ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
"ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МЕЖОТРАСЛЕВОЙ ИНФОРМАЦИИ — ФЕДЕРАЛЬНЫЙ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР
ОБОРОННОЙ ПРОМЫШЛЕННОСТИ" (ФГУП "ВИМИ")

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

1 (92)

Москва
2011
Основан
в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн./ФГУП "ВИМИ", 2011. Вып. 1 (92). С. 1—72.

Редакторы: *Г. А. Никитин, Л. К. Андрианова*
Корректоры: *Н. С. Кузьмина, М. А. Николенко*
Компьютерная верстка *Н. В. Соколова*

Подписано в печать 22.02.2011.
Формат 60x84 1/8.
Бумага офсетная. Печать офсетная. Усл. печ. л. 8,4.
Уч.-изд. л. 9,4. Тираж 500 экз.
Заказ 1678. Цена договорная.
Отпечатано в ФГУП "ВИМИ".
125993, Москва.
E-mail: office@vimi.ru
http://infogoz.vimi.ru/main_izd.php
Индекс 79187.

Свидетельство о регистрации
ПИ № ФС77-35665 от 24.03.2009 г.

ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВОЗМОЖНОЙ УТЕЧКИ ИНФОРМАЦИИ

УДК 004.056

Оценка коэффициента шума технического канала утечки информации

В. В. Гришачёв, канд. физ.-мат. наук; *О. А. Косенко*
Институт информационных наук и технологий безопасности, РГГУ, Москва, Россия

Рассмотрены методы оценки коэффициента шума в техническом канале утечки информации на основе генерации шумов при преобразовании информационного сигнала в сигнал утечки. Формирование шума связывается с двумя процессами — искажением спектра и интерференцией от разных источников сигнала утечки.

Ключевые слова: защита объекта информатизации, технический канал утечки информации, коэффициент шума канала утечки.

Комплексная защита объекта информатизации является сложной и многогранной проблемой [1—4]. При построении системы защиты большое внимание уделяется выявлению потенциальных технических каналов утечки информации. Способность выявить канал утечки и оценить его опасность является важным показателем эффективности служб безопасности. Особую роль играет способность теоретической оценки защищенности объекта от утечек по многим каналам, различающихся между собой по физической природе носителя информации, среды канала утечки и другим характеристикам. Такой подход важен как при проектировании, строительстве специализированных помещений, зданий, так и при переоборудовании обычных помещений в выделенные и при их эксплуатации.

При создании защищенных объектов большое значение играет снижение эффективности естественных каналов утечек, связанных со штатными коммуникациями всех видов, конструкцией здания и его помещений [1—4]. Практически очень сложно оценить все потенциально возможные технические каналы утечек информации, что связано с быстрым развитием технических средств разведки, появлением новых принципов функционирования каналов утечки, в том числе и на новых физико-технических принципах. Например, развитие техники кабельной связи приводит к повсеместной замене электрических кабельных систем связи на оптические кабельные системы, которые имеют существенные отличия в физических принципах функционирования, что приводит к возможности создания новых каналов утечки, непохожих на ранее существовавшие. Попытки обеспечить защиту объекта в новых условиях неизбежно создадут бреши в системе безопасности, связанные с неоцененными угрозами от новых утечек.

Одним из элементов подобной системы оценок старых и новых угроз может выступать коэффициент эффективности канала утечки (CEL), который позволяет получить теоретическую оценку вероятности прохождения бита информации через канал утечки [5, 6]. При его вычислении необходимо знать отношение сигнала к шуму [7, 8] на выходе канала утечки $SNR_{out} = (P_S/P_N)_{out}$ или, что более просто, отношение сигнала к шуму на входе канала утечки $SNR_{in} = (P_S/P_N)_{in}$ и коэффициент шума канала утечки $CNL = (SNR_{in} / / SNR_{out})$. Здесь использовано обозначение для средней мощности сигнала P_S и шума P_N выходного и входного сигналов канала утечки.

Отношение SNR_{in} известно изначально по параметрам работающей аппаратуры, объектов носителей информации. Например, отношение сигнал/шум для разговора в спокойной обстановке может превышать 40 дБ при уровне шумов менее 30 дБ. Любое штатное оборудование имеет известные технические характеристики по излучениям и собственным шумам, а конструкции зданий — известные инженерно-технические параметры, что позволяет провести вычисление коэффициента шума всех элементов, составляющих канал утечки.

К основным элементам канала утечки относятся такие процессы, как преобразование входного информационного сигнала в сигнал утечки в среде канала связи, его распространение и регистрация техническими средствами разведки. При прохождении сигнала утечки на каждом этапе происходит изменение отношения сигнал/шум. Если на входе канала утечки имеем SNR_{in}, то после преобразования (модуляции) в среде канала связи — SNR_m, на выходе канала связи — SNR_t и на выходе ре-

гистрирующей аппаратуры — SNR_{out}. Введем коэффициенты шума: при преобразовании (модуляции) — $CNL_m = (SNR_{in}/SNR_m)$, канала передачи сигнала утечки — $CNL_t = (SNR_m / SNR_t)$, регистрирующей аппаратуры — $CNL_r = (SNR_m/SNR_{out})$, тогда общий коэффициент шума канала утечки, выраженный в дБ, $CNL = CNL_m + CNL_t + CNL_r$. В любом канале утечки можно выделить элемент с максимальным вкладом в зашумление сигнала утечки. Как правило, это зашумление при модуляции несущего поля информационным сигналом и формировании сигнала утечки или при его генерации.

Информационный сигнал испытывает несколько зашумлений при своем распространении через канал утечки — при преобразовании (модуляции), при распространении и при регистрации [5, 6], в которых отношение сигнал/шум уменьшается. Зашумление при регистрации определяется возможностями злоумышленника, поэтому можно считать $CNL_r \approx 0$, что соответствует наилучшим техническим средствам разведки. Зашумление сигнала при распространении определяется внешними условиями и действиями служб безопасности при проведении мероприятий по противодействию угрозам утечки информации, т. е. установленными средствами физической защиты. Для теоретической оценки можно предположить, что службы безопасности не контролируют данный канал утечки, т. е. инженерно-технические средства защиты не используются ($CNL_t \approx 0$). Это позволит считать проведенную оценку эффективности канала утечки максимально возможной в идеальных условиях для злоумышленника.

Последний элемент включает преобразование информационного сигнала в сигнал утечки в виде физического поля, переносящего информацию для технического канала утечки, оценка которого производится. Как правило, преобразование происходит в выделенном помещении, которое проверяется на наличие закладных устройств, поэтому можно считать, что таковые отсутствуют. Формирование сигнала утечки происходит вследствие воздействия информационного сигнала на штатные элементы систем связи, конструкции здания и другие элементы, которые должны обладать плохими преобразующими, модуляционными и генерирующими характеристиками. Все это приводит к тому, что $CNL_m > 1$, дБ. Таким образом, можно принять $CNL \approx CNL_m$, и расчет сводится к определению зашумления при преобразовании информационного сигнала в сигнал утечки.

Зашумление сигнала при преобразовании

Отличительной особенностью процесса преобразования информационного сигнала в сигнал утечки является малая эффективность, что связывается с использованием естественных, непредназначенных для преобразования элементов. К таким элементам могут относиться штатные и естественные волноводы, используемые для разведки. Например, использование трубопроводной системы отопления, воздуховодов для формирования канала утечки речевой информации [3] или волоконно-оптических коммуникаций для тех же целей [9—11]. При создании таких систем основной упор делается на решение соответствующих функциональных задач отопления, кондиционирования, связи и т. д., при этом полностью избежать нецелевого использования невозможно. Но их использование для разведки всегда сопровождается плохой эффективностью. Основной параметр, характеризующий эффективность преобразования, — коэффициент модуляции канала утечки CML, который определяет глубину модуляции проходящего физического поля (<<1) или генерации (=1) физического поля утечки. Можно ввести понятие коэффициента модуляции шумов CML_N и сигнала CML_S по мощности, а буквой m по амплитуде с соответствующим индексом, тогда отношение сигнал/шум после преобразования будет определяться выражением

$$SNR_m = \frac{CML_S}{CML_N} = \left(\frac{m_S}{m_N}\right)^2, \qquad (1)$$

что обусловлено связью коэффициентов $CNL_S \sim (m_S)^2$, $CNL_N \sim (m_N)^2$ со средней мощностью сигнала P_S, шума P_N.

Предлагаемое выражение позволяет рассчитать отношение сигнал/шум на практике путем разделения процессов модуляции от информационного сигнала и помехи. При зашумлении происходят процессы, которые можно характеризовать изменениями коэффициента модуляции. Неэффективность преобразования (зашумление), как правило, связывается с двумя процессами:

- искажениями сигнала утечки при модуляции или генерации, связанными с нетрадиционным использованием преобразующего элемента, оно характеризуется спектральной нелинейностью коэффициента модуляции;
- интерференционным наложением сигналов утечки от разных преобразующих элементов со случайным фазовым рассогласованием.

Все эти процессы вызывают понижение отношения сигнал/шум, которое характеризуется коэффициентом шума преобразования. Процедура определения CNL сводится к вычислению отношения сигнал/шум SNR_m после преобразования. Если зашумление сигнала связано сразу с двумя независимыми друг от друга процессами, то результирующее отношение

$$SNR_m = \frac{SNR_I \cdot SNR_D}{\sqrt{SNR_I^2 + SNR_D^2}}, \qquad (2)$$

где SNR_I — отношение сигнал/шум после интерференции сигнала и шума;

SNR_D — отношение сигнал/шум после искажений сигнала.

Выражение получается в результате сложения двух нормальных распределений независимых случайных величин, когда мощность результирующего шума определяется как среднеквадратичная величина складываемых шумов [12].

В случае зашумленного информационного сигнала с отношением сигнал/шум на входе, равным SNR_{in}, учитывая независимость друг от друга и нормальное распределение входного и преобразованного сигналов, получим отношение сигнал/шум на выходе канала утечки

$$SNR_{out} \approx \frac{SNR_{in} \cdot SNR_m}{\sqrt{SNR_{in}^2 + SNR_m^2}}. \qquad (3)$$

Тогда коэффициент шума всего канала утечки можно вычислить как

$$CNL = \sqrt{1 + \left(\frac{SNR_{in}}{SNR_m}\right)^2}. \qquad (4)$$

Заметим, что учет других видов зашумления сигнала утечки на этапе распространения или регистрации может производиться по похожей схеме, принимая независимость процессов зашумления на каждом из этапов.

Шумы преобразования, связанные с искажениями

При преобразовании сигнала из формы существования в источнике в форму для передачи через канал связи происходят искажения сигнала утечки, связанные с неидеальностью преобразования на различных частотах его спектра. Пусть ширина полосы сигнала утечки составляет $\Delta f = f_{\max} - f_{\min}$, где $f_{\max}$ и $f_{\min}$ — максимальное и минимальное значения частот, на которых сигнал теряет 3 дБ своей мощности по отношению к средней части спектра. В этой области спектра идеальное преобразование соответствует некоторому коэффициенту модуляции по амплитуде m_0, являющейся постоянной, независящей от частоты, что соответствует простому масштабированию сигнала по амплитуде с сохранением его формы. В реальном случае спектр коэффициента модуляции $m(f)$ изменяется в зависимости от частоты. Искажения проявляются в отклонении m от постоянной m_0. Если принять, что искажения по спектру не связаны между собой, т. е. каждый процесс преобразования в отдельных частях спектра независим один от другого, тогда относительные отклонения коэффициента модуляции на каждой из частот можно принять за погрешность по амплитуде. Относительную погрешность для мощности можно вычислить как

$$E_m = \frac{1}{\Delta f} \int_{f_{\min}}^{f_{\max}} \eta \cdot (1 - m/m_0)^2 \, df, \qquad (5)$$

где введен $0 < \eta\ (f) < 1$ — весовой множитель вклада спектральной составляющей в сигнал утечки.

Например, для речевого сигнала весовой множитель максимален для формантов и минимален для промежуточных частот. Учитывая определение относительной погрешности, получим

$$SNR_D = 1/E_m = \Delta f \Big/ \int_{f_{\min}}^{f_{\max}} \eta \cdot (1 - m/m_0)^2 \, df. \qquad (6)$$

В случае измерения коэффициента модуляции для эквидистантного набора частот из полосы частот сигнала (рис. 1) всю полосу Δf разбиваем на N равных участков с одинаковыми средними энергиями, пропорциональными $m_0^2 P_0 / N$, тогда мощность шумов можно оценить как

$$P_N = \sum_{i=1}^{N} \eta_i \cdot (m_i - m_0)^2 \, P_0 / N, \qquad (7)$$

а мощность сигнала

$$P_S = m_0^2 P_0, \qquad (8)$$

где P_0 — мощность несущего сигнала.

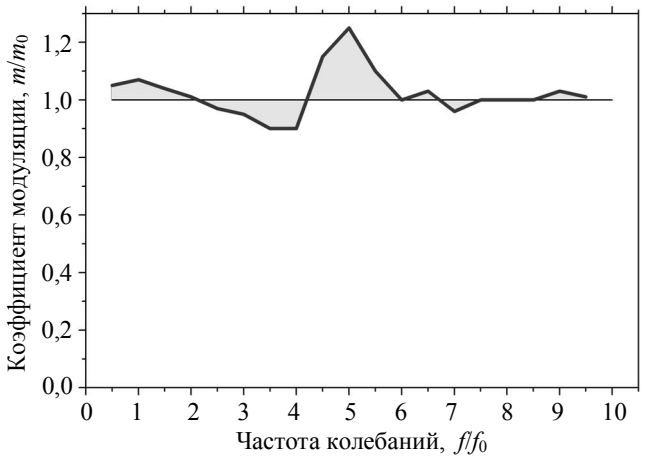

Рис. 1. Искажения спектра сигнала при преобразовании информационного сигнала в сигнал утечки:
——— — m_0; ▬▬ — m/m_0

Следовательно, для отношения сигнал/шум при помехах в виде искажений при дискретном наборе контролируемых частот получим

$$SNR_D = P_S/P_N = N\Big/\sum_{i=1}^{N}\eta_i\cdot(1-m_i/m_0)^2, \qquad (9)$$

здесь $0 < \eta_i < 1$ — весовой множитель вклада i-го участка из полосы частот сигнала.

Применим предложенную методику к вычислению помех в акустооптическом (волоконном) речевом канале утечки [9—11], смысл которого состоит в том, что звук воздействует на элементы волоконно-оптических коммуникаций, модулирует проходящий через них световой поток и формирует сигнал утечки. Модулированный звуком световой поток выходит за пределы охраняемой зоны, где может быть демодулирован. В работе [6] проводились практические исследования спектральной зависимости коэффициента модуляции в акустооптическом (волоконном) канале утечки речевой информации. Представленные результаты можно пересчитать в вид, подходящий для вычисления по вышеописанной методике отношения сигнал/шум. Пересчитаем коэффициент модуляции интенсивности света от 25 дБ октавной ширины до спектральной полосы в 1 кГц (рис. 2).

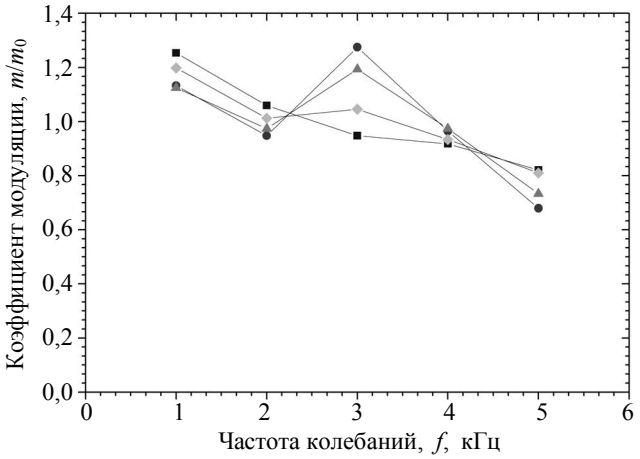

Рис. 2. Нормированный коэффициент модуляции (m/m_0) в зависимости от частоты (f) звукового воздействия для различных значений уровня звукового давления (SPL) в акустооптическом (волоконном) канале утечки речевой информации:
■ — 50 дБ; ◆ — 65 дБ; ▲ — 80 дБ; ● — 90 дБ

Без потери общности весовой множитель в формуле (6) для вычисления SNR_D можно принять равным 1. Зависимость отношения сигнал/шум от уровня звукового давления при идеальном (без шумов) входном сигнале, рассчитанная для спектральных искажений, представлена рис. 3. Как видно, с увеличением уровня звукового давления от 50 до 65 дБ качество преобразования сначала растет, а затем падает. Подобное поведение преобразования сигнала может быть связано с возбуждением акустических резонансов в такой многорезонансной системе как оптический кросс, на котором проводились экспериментальные исследования. Необходимо обратить внимание на высокое отношение сигнал/шум, которое в максимуме приближается к шумам микрофона. На самом деле, его значение ниже, так как сужение полосы частот с 25 дБ от октавы до 1 кГц очень сильно сглаживает реально существующие искажения. Для получения результатов, приближенных к действительности, необходимо провести более точные измерения, но как показывают результаты исследований, предложенная методика оценки зашумления по искажениям спектра соответствует действительности и вносит свой вклад в зашумление сигнала утечки.

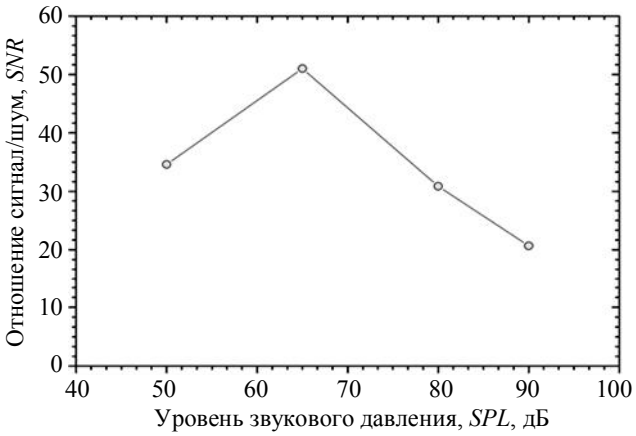

Рис. 3. Зависимость отношения сигнал/шум (SNR) от уровня звукового давления (SPL) в акустооптическом (волоконном) канале утечки речевой информации, зашумление которого связанно со спектральными искажениями сигнала

Шумы преобразования вследствие интерференционных процессов

Формирование технических каналов утечки вследствие неконтролируемой генерации собственных или модуляции сторонних физических полей от источника информации к злоумышленнику происходит на элементах защиты объекта от утечки, ими могут быть стены помещения, корпуса устройств, специальные экраны полей и другое [1—4]. Преобразование защищаемого информационного сигнала в сигнал утечки происходит при попадании его в среду канала утечки, по которому он достигает злоумышленника. Процесс преобразования является сложным и трудно контролируемым. При защите объекта создаются специальные технические элементы, которыми подобный процесс ограничивается, ослабляется, локализуется, но полностью исключить его невозможно. В связи с этим можно считать, что в защищенном помещении, в котором по определению нет закладных

устройств, формирующих утечку, существует возможность неконтролируемых генераций и модуляций, приводящих к формированию незначительных, случайно интерферируемых между собой физических полей, переносящих конфиденциальную информацию.

Процесс случайной интерференции физических полей может происходить по следующему сценарию. Конфиденциальная информация от источника, который можно считать точечным, распространяется во все стороны в виде когерентного физического поля (рис. 4). Достигая защитных элементов объекта (стен, экранов), физическое поле преобразуется в сигнал утечки путем генерации на этих элементах физических полей или модуляции сторонних внешних физических полей, формируемых естественными источниками или искусственными источниками от злоумышленника. В подобном сценарии формирования канала утечки информации важное значение приобретает процесс преобразования информационного сигнала в сигнал утечки. Если область преобразования пространственно распределена по защитным элементам, то злоумышленник, имея дело со слабым сигналом, должен максимально его усилить, увеличив пространственную область сбора, т. е. формировать сигнал утечки, интегрируя его от различных участков элементов защиты. В другом случае, если для формирования сигнала утечки используется нештатное пространственно локализованное устройство генерации или модуляции, то оно не должно быть хорошим генератором или модулятором, т. е. в нем не подавлены все конкурирующие между собой процессы, как это делается в штатных устройствах генерации или модуляции.

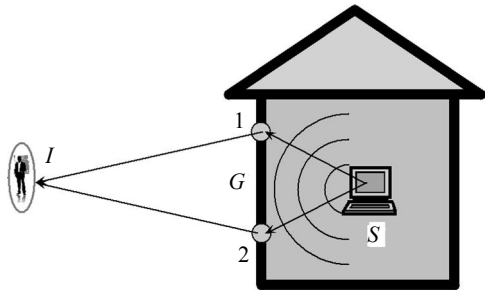

Рис. 4. Условная структурная схема зашумления сигнала утечки при преобразовании вследствие интерференционных процессов:

S — источник информации внутри охраняемой зоны; *I* — злоумышленник за пределами охраняемой зоны; *G* — экран, пространственные элементы системы защиты объекта; 1, 2 — элементы экрана с наибольшим коэффициентом модуляции

Например, в микрофонах стараются использовать для преобразования только один физический эффект, другие эффекты, которые могут давать вклад в формируемый электрический сигнал, подавляются, в противном случае наблюдаются искажения, связанные с интерференцией сигналов от конкурирующих преобразований. В нештатных устройствах такого подавления нет, они просто не предназначены для такого использования, если только это не сделано преднамеренно злоумышленником для улучшения параметров канала утечки.

Таким образом, конкурирующие преобразования, пространственно распределенные по объекту защиты или локализованные в одном элементе с нештатным использованием, приводят к перекрестной интерференции со случайной фазой, что уменьшает отношение сигнал/шум преобразованного сигнала утечки. Формализуем описанный сценарий формирования технического канала утечки информации.

Мощность сигнала вместе с шумом в точке наблюдения вычисляется в соответствии с принципом Гюйгенса—Френеля в аналитической форме (см. рис. 4). Поле когерентного информационного сигнала с амплитудой $\vec{A}_0$ и мощностью P_0 у источника распространяется во все стороны, достигает ослабляющих, отражающих, поглощающих, искажающих элементов экрана системы защиты в виде поверхности G, где происходит преобразование сигнала с коэффициентом модуляции по амплитуде $\tilde{m}_j$ и случайным изменением фазы на $\tilde{\varphi}_j$ в данной точке поверхности $\vec{r} \subset G$. Множество коэффициентов $\tilde{m}_j$ связывается с множественностью механизмов преобразования сигнала, $\tilde{m}_j$ соответствует j-му механизму из X возможных преобразований в данной точке экрана. Информационный сигнал в точке $\vec{r} \subset G$ экрана имеет амплитуду $\vec{A}(\vec{r})$ и фазу $\varphi(\vec{r})$, а после прохождения экрана в результате преобразования амплитуду $\vec{A}(\vec{r})\tilde{m}_j(\vec{r})$ и фазу $\varphi(\vec{r}) + \tilde{\varphi}_j(\vec{r})$. Изменение фазы при прохождении экрана $\tilde{\varphi}_j(\vec{r})$ имеет случайное значение относительно других точек экрана и других преобразований в данной точке экрана, что определяется защитными функциями экрана, который не только ослабляет, но и должен рассеивать информационный сигнал. Мощность сигнала утечки вместе с шумом в точке наблюдения определяется усреднением по пришедшим от разных участков экрана полям, так что

$$P_S + P_N \sim \left\langle \left| \vec{A}_S + \vec{A}_N \right|^2 \right\rangle. \qquad (10)$$

Тогда результирующая мощность сигнала с шумом в точке наблюдения будет определяться как поверхностный интеграл по защитному экрану, усредняемый по времени наблюдения от квадрата амплитуды

$$P_S + P_N \sim \left\langle \left| \oint\limits_G \int K(\vec{r})\,\vec{A}(\vec{r}) \exp\left(i\varphi(\vec{r})\right) \times \right.\right.$$
$$\left.\left. \times \left\{ \sum_{j=1}^{X} m_j(\vec{r}) \exp\left(i\varphi_j(\vec{r})\right) \right\} d\vec{S} \right|^2 \right\rangle, \qquad (11)$$

здесь введен некоторый комплексный коэффициент $K(\vec{r})$, который определяется направлением на точку наблюдения из точки экрана $\vec{r} \subset G$, расстоянием между ними и другими характеристиками пространства от точки наблюдения до точки экрана. Фактически предложенный метод вычисления сигнала утечки на выходе канала является модификацией принципа Гюйгенса—Френеля, выраженного в виде дифракционного интеграла Френеля [13]. Предложенная методика вычисления может быть применена для электромагнитного, оптического, акустического или какого-либо иного вида поля, важно, чтобы для него выполнялся принцип суперпозиции полей.

Полученное общее выражение задает физические принципы вычисления поля утечки в точке наблюдения, но не позволяет осуществить практическое вычисление поля, что связано с множеством неизвестных параметров. Оно является определением принципа расчета, подобно принципу Гюйгенса—Френеля для вычисления распределения интенсивности в результате дифракции. Адаптируем данное выражение к практическим вычислениям мощности поля утечки. Разобьем защитный экран на участки с когерентным преобразованием информационного сигнала с одинаковой фазой, наподобие зон Френеля, но только нумерацию зон проведем не по фазе, а по убыванию коэффициента модуляции на этих участках защитного экрана (см. рис. 4). В этом случае получим бесконечный набор участков с коэффициентом модуляции амплитуды $\{m_k\}$ и связанной с ним фазой $\{\varphi_k\}$, которые можно будет расположить следующим образом, $m_0 > m_1 > \ldots > m_k > m_{k+1} > \ldots$, все коэффициенты имеют фазы φ_k, $k = 0, 1, 2\ldots$ со случайным значением друг относительно друга и можно принять $\varphi_0 = 0$, тогда

$$P_S + P_N = P_0 \left\langle \left| m_0 + \sum_{k=1}^{\infty} m_k \exp(i\varphi_k) \right|^2 \right\rangle, \qquad (12)$$

здесь, как было введено ранее, P_0 — мощность информационного сигнала у источника. После выполнения операции усреднения, окончательно получаем

$$P_S + P_N = P_0 \left(m_0^2 + \sum_{k=1}^{N} m_k^2 \right), \qquad (13)$$

здесь число учитываемых областей защитного экрана ограничено некоторым числом, равным N, на практике это число составляет 3—5 и не может превышать 10 из общих соображений. Учет большего числа областей теряет смысл из-за малости коэффициентов модуляции, основное значение имеют первые 3—4.

Все коэффициенты модуляции $m_k^2 = CML_k$ между собой не коррелируют, они не связаны между собой вследствие случайности их фазы после прохождения экрана. При формировании канала утечки в первую очередь регистрируется самый мощный приходящий от источника когерентный сигнал, все остальные составляющие сигнала утечки из-за случайности фазы можно считать помехой для основного, поэтому принимаем, что мощность сигнала утечки в точке наблюдения равна

$$P_S = P_0 m_0^2, \qquad (14)$$

а мощность шумов

$$P_N = P_0 \sum_{k=1}^{N} m_k^2. \qquad (15)$$

Таким образом, получаем отношение сигнал/шум вследствие интерференционных процессов в виде

$$SNR_I = P_S / P_N = CML_0 \Big/ \sum_{k=1}^{N} CML_k. \qquad (16)$$

Полученное выражение имеет логическое обоснование. Брешь в системе защиты формируется по наиболее эффективному каналу утечки с максимально большим коэффициентом модуляции, все остальные к нему являются помехой. Поэтому злоумышленник старается подавить случайные помехи и выделить основной канал утечки. Он может использовать механизмы пространственной селекции сигналов, т. е. регистрировать сигнал, идущий только от одной области защитного экрана, или частотной селекции, уменьшая мощность помех, или какие-либо другие методы. Все эти действия приводят к уменьшению шумовых составляющих в сигнале утечки, т. е. оптимизации суммы $\sum_{k=1}^{N} CML_k$. В мероприятиях по защите информации, наоборот, стараются уменьшить и выровнять вклады от различных каналов, создавая ситуацию, когда сигнал утечки сам себе создает помехи.

Рассмотрим практическую ситуацию по вычислению отношения сигнал/шум для сигнала утечки в акустооптическом (волоконном) канале утечки речевой информации [9—11]. Один из возможных механизмов амплитудной модуляции реализуется на механических разъемах оптического кабеля [5, 6], в которых на одном и том же механическом соединении происходит модуляция интенсивности проходящего или отраженного света вследствие трех возможных упругих смещений: углового рассогласования $\delta\Theta$, неплотного соединения δd и радиального смещения δs соединяемых волокон (рис. 5). Каждый механизм дает свой вклад в мо-

дуляцию, наибольший из которых дает угловое рассогласование CML_Θ, а остальные два — радиального смещения CML_d и неплотного соединения CML_s, имея случайную фазу между собой и основным, являются помехой. Отношение сигнал/шум данного канала утечки [5] можно определить как

$$SNR_{out} = \frac{CML_\Theta}{CML_d + CML_s} = \\ = \frac{2(n_0/NA)(\delta\Theta/\pi)}{(\delta s/a)\,\mathrm{tg}(\arcsin NA/n_0) + (\delta d/a)(2/\pi)}, \quad (17)$$

где a — диаметр сердцевины волокна;
n_0 — показатель преломления сердцевины волокна;
NA — числовая апертура.

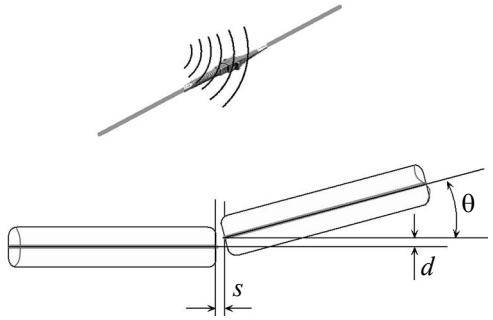

Рис. 5. Вызываемые акустической волной одновременные механические деформации волоконно-оптического разъема, приводящие к осевым (s), радиальным (d) и угловым (θ) относительным смещениям волокон

Оценим угловые колебания $\delta\Theta$ = 0,03 рад; примем, что смещения по оси и по радиусу по порядку величины совпадают и равны $\delta d = \delta s$ = = 0,1 мкм; значения n_0 = 1,45; числовую апертуру NA примем равным 0,15 для одномодового волокна диаметром a = 10 мкм и 0,3 для многомодового волокна диаметром a = 50 мкм. Тогда значение отношения сигнал/шум после прохождения идеального сигнала можно оценить как 30 и 70 для одно- и многомодового волокон, соответственно. Такие большие значения SNR_{out} можно связать с тем, что в реальных условиях в шумы сигнала утечки существенный вклад дают также искажения звукового сигнала при модуляции в разъеме, помехой могут являться интерференционные явления с сигналами, формируемыми на соседних пассивных элементах общего канала утечки. Но даже такие упрощения показывают высокую опасность формирования сигнала утечки на пассивных элементах волоконно-оптических коммуникаций, особенно если технические средства разведки позволят выделить сигнал только с одного разъема.

Представленные теоретические исследования, дополненные сравнением с практическими измерениями по исследованию акустооптического (оптоволоконного) канала утечки, показывают возможность использования на практике полученных выражений для оценки коэффициента шума канала утечки, а значит и коэффициента эффективности канала утечки.

Литература

1. *Ярочкин В. И.* Информационная безопасность: уч. пос. для непрофильных вузов. — М.: Международные отношения, 2000. — 400 с.
2. *Торокин А. А.* Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005. — 960 с.
3. *Халяпин Д. Б.* Защита информации. Вас подслушивают? Защищайтесь. — М.: НОУ ШО "БАЯРД", 2004. — 431 с.
4. *Хорев А. А.* Технические каналы утечки информации. — М.: НПЦ "Аналитика", 2008. — 436 с.
5. *Гришачёв В. В., Косенко О. А.* Количественная оценка эффективности канала утечки информации по техническим параметрам каналов связи//Вопросы защиты информации. 2010. № 4. С. 9—17.
6. *Гришачёв В. В., Косенко О. А.* Практическая оценка эффективности канала утечки акустической (речевой) информации через волоконно-оптические коммуникации//Там же. 2010. № 2. С. 18—25.
7. *Харкевич А. А.* Борьба с помехами. — М.: Книжный дом "ЛИБРОКОМ", 2009. — 280 с.
8. *Белоусов А. П., Каменецкий Ю. А.* Коэффициент шума. — М.: Радио и связь, 1981. — 112 с.
9. *Гришачёв В. В., Халяпин Д. Б., Шевченко Н. А.* Волоконно-оптический телефон в акусто-оптоволоконном канале утечки конфиденциальной речевой информации//Вопросы защиты информации. 2009. № 3. С. 22—30.
10. *Гришачёв В. В., Халяпин Д. Б., Шевченко Н. А., Мерзликин В. Г.* Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС//Специальная техника. 2009. № 2. С. 2—9.
11. *Гришачёв В. В., Халяпин Д. Б., Шевченко Н. А.* Анализ угроз утечки речевой информации через волоконно-оптические коммуникации//Вопросы защиты информации. 2008. № 4. С. 12—17.
12. *Кунце Х.-И.* Методы физических измерений. — М.: Мир, 1989. — 216 с.
13. *Ахманов С. А., Никитин С. Ю.* Физическая оптика. — М.: Изд-во МГУ, Наука, 2004. — 656 с.

Estimation of noise coefficient of technical convert channel

V. V. Grishachev, O. A. Kosenko

The Institute of Information Sciences and Security Technologies, The Russian State University for the Humanities (RSUH), Moscow, Russia

Estimation methods of noise coefficient in the technical convert channel are discussed on the basis of noise generation at transformation of an information signal to a leak signal. Noise formation is related to two processes — spectrum distortion and interference from different sources of a leak signal.

Keywords: data object protection, technical covert channel, and convert channel noise coefficient.

Гришачёв Владимир Васильевич, доцент кафедры инженерно-технической защиты информации.
Тел./факс 8 (495) 387-20-18. E-mail: grishachev@mail.ru
Косенко Оксана Александровна, студентка.
Тел./факс 8 (495) 387-20-18. E-mail: ksasha88@bk.ru