известные методы оценки защищенности речевых сигналов в каналах утечки информации (КУИ) реализуют точность, чувствительность и оперативность, определяемые длительностью сигнала, и представляют результаты оценки в виде разборчивости речи или отношения сигнал/шум (ОСШ) на выходе канала утечки (КУ) речевой информации. Установлено, что для

качественной оценки защищенности речевых сигналов в КУИ необходимо учитывать воздействующие факторы: неравномерность спектральной плотности речевого сигнала, предельную бинауральную чувствительность уха, затухание в типовых элементах ограждающих конструкций, спектральную плотность фонового акустического шума, реверберационные помехи и резонансные явления замкнутых пространств. Методы оценки защищенности речевого сигнала гармоническим измерительным сигналом (ИС), включенным в СТБ 34.101.29-2011, и широкополосным ЛЧМ ИС обладают рядом преимуществ, необходимых для получения высокой точности при допустимом времени обработки. Использование гармонического ИС на средних частотах в k -полосах равной разборчивости (ППР) допускает увеличение погрешности при оценке КУ речевой информации в широком (от 100 Гц до 10 кГц) диапазоне частот с явно выраженными неравномерностями АЧХ. Более высокая чувствительность получена при использовании метода широкополосного ЛЧМ-сигнала с предварительной обработкой Вигнера. Однако, при некоторых методических преимуществах перед методом гармонического ИС при оценке защищенности речевых сигналов в КУИ при неравномерности АЧХ, данный метод уступает по времени обработки. Поэтому с учетом последних достижений в использовании измерительных автоматизированных систем, обеспечивающих повышение точности и оперативности представления результатов обработки данных, возникла необходимость в разработке нового метода оценки и выбора оптимальных параметров ИС в ППР.

В предлагаемом методе в качестве измерительных используют сложные ИС с большой базой, имеющие преимущество перед методом гармонического ИС, равное величине базы B , в ППР с обоснованными оптимальными постоянными значениями длительности $T_c = 4$ с и девиацией частоты $\pm \Delta f_k$, перекрывающей каждую из k -полос равной разборчивости, и различными значениями базы. Предлагаемая методика оценки базируется на методах корреляционного анализа исходного сложного ИС с большой базой и сигнала на выходе КУ речевой информации и с учетом различий между помехой и полезным сигналом. Даже небольшое случайное запаздывание длительностью 10–200 мс, обусловленное прохождением ИС через среду распространения и задержками аппаратуры, значительно увеличивает погрешность оценки выходных параметров, поэтому применение для оценки защищенности функции взаимной корреляции (ВКФ) по времени $R_{1,2}(\tau)$ двух сигналов – не зашумленного входного ИС $s_1(t)$ и зашумленного в КУИ выходного ИС $s_2(t)$

$$R_{1,2}(\tau) = \int_{-\infty}^{\infty} s_1(t) s_2(t - \tau) dt, \quad (1)$$

где τ – сдвиг по времени между входным $s_1(t)$ и выходным $s_2(t)$ сигналами, позволило с помощью процесса корреляции подавить шумовую составляющую и повысило точность оптимальной оценки параметров сигнала при приеме на фоне шумов высокого уровня, исключив погрешности, связанные с запаздыванием сигнала в КУИ. Функция (1) оценивает степень сходства формы двух сигналов, а также их взаимное расположение по оси времени. В момент времени, когда выходной сигнал $s_2(t)$ наиболее подобен входному $s_1(t)$, корреляционная функция максимальна. При условии $s(t) = s_1(t) = s_2(t)$ выражение (1) является выражением автокорреляционной функции (АКФ) сигнала. АКФ можно рассматривать как частный случай ВКФ при одном и том же сигнале. Для оценки сдвига по времени τ между сигналами на входе $s_1(t)$ и выходе $s_2(t)$ формируют АКФ входного сигнала, определяют ее максимальное значение в точке $\tau = 0$ и находят максимальное значение ВКФ. В отличие от АКФ, ВКФ не является четной и не обладает симметрией относительно оси ординат. Сдвиг пика ВКФ точно равен времени задержки сигнала $s_2(t)$ относительно $s_1(t)$. Следовательно, случайное запаздывание можно определить с точностью до одного периода дискретизации T_0 как разность точек, соответствующих времени максимума ВКФ между измерительными сигналами на выходе и входе КУИ и максимума АКФ исходного сложного ИС с большой базой.

При прохождении сигнала через преграду могут иметь место и задержки по частоте, вызванные присутствием фоновых шумов. Экспоненциальное спадание спектральной плотности шума в область высоких частот приводит к сдвигу по частоте сигнала на выходе КУИ относительно исходного ИС, что снижает точность оценки, поэтому применение предварительного синхронного накопления спектральных составляющих сложного ИС на выходе КУИ до превышения над уровнем шума с использованием быстрого прямого и обратного преобразований Фурье (БПФ и ОБПФ), а также представление сложного ИС с большой базой в виде комплексной переменной частотно-временным преобразованием Гильберта позволили расширить возможности метода.

Если $s_1(t) \leftrightarrow F_1(\omega)$ и $s_2(t) \leftrightarrow F_2(\omega)$, то обработку сигналов в частотной области можно представить следующим образом:

$$R_{1,2}(\Omega) = \int_{-\infty}^{\infty} F_1(\omega) F_2^*(\omega - \Omega) d\omega, \quad (2)$$

где $R_{1,2}(\Omega)$ – ВКФ двух сигналов $s_1(t)$ и $s_2(t)$ по частоте; $F_1(\omega), F_2^*(\omega - \Omega)$ – соответственно спектры исходного и принятого ИС с учетом операции комплексного сопряжения (*); Ω – частотная переменная сдвига по

частоте между $F_1(\omega)$ и $F_2(\omega)$. При условии $F(\omega) = F_1(\omega) = F_2(\omega)$ спектральная АКФ является частным случаем спектральной ВКФ. Временная форма $s_1(t)$ сигнала и его частотное представление $F(\omega)$ позволяют проводить оценку одновременно по времени и по частоте, так как оба представления взаимосвязаны и модификация одного из них приводит к изменению другого, т. е. некоторый временной сдвиг эквивалентен частотному фазовому сдвигу: $s(t - \tau) \leftrightarrow F(f)e^{-2\pi i f \tau}$, а частотный сдвиг эквивалентен временному фазовому сдвигу: $F(f - \varphi) \leftrightarrow s(t)e^{+2\pi i f \tau}$. Отметим, что функция частотной корреляции имеет свойства, аналогичные свойствам функции временной корреляции: $|R_{1,2}(\Omega)| \leq |R_{1,2}(0)|$ и имеет максимум при $\Omega = 0$.

Исследования проводились при зашумлении исходного ИС сгенерированным генератором шумом, преобразованным в хаотическую импульсную последовательность (ХИП). Корреляция сложного ИС с большой базой и шума ХИП стремится к нулю. Временная и частотная огибающие АКФ сложного ИС с большой базой в третьей N_3 ПРП с частотой $f_0 = 640$ Гц и полной девиацией частоты $2\Delta f = 140$ Гц одновременно показаны на входе (рис. 1, а) и выходе (рис. 1, б) КУИ.

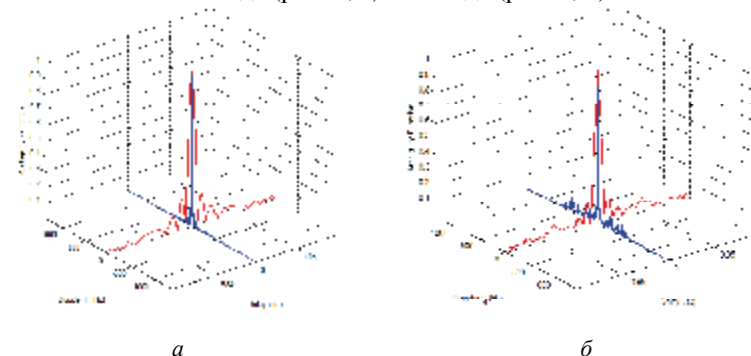


Рис. 1. Временные и частотные АКФ сложных ИС с большой базой: а – на входе КУ речевой информации; б – на выходе КУ речевой информации

Обобщенная ВКФ одновременно во временной и спектральной плоскостях строится по формуле

$$R_{1,2}(\tau, \Omega) = \int_0^{T_0} s_1^g(t) s_2^{g*}(t - \tau) e^{i\Omega t} dt, \quad (3)$$

где $s_1^g(t), s_2^{g*}(t - \tau)$ – комплексные огибающие исходного и принятого ИС с учетом операции комплексного сопряжения (*); i – мнимая единица.

Функция $R_{1,2}(\Omega)$ называется взаимной функцией неопределенности (ВФН) сигнала и позволяет одновременно оценить степень различия сигналов, отличающихся значениями запаздывания по времени τ и по частоте Ω .

ВФН сложного ИС с большой базой на входе и выходе КУ речевой информации (рис. 2) имеет главный пик, который определяет энергию сигнала. Ширина этого пика зависит от значения произведения

$$\mu T_c = 2\omega_c,$$

где $\omega_c = 4\pi\Delta f$ – девиация частоты, μ – скорость нарастания частоты.

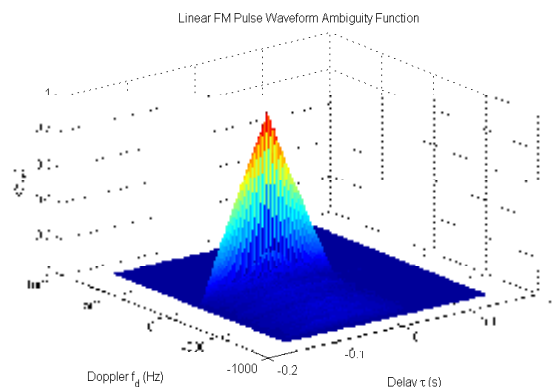


Рис. 2. ВФН между сложными ИС с большой базой на входе и выходе КУИ в третьей N_3 ПРР

Чем больше значение девиации частоты $\pm\Delta f_k$ сложного ИС с большой базой, тем уже главный максимум ВФН и, тем лучше разрешающая способность системы.

Таким образом, метод оценки защищенности речевого сигнала в КУИ взаимокорреляционной частотно-временной обработкой сложного ИС с большой базой в условиях воздействия шумов высокого уровня и других факторов позволил повысить численные значения основных параметров оценки защищенности речевых сигналов в КУИ и оперативность представления результатов. Взаимокорреляционная временная обработка сложного ИС с большой базой в 20 ПРР повысила чувствительность оценки на 27 дБ, а представление его в виде комплексной переменной и взаимокорреляционная частотно-временная обработка дополнительно улучшили ОСШ на выходе КУИ на 6 дБ и повысили разрешающую способность по частоте и времени и предельную чувствительность, обеспечив точность обработки до одного периода дискретизации T_d .

В заключение отметим, что разработанный метод является дальнейшим направлением развития и расширения функциональных возможностей программно-аппаратного комплекса «Филин-А», который в настоящее время используется для проведения контроля защищенности помещений от утечки речевой информации, включая генерацию протоколов, согласно нормативной базе Республики Беларусь.

УДК 004.054

Д.И. Жукова

**ПОРЯДОК ПОДТВЕРЖДЕНИЯ СООТВЕТСТВИЯ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ТРЕБОВАНИЯМ
ТЕХНИЧЕСКОГО РЕГЛАМЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ
«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ.
СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (ТР 2013/027/ВУ)**

С 1 января 2014 г. введен в действие технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ), утвержденный постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375.

Согласно положениям технического регламента ТР 2013/027/ВУ средства защиты информации (СЗИ) должны быть разработаны и изготовлены таким образом, чтобы, применяемые по назначению и выполняющие требования к эксплуатации и техническому обслуживанию, они обеспечивали: выполнение функций в соответствии с эксплуатационными документами; защиту от несанкционированного раскрытия и (или) модификации критических параметров; контроль целостности конфигурации; самотестирование; контроль доступа к функциям управления и настройкам; сохранение работоспособности при обработке некорректных данных.

Технический регламент распространяется на выпускаемые в обращение на рынке Республики Беларусь СЗИ независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов.

Все СЗИ, распространяемые на территории Республики Беларусь, должны быть подвергнуты процедуре подтверждения соответствия тре-