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

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

4 (91)

Москва
2010
Основан
в 1974 г.

СОДЕРЖАНИЕ

Криптография

Бабаш А. В. Метод приближенных моделей в решении задач определения входного слова автомата 2

Выявление и предотвращение возможной утечки информации

Гришачев В. В., Косенко О. А. Количественная оценка эффективности канала утечки информации по техническим параметрам каналов связи 9

Биометрические методы и средства защиты информации

Имамвердиев Я. Н. Метод биометрического хеширования на основе ортогональных преобразований для защиты биометрических шаблонов 18

Автоматизированные системы, технологии и программные средства защиты информации от несанкционированного доступа

Коллеров А. С. Метод формирования значений параметров сетевого трафика, характеризующих канал передачи, в задаче тестирования сетевых систем обнаружения атак 24

Защита информации в компьютерных системах и системах связи

Гайдамакин Н. А., Леонтьев С. В. Метрический анализ качества стандартных (номинально-охватных) подходов к классификации безопасности компьютерных систем 31

Рагимов Э. Р. Механизм верификации безопасности программных средств, функционирующих в системе защиты информации корпоративных сетей 37

Черкашин О. А. Методика выбора и оптимизации параметров циклического кода для систем защиты информации с решающей обратной связью ... 41

Перченок А. А. Мультиязычный высокоскоростной протокол передачи данных, основанный на принципах сериализации 45

Общие вопросы безопасности информации и объектов

Карпычев В. Ю., Скрыль С. В., Сычев А. М., Курило А. П. Проблема синтеза системы показателей для оценки качества защиты информации 51

Указатель материалов, опубликованных в журнале в 2010 г. 58

Вопросы защиты информации: Науч.-практ. журн./ФГУП "ВИМИ", 2010. Вып. 4 (91). С. 1—60.

Редакторы: *Г. А. Никитин, Л. К. Андрианова*
Корректор *Н. С. Кузьмина*
Компьютерная верстка: *Н. В. Соколова, И. А. Жамальдинова*

Подписано в печать 2.11.2010.
Формат 60x84 1/8.
Бумага офсетная. Печать офсетная. Усл. печ. л. 7,0.
Уч.-изд. л. 7,8. Тираж 500 экз.
Заказ 1654. 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

Количественная оценка эффективности канала утечки информации по техническим параметрам каналов связи

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

На основе стандартных характеристик по определению качества функционирования каналов передачи информации предлагается набор параметров по оценке эффективности каналов утечки информации. Рассмотрены методы расчета параметров для практического использования при описании каналов утечки различного вида и природы. В качестве примера проведена оценка характеристик акустооптоволоконного канала утечки.

Ключевые слова: защита объекта информатизации, канал утечки информации, эффективность канала утечки информации.

В современном мире информация приобретает все возрастающее значение, ее огромные потоки непрерывно циркулируют в обществе. В геометрической прогрессии возрастает и ее влияние на объективность принятых решений — наличие достоверной информации позволяет разносторонне оценивать ситуацию и просчитывать разные варианты протекания событий. Обладание знаниями делает нас смелыми и уверенными, а их отсутствие — нерешительными и уязвимыми. Поэтому получение и распространение информации стало основополагающей функцией многих структур, а на ее защиту тратятся немалые силы и средства. Опасность ее утечки может поставить под угрозу благосостояние отдельного человека, организации и целого государства [1—3].

Значительная роль в деле защиты информации отведена службам безопасности, обладающим необходимыми техническими средствами и навыками практической работы. Их обеспеченность нормативно-методическими документами позволяет проводить эффективную оценку защищенности объектов информатизации как с помощью технических средств, так и теоретических методов на основе инженерно-технических характеристик объектов. Если первый способ оценки довольно трудоемок и требует привлечения на длительный срок большого числа специалистов с необходимой аппаратурой, то для осуществления второго — достаточно даже одного специалиста, владеющего инженерно-техническими характеристиками охраняемого объекта и набором методик по оценке защищенности информации. Причем, подобные исследования могут быть проведены без выезда на объект в течение короткого времени на любом этапе его функционирования (проектирования, строительства, ремонта и т. д.). Таким образом, результативность подобных методик может быть достаточно высокой, если будет доказана их надежность, достоверность и объективность [4, 5].

Защищенность современных информационных систем целесообразно оценивать по наличию и эффективности потенциальных каналов утечки информации. Чем выше вероятность прохождения каждого бита информации от источника к злоумышленнику, тем менее надежной можно считать данную информационную систему. Однако объективно оценить эффективность каждого канала утечки представляется возможным только по параметрам его составных элементов. Поэтому разработка теоретических методов оценки защищенности информационных систем по техническим характеристикам канала утечки является актуальной проблемой информационного общества [6—8].

Обобщенный канал утечки информации

Для управления риском информационной утечки рассмотрим типовую структуру ее обобщенного канала (рис. 1) [1—5]. В нем можно выделить источник и получатель информации, которая через канал связи передается от передатчика к приемнику и подвергается воздействию шумов на каждом этапе.

Источник информации — обладатель конфиденциальной информации. В качестве наиболее часто встречающегося источника, с учетом перевода в электронный вид современного документообо-

рота, могут выступать данные, циркулирующие в информационной системе. Такая информация представляется в виде модулированного электромагнитного поля, передаваемого через окружающую среду или по волноводам. Кроме данных источниками могут выступать электромагнитное, акустическое, тепловое, радиационное, гравитационное и другие поля, существующие внутри защищаемого объекта, интегрированные в форме изображений, речи и других специальных видов информации. Каждый вид конфиденциальной информации имеет свои особенности формирования, существования и распространения, что изначально задает способ утечки.

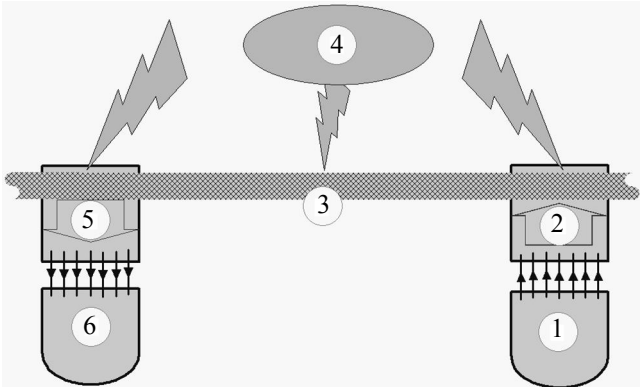

Рис. 1. Типовая структура обобщенного канала утечки информации:
1 — источник информации; 2 — передатчик; 3 — канал связи, 4 — шумы; 5 — приемник; 6 — адресат

Передатчик — устройство ввода информации в канал утечки (модулятор, преобразователь). Вывод информации за пределы охраняемой зоны во многом определяется тем, какое поле является носителем. Во-первых, поле носителя не совпадает с изначальной формой представления конфиденциальной информации. Например, подслушивание путем высокочастотного навязывания через электропроводку, в этом случае акустическое поле модулирует высокочастотное электромагнитное поле в проводнике. Во-вторых, поле носителя совпадает с изначальной формой представления конфиденциальной информации. Например, подслушивание через стенку, это случай, когда акустическое поле в воздушной среде (комната) проникает через твердую среду (стена) в окружающее пространство (улица). Хотя технические особенности формирования каналов утечки различны — в первом есть модулятор, а во втором нет. Но принципиальной разницы по оценке эффективности утечки нет. Переход поля одного вида из одной среды в другую можно рассматривать как генерацию, что по принципам описания близко к описанию модуляции. Такое обобщение должно осуществляться отдельно для каждого случая, но позволяет при математическом описании процессов пользоваться общими подходами, чем и воспользуемся в дальнейшем. Наверное, исключения возможны, но и они могут быть адаптированы путем введения специальных коэффициентов.

Надо отметить, что выявление преобразователей — одна из главных задач поиска каналов утечки. Определив возможные преобразования можно однозначно определить эффективность канала утечки и способы их подавления. Эффективность преобразования во многом определяется коэффициентом модуляции и собственными шумами. В частности, коэффициент модуляции для канала утечки без изменения вида полевого носителя можно принять равным единице.

Канал передачи (связи) — среда, через которую происходит передача преобразованной в передатчике информации. Во-первых, это окружающая источник среда, сигнал в которой распространяется прямолинейно или по более сложной ломаной линии. В другом случае передача происходит через искусственный/естественный и штатный/нештатный волновод. Наиболее просто идентифицируется штатный искусственный волновод, для обнаружения других типов требуется специальные исследования или знание конструктивных и технических особенностей защищаемых объектов. На качество передачи информации влияет ослабление сигнала при прохождении канала, а также его искажение и зашумление внешними источниками.

Шумы — случайные воздействия на передатчик, канал связи и приемник, связанные с преобразованием, передачей и регистрацией информации. Возникновение шумов связано со многими процессами. При преобразовании сигнала в передатчике и приемнике он может быть искажен или зашумлен другими сигналами, а при распространении в канале связи возможно добавление к информационному сигналу посторонних сигналов, которые являются шумами. Все шумы можно разделить на два вида: мультипликативные — связанные с искажениями самого сигнала и внутренними шумами аппаратуры связи, и аддитивные — связанные с внешними помехами. Примером мультипликативных шумов является искажение сигнала при модуляции, что связано с высокой нелинейностью процесса в элементах информационного объекта, не предназначенного для подобного преобразования. Считается, что закладных устройств нет, существует модуляция только на штатных элементах системы, являющаяся нежелательным, паразитным, трудно контролируемым процессом, а также шумы, которые возникают при модуляции, передаче и регистрации, и связаны с откликом элементов канала на прохождение сигнала. Примером аддитивных шумов можно считать любые посторонние сигналы, которые интерферируют с информационным сигналом со случайным сдвигом фазы. К ним

относятся и системы искусственной постановки помех для предотвращения утечки путем зашумления.

Для идеального канала утечки аддитивные шумы можно принять равными нулю, а зашумленность канала утечки должна определять мультипликативные шумы. Подобное соотношение между шумами является отличием канала утечки от канала передачи информации, в котором, наоборот, искажения различными техническими средствами минимизируются, и основной вклад дают неконтролируемые внешние естественные шумы. Еще одно отличие состоит в уровне шумов: как правило, уровень шумов современных систем связи намного меньше уровня информационного сигнала, а в канале утечки выполняется обратное условие — шумы сравнимы с сигналом утечки. Естественным критерием самого существования утечки является равенство или превышение сигнала утечки шумов ($SNR \le 1$).

Приемник — устройство вывода информации (демодулятор). Включает аппаратуру регистрации сигнала и последующей демодуляции и преобразования принятой информации в требуемый вид. Как правило, приемная аппаратура много эффективнее передающей, поэтому при обсуждении функционирования канала утечки можно считать, что прием является идеальным и все отклонения происходят на этапе преобразования (модулирования) в передатчике или в канале связи.

Адресат — злоумышленник, получатель информации.

Рассмотрим некоторые общие особенности канала утечки. Все каналы утечки можно разделить на основные и побочные. К первым относятся утечка информации, циркулирующая в самой информационной системе, как правило, в электронном виде или оптическом виде, которая создается и передается штатным оборудованием. Канал утечки может быть осуществлен методами несанкционированного доступа или перехвата из каналов связи. Вторые связаны с возможностью использования существующих штатных систем связи для сбора специальной информации, несвязанной с передаваемой. Например, циркулирующие внутри объекта сопутствующие звуки, которые модулируют информационный сигнал штатных систем связи; распределение температур внутри объекта, влияющие на работу аппаратуры связи и т. д. Также ко второму типу каналов можно отнести использование естественных и искусственных волноводных каналов, существующих на объекте, которые могут быть использованы для утечки.

Эффективность формирования и функционирования канала утечки зависит от вида сигнала, с которым имеем дело — цифровой или аналоговый. Основное различие между ними связано с тем, что форма и параметры цифрового сигнала изначально известны, поэтому при двоичном кодировании вероятность ошибки в распознании (0 или 1) не может быть меньше 50 %, так как различаются два известных уровня. Для аналогового сигнала ошибка достигает 100 %, так как изначально неизвестен ни уровень, ни форма сигнала. По своей природе цифровой канал утечки связан с формированием утечки данных из систем связи или с работой закладного цифрового устройства. В технических средствах разведки наиболее часто встречается аналоговый канал утечки, что связано с нештатным использованием штатных каналов связи или с применением специальных средств вывода информации. Когда проводится оценка защищенности объекта информатизации предполагается, что закладные устройства отсутствуют. В противном случае, эффективность утечки не определена и зависит от закладного устройства.

Существующие методы оценки защищенности системы, как правило, используют вероятностные методы. Они позволяют эффективно и интуитивно понятно вычислить вероятность защищенности, часто они связаны с общими теоретическими предпосылками, которые сложно выявить [4—8]. Разработка практических методик оценки эффективности инженерно-технических каналов утечки информации, а значит, и защищенности объекта информатизации, является целью настоящей работы.

Эффективность канала утечки и его теоретическая оценка

Принципы функционирования канала утечки во многом совпадают с принципами работы обычного канала связи [9—11] — все основные элементы совпадают, что позволяет перенести способы оценки качества связи на оценку эффективности функционирования канала утечки с учетом его особенностей. К ним можно отнести высокую зашумленность, плохие характеристики передатчика и отличные показатели приемника и ряд других отличий. Выделим базовые технические параметры информационной системы, влияющие на эффективность функционирования канала связи.

- *SNR* [12, 13], отношение сигнал/шум, определяющее долю шума в измеряемом сигнале по отношению к полезному сигналу:

$$SNR = \frac{P}{N} = \left(\frac{A_s}{A_n}\right)^2,$$

где P, N — средняя мощность сигнала и шума, соответственно;

A — среднеквадратичные значения амплитуд.

Обычно *SNR* измеряется в децибелах. Чем больше это отношение, тем меньше шум влияет на характеристики системы.

• F [14], коэффициент шума, характеризующий шумы, привнесенные информационной системой или ее подсистемами при условии полного согласования приема—передачи системы связи:

$$F = \frac{SNR_{\text{in}}}{SNR_{\text{out}}},$$

где SNR_{in} — отношение сигнал/шум на входе канала связи;

SNR_{out} — отношение сигнал/шум на выходе канала связи.

Часто F выражается в децибелах. Если канал связи не вносит собственных шумов при прохождении сигнала, и, следовательно, отношение сигнал/шум на входе сохраняется и остается равным отношению на выходе, тогда $F = 1$. В случае реального канала связи $F > 1$, так как прохождение информативного сигнала по каналу связи приводит к увеличению в нем доли шума — его зашумлению, а значит уменьшению отношения сигнал/шум на выходе.

• Q-фактор, контролирующий качество связи по коэффициенту ошибок в цифровых системах связи [9, 10]:

$$Q = \frac{|I_1 - I_0|}{\sigma_1 + \sigma_0},$$

где I_i и σ_i (при $i = 0,1$) — ток и среднеквадратичное отклонение тока при приеме единичного и нулевого битов, соответственно. Если принять, что $\sigma_1 = \sigma_0$ и $I_1 = 0$, а также учесть, что средняя мощность шумов совпадает со среднеквадратичным отклонением мощности сигнала, то получим следующую связь Q-фактора с SNR_{out} : $Q \approx SNR_{\text{out}}/2$. Подобная связь коэффициентов позволяет перенести выражения для параметров, характеризующих передачу информации в цифровом виде на аналоговые системы связи.

• BER [9—11], вероятность появления ошибочного бита за одну секунду при приеме информации при нормальном распределении вероятностей нулевых и единичных битов. Основываясь на Гауссовой аппроксимации распределения шума, можно вывести соотношение между вероятностью ошибки и Q-фактором:

$$BER = \frac{1}{2}\left[1 - \text{erf}\left(\frac{Q}{\sqrt{2}}\right)\right],$$

где $\text{erf}(x) = 1 - \text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \exp\left(-t^2\right) dt$ — функция ошибок.

По величине BER определяют качество связи. В современных волоконно-оптических системах величина передачи информации не должна быть больше 10^{-12} в соответствии с международным стандартом ITU-T G.692.

• B, полоса пропускания канала связи [9—11], разница между максимальной и минимальной частотами, которые могут быть надежно переданы каналом связи. Обычно это частоты, на которых сигнал теряет половину своей мощности по сравнению с уровнями мощности для частот в середине диапазона, что соответствует ослаблению сигнала на 3 dB. С полосой пропускания связана C — максимальная скорость передачи данных за единицу времени через канал связи с шумами, определяемая теоремой Шеннона—Хартли, выражаемая в битах в секунду: $C = B \cdot \log_2(1 + SNR)$.

• β [9, 10], полный коэффициент ослабления сигнала в канале связи:

$$\beta = 10 \cdot \lg\left(\frac{P_{\text{in}}}{P_{\text{out}}}\right),$$

где P_{in} — мощность сигнала на входе канала связи;

P_{out} — мощность сигнала на выходе канала связи;

α — коэффициент ослабления сигнала в канале связи на километр: $\alpha = \beta/L$, где L — длина линии связи. Коэффициент ослабления является одной из характеристик бюджета канала связи, который определяется соотношением между ресурсами передачи и приема, источниками шума, ослабления сигнала.

• m, коэффициент (глубина) модуляции несущего поля информационным сигналом, характеризует эффективность преобразования в модуляторе. Например, в случае амплитудной модуляции гармонического несущего поля на частоте ω гармоническим информационным полем на частоте Ω коэффициент модуляции определяется из выражения

$$P = P_0 (1 + m \cdot \sin \Omega t) \sin \omega t,$$

где P и P_0 — мощности модулированного и немодулированного несущего поля, соответственно. Коэффициент модуляции в реальных системах обычно достигает единицы.

Представленные выше характеристики не составляют полную систему, применяемую для описания систем передачи информации, но они являются наиболее общими и знание их численного значения позволяет оценить качество связи. Такие же параметры можно ввести и для оценки качества канала утечки с учетом их особенностей, таких как высокая зашумленность, аналоговая форма сигнала и т. д. Выберем из выделенных параметров характеристики, способные наиболее эффективно оценить качество функционирования канала утечки.

Основными техническими характеристиками канала утечки информации можно принять сле-

дующие величины: $P_{\text{in}}(N_{\text{in}})$ — мощность сигнала (шума) на входе канала утечки и $P_{\text{out}}N_{\text{out}})$ — мощность сигнала (шума) той же природы на выходе канала утечки, на основе которых вводятся отношения средних мощностей сигнала к шуму на входе канала утечки SNR_{in} и на его выходе SNR_{out}. По аналогии с техническими параметрами канала связи рассмотрим характеристики канала утечки, наиболее существенные для оценки его эффективности:

• *CML* [15], ***коэффициент модуляции канала утечки***, определяется в зависимости от вида несущего поля и модулируемого параметра. Коэффициент модуляции является характеристикой конкретного преобразования и определяет долю информационного сигнала от амплитуды несущего. Отличительной особенностью является то, что его величина в канале утечки имеет значение, намного меньшее единицы. Это естественное приближение, связанное с тем, что модуляция является паразитным эффектом, которое стремятся максимально ослабить. Практические методы определения коэффициента модуляции связаны с экспериментальным измерением коэффициента (глубины) модуляции несущего поля внешним информационным полем в зависимости от величины внешнего воздействия.

• *CNL*, ***коэффициент шума канала утечки***:

$$CNL = \frac{SNR_{\text{in}}}{SNR_{\text{out}}}.$$

Отличительной особенностью *CNL* является то, что $SNR_{\text{in}} >> SNR_{\text{out}}$, так как сам канал утечки создает значительное зашумление сигнала, вызываемое непрофильным его использованием, влиянием пассивных и активных систем защиты информации. Основной задачей любой службы безопасности является увеличение *CNL* по всем видам инженерно-технических каналов утечки информации, реализуемых для объекта информатизации.

• *CLL*, ***коэффициент потерь (бюджет) канала утечки***:

$$CLL = 10\lg\left(\frac{P_{\text{in}}}{P_{\text{out}}}\right).$$

Бюджет канала ограничивает возможности технических средств разведки для съема информации за счет естественного ослабления. На основе *CLL* становится возможным определение такого параметра, как минимальная чувствительность регистрирующей аппаратуры. В случае мощности входного сигнала P_{in} имеем

$$S_{\min} = P_{\text{out}} = \frac{P_{\text{in}} \cdot CML}{10^{CLL/10}},$$

где было учтено, что информационная составляющая сигнала определяется глубиной модуляции несущего поля. Надо отметить, что чувствительность регистрирующей аппаратуры определяет пространственные параметры канала утечки, такие как минимальное расстояние от источника информации (сигнала) до регистрирующей аппаратуры, по которому рассчитывают размеры охранной зоны.

• *CEL*, ***коэффициент эффективности канала утечки*** [16, 17]:

$$CEL = \frac{H_x}{H_0} = \left(1 - \frac{\Delta H}{H_0}\right),$$

где H_0 — объем информации на входе канала утечки в битах;

H_x — объем информации на выходе канала утечки в битах;

$\Delta H = H_0 - H_x$ — объем потерянной информации в канале утечки в битах.

Коэффициент эффективности канала утечки является обобщающим понятием, позволяющим численно оценить опасности утечки. *CEL* определяет вероятность прохождения одного бита информации через данный канал утечки, которая зависит от представления информации в цифровом (дискретном) или аналоговом (непрерывном) виде.

В случае канала утечки с цифровым представлением информации величина $(\Delta H/H_0) \equiv BER$, что соответствует определению *BER* как вероятности появления ошибочного бита в цифровых системах связи. Следовательно, коэффициент эффективности цифрового канала утечки будет определяться следующей формулой

$$CEL = 1 - BER = \frac{1}{2}\left[1 + \text{erf}\left(\frac{Q}{\sqrt{2}}\right)\right] \geq 0,5.$$

Таким образом, эффективность цифрового канала утечки всегда выше 50 %. Однако техническая реализация данного канала затруднена и может быть реализована только в виде закладок, поэтому дальнейшее рассмотрение подобного вида утечки мы не проводим.

В случае канала утечки с аналоговым представлением информации величина $(\Delta H/H_0) = 2BER$, что связано дополнительной неопределенностью в разрешении непрерывного сигнала, которая проявляется в том, что уровень изменения сигнала не определен, он может быть в следующий момент как выше, так и ниже исходного. Подобную неопределенность можно принять как удвоение вероятности появления ошибки для цифрового канала утечки, в котором уровни сигналов изначально определены. Тогда коэффициент эффективности аналогового канала утечки определяется как

$$CEL = 1 - 2BER = \text{erf}\left(0,35\frac{SNR_{\text{in}}}{CNL}\right).$$

Представленный набор характеристик позволяет теоретически оценить эффективность канала утечки и выявить наиболее опасные направления, представляющие угрозу для объекта информатизации. Что касается практического расчета, то он имеет смысл для коэффициентов модуляции, шума и потерь, так как коэффициент эффективности канала утечки имеет лишь обобщающее значение. Рассмотрим далее методы расчета CNL и CLL.

Выходной сигнал зависит от параметров входного сигнала и преобразований в канале утечки. Мощность выходного сигнала можно выразить как произведение мощности входного сигнала и некоторого коэффициента, зависящего от характеристик процесса модуляции сигнала при его передаче (M), от показателей канала связи (T) и от параметров регистрирующей аппаратуры (R):

$$P_{\text{out}} = f(M,T,R)\,P_{\text{in}} + N_{\text{add}}.$$

Здесь N_{add} — внешние аддитивные к сигналу помехи, зависящие от состояния окружающей среды, ее зашумленности. Величина аддитивных помех может изменяться со временем случайным образом, а также путем создания внешних искусственных помех специальными генераторами шума. Для оценки естественного зашумления, связанного только с преобразованием сигнала в канале утечки, можно принять $N_{\text{add}} = 0$, что соответствует идеальным условиям прохождения сигнала и максимальной эффективности канала утечки. Включение специального устройства, создающего шум в канале утечки, приведет к увеличению доли шума в сигнале.

При нормальном распределении вносимых в канал утечки шумов можно получить выражение для вычисления коэффициента шума, если использовать для расчета выражение относительной погрешности при косвенных измерениях [18]. После преобразований выражение примет следующий вид:

$$CNL = \sqrt{1 + (D_M CNL_M)^2 + (D_T CNL_T)^2 + (D_R CNL_R)^2},$$

где $D_i = i(\partial f/\partial i) f^{-1}$ при $i = M,T,R$. CNL_i $(i = M,T,R)$ — коэффициент шума соответствующего элемента канала утечки при входном сигнале с отношением сигнал/шум, равном SNR_{in}. По аналогии коэффициент потерь канала утечки примет вид:

$$CLL = 10 \cdot \left|\lg\left[f(M,T,R)\right]\right|.$$

Дальнейшее уточнение расчетных выражений требует более конкретного описания принципов функционирования канала утечки, т. е. необходимо определить, как происходит модуляция поля в канале передачи, чем вызваны потери, каковы параметры регистрирующей аппаратуры. Сделав дополнительные предположения об особенностях канала утечки, можно еще сильнее упростить представленные выражения. Во-первых, будем считать, что канал имеет мультипликативную природу, т. е. $f(M,T,R) = MTR$, тогда $D_i = 1$ для любого i. Во-вторых, основной вклад в зашумление сигнала происходит на стадии модуляции поля, т. е. $SNR_M << SNR_T$, $SNR_R << SNR_{\text{in}}$, тогда коэффициент шума будет приближенно равен

$$CNL \approx \frac{SNR_{\text{in}}}{SNR_M},$$

а коэффициент эффективности, если ввести $SNR_{\text{out}} = \min\{SNR_M, SNR_T, SNR_R\} << SNR_{\text{in}}$, примет вид

$$CEL = \text{erf}(0{,}35 \cdot SNR_{\text{out}}).$$

Примером реализации подобного приближения является подслушивание через толстую стену. Множитель M соответствует коэффициенту прохождения звуковой волны из воздушной среды в стену, а T — затуханию в стене без учета интерференции для многократно отраженных волн. Коэффициент R характеризует чувствительность приемной аппаратуры, вплотную прижатой к стене.

На рис. 2 представлен график зависимости $CEL(SNR_{\text{out}})$. На графике указан некоторый переходной участок с $SNR_{\text{out}} = 1$, когда $CEL = 0{,}38$. Вычислим CEL, когда сигнал в два раза превышает шум на входе канала утечки $(SNR_{\text{in}} = 2)$, а зашумление сигнала происходит в основном на стадии модуляции $(SNR_M = 0{,}5)$, в этом случае получаем $CEL = 0{,}19$. Данное значение вполне соответствует действительности, когда сигнал в регистрирующей аппаратуре меньше шумов в два раза.

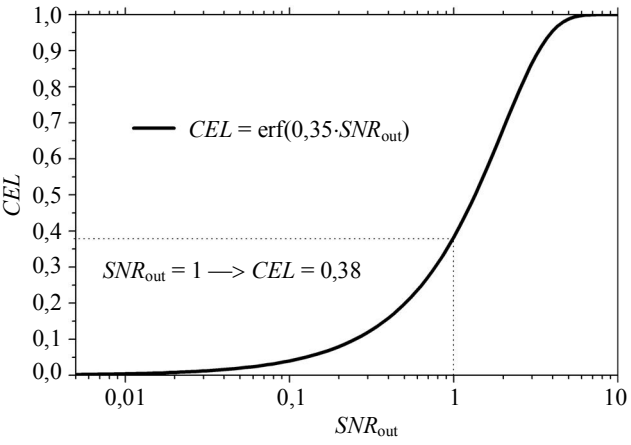

Рис. 2. График зависимости коэффициента эффективности канала утечки от отношения сигнал/шум на выходе $CEL(SNR_{\text{out}})$

Оценка параметров акустооптоволоконного канала утечки

Акустооптоволоконный канал утечки заключается в подслушивании или получение другой звуковой информации через волоконно-оптические коммуникации учреждения. Суть эффекта состоит в том, что акустическое поле или связанные с ним вибрационные колебания действуют на оптический кабель, проходящий через помещение, вызывая модуляцию световых потоков в нем по амплитуде, фазе, поляризации и частоте. Модулированный свет по оптическому кабелю выходит за пределы охраняемой зоны и демодулируется, тем самым восстанавливается исходный акустический сигнал. В представленной модели световые потоки могут формироваться штатным оборудованием или специальными источниками, включаемыми в сеть злоумышленником. Модуляция может происходить на пассивных и активных элементах сети. В работе [1] представлено качественное описание физических принципов модуляции в местах разъемного соединения волокон, как показывают исследования это один из наиболее эффективных механизмов утечки наряду с виброакустическим воздействием на кабель в местах контакта с конструкциями зданий и монтажными элементами сети [15–17].

В качестве основного механизма формирования модулированного сигнала будем считать несогласованность в месте разъемного соединения (рис. 3). Механическое торцевое соединение двух волокон приводит к оптическим потерям в виде обратного френелевского отражения, на основе которого возможно формирование утечки. Величина потерь для современных разъемов составляет порядка 0,75 дБ [19, 20]. В зависимости от вида рассогласования величина потерь варьируется и дается выражениями [19, 20]:

$\alpha_\Theta = 10 \cdot \lg\left(1 - \frac{2n_0}{NA} \cdot \frac{\Theta}{\pi}\right)$ — для углового рассогласования на угол Θ;

$\alpha_s = 10 \cdot \lg\left(1 + \frac{s}{a} \cdot \mathrm{tg}\left[\arcsin\frac{NA}{n_0}\right]\right)$ — для неплотного соединения волокон с промежутком s;

$\alpha_d = 10 \cdot \lg\left(1 - \frac{2}{\pi} \cdot \frac{d}{a}\right)$ — для радиального смещения между ступенчатыми волокнами на расстояние d.

Здесь введены обозначения:

a — диаметр сердцевины оптического волокна;

n_0 — показатель преломления иммерсионного слоя в стыке между волокнами;

NA — числовая апертура волокна.

При воздействии звука геометрические параметры соединения Θ, s, d изменяются в зависимости от уровня звукового давления, что вызывает модуляцию отраженного и проходящего света. Оценим величину коэффициента модуляции света CML. В зависимости от вида разъема, материала и других параметров каждый из механизмов будет давать различные вклады. Во-первых, имеем модуляцию интенсивности света при радиальном смещении внутри соединения, для которого

$$CML_d = \frac{2}{\pi} \cdot \frac{\delta d}{a},$$

здесь δd — изменение радиального смещения между волокнами при воздействии акустического поля. Второй вклад в модуляцию света в волноводе по порядку величины, близкий к CML_d, будет давать механизм, связанный с неплотным соединением, определяемый выражением

$$CML_s = \frac{\delta s}{a} \cdot \mathrm{tg}\left[\arcsin\frac{NA}{n_0}\right],$$

где δs — изменение расстояния между волокнами при воздействии акустического поля.

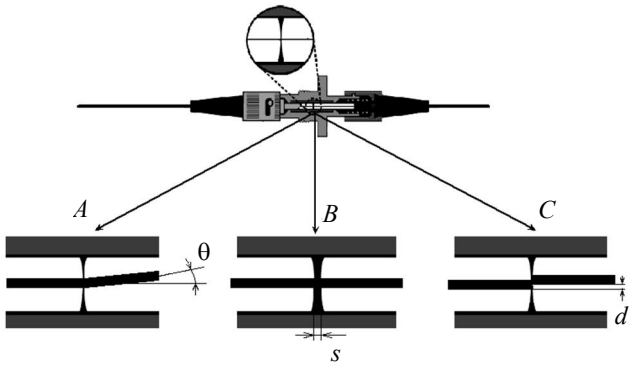

Рис. 3. Схематическое изображение разъемного соединения с возможными не идеальностями в оптическом соединении:

A — угловое рассогласование с углом θ; *B* — неплотное соединение с расстоянием между волокнами *s*; *C* — радиальное смещение на расстояние *d*

Представленные выше два механизма модуляции дают наибольший вклад для одномодовых разъемных соединений, что связано с обратной зависимостью коэффициентов CML_d и CML_s от диаметра сердцевины волокна a, которая для многомодового на порядок выше, чем у одномодового волокна. Если принять для одномодовых соединений максимальное смещение вдоль или перпендикулярно оси волокна по порядку величины, равным 0,05 мкм, то коэффициент модуляции может достигать 1 % в обоих случаях.

Вклад угловых рассогласований присутствует в обоих случаях, он определяется упругими свойствами материала и геометрическими размерами фиксирующей соединение втулки. Его величина определяется выражением

$$CML_{\Theta} = \frac{2n_0}{NA}\frac{\delta\Theta}{\pi},$$

здесь $\delta\Theta$ — изменение углового рассогласования при акустическом воздействии. Постоянный множитель в выражении имеет величину порядка $(2n_0/NA) = 5$, что выше, чем в предыдущих механизмах. Таким образом, при угловых колебаниях (дрожаниях) порядка 0,01 от π получим CML_{Θ} = = 1 %.

Кроме представленных механизмов возможны и другие, связанные с неидеальной согласованностью параметров волокон [19, 20], таких как неодинаковые показатели преломления соединяемых волокон, различия числовых апертур, различие диаметров сердцевин, которые усиливают потери и могут оказать существенное влияние и на глубину модуляции.

Бюджет канала связи в оптоволокне определяется оптическим затуханием, которое можно принять, равным 0,5 дБ/км.

Определим предельное расстояние, на котором простейшее фотоприемное устройство, типа волоконно-оптический тестер-телефон "Рубин-021" [21, 22], может регистрировать переговоры. Мощность оптического источника света тестера составляет 0,1 мВт (−10 дБм), чувствительность приемника равна 10^{-10} Вт (−70 дБм). Для простейшего приема речи требуется динамический диапазон порядка 20 дБ, поэтому минимальное значение мощности на входе фотоприемника, соответствующее максимальной громкости, будет 10^{-8} Вт (−50 дБм). Таким образом, бюджет канала связи для тестера "Рубин-021" составит −10 дБм + 50 дБм = 40 дБм и тогда с учетом глубины модуляции 1 % (−20 дБ) получим предельную длину оптического кабеля порядка 20 дБ/0,5 дБ/км = 40 км.

Определим эффективность канала утечки CEL. Обычный разговор имеет превышение уровня звукового давления речи над уровнем шума порядка 20 дБ, что соответствует уровню спокойного разговора 65 дБ при шуме 45 дБ, следовательно, имеем $SNR_{\text{in}} = 100$. Вычисление $SNR_{\text{out}} = (SNR_{\text{in}} / /CNL)$ требует знания коэффициента шума канала утечки CNL, способ расчета которого будет рассмотрен в последующих работах. Пока произведем обратную оценку — по ранее полученным результатам измерения разборчивости речи 0,5 = CEL при тех же условиях [16, 17]. По графику на рис. 2 для CEL = 0,5 получаем $SNR_{\text{out}} = 1,4$, что соответствует $CNL \approx 70$. Основное зашумление канала происходит на стадии модуляции света звуком. На остальных элементах зашумление минимально, что связано с высокими качествами по передаче сигнала по волоконно-оптическому каналу, шумы которого минимальны.

Заключение

Таким образом, на основе представленных исследований можно провести оценку параметров акустооптоволоконного канала утечки речевой информации. Безопасным можно считать канал утечки с коэффициентом модуляции не выше CML = = 0,1 %, коэффициентом шума не ниже CNL = 100 (20 дБ), тогда эффективность канала утечки не превысит CEL = 40 %. Бюджет канала утечки можно принять равным CLL = 20 дБ. Представленные оценочные значения характеристик акустооптоволоконного канала утечки показывают его высокую опасность для подслушивания. Надо отметить, что полученные оценки можно экстраполировать и на другие инженерно-технические каналы утечки.

На основе технических параметров канала связи выбраны характеристики, наиболее полно отвечающие оценке параметров канала утечки и адаптированные для практических расчетов. В качестве примера проведена оценка характеристик акустооптоволоконного канала утечки.

Литература

1. *Ярочкин В. И.* Информационная безопасность: Учеб. пособие для не профильных вузов. — М.: Международные отношения, 2000. — 400 с.

2. *Торокин А. А.* Инженерно-техническая защита информации: Учеб. пособие. — М.: Гелиос АРВ, 2005. — 960 с.

3. *Хорев А. А.* Техническая защита информации: Учеб. пособие для студ. вузов в 3 т. Том 1. Технические каналы утечки информации. — М.: НПЦ "Аналитика", 2008. — 436 с.

4. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных: В 2-х кн. — М.: Энергоатомиздат, 1994.

5. *Железняк В. К.* Защита информации от утечки по техническим каналам: Учеб. пособие. — Санкт-Петербург: ГУАП, 2006. — 188 с.

6. *Атоманов Г. А.* Технические каналы утечки информации: определение, сущность, классификация// Защита информации. 2010. № 1. С. 28–33.

7. *Платонов В. В.* Оценка эффективности средств интегрированной защиты информации комплексных систем безопасности объектов// Вопросы защиты информации, 2008. № 2. С. 38–40.

8. *Рогозин Е. А., Ланкин О. В., Багаев Д. А.* Способ определения комплексного показателя защищенности автоматизированных систем// Там же. 2009. Вып. 2. С. 8–10.

9. *Скляр Бернард.* Цифровая связь. Теоретические основы и практическое применение: 2-е изд.: пер. с англ. — М.: Изд. дом "ВИЛЬЯМС", 2003. — 1104 с.

10. *Прокис Джон.* Цифровая связь: Пер. с англ./ Под ред. Д. Д. Кловского. — М.: Радио и связь, 2000. — 800 с.

11. *Рид Ричард.* Основы теории передачи информации: Пер. с англ. — М.: Изд. дом. "Вильямс", 2005. — 320 с.

12. *Харкевич А. А.* Борьба с помехами: изд. 3-е — М.: Книжный дом "ЛИБРОКОМ", 2009. — 280 с.

13. *Шестов Н. С.* Выделение оптических сигналов на фоне случайных помех/ Под ред. акад. А. А. Лебедева. — М.: Сов. радио, 1967. — 348 с.

14. *Белоусов А. П., Каменецкий Ю. А.* Коэффициент шума. — М.: Радио и связь, 1981. — 112 с.

15. *Гришачев В. В., Косенко О. А.* Практическая оценка эффективности канала утечки акустической (речевой) инфор-

мации через волоконно-оптические коммуникации// Вопросы защиты информации. 2010. № 2. С.18—25.

16. *Гришачев В. В., Халяпин Д. Б., Шевченко Н. А.* Анализ угроз утечки речевой информации через волоконно-оптические коммуникации// Там же. 2008. № 4. С. 12—17.

17. *Гришачев 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.

18. *Кунце Х.-И.* Методы физических измерений: пер. с нем. — М.: Мир, 1989. — 216 с.

19. *Листвин А. В., Листвин В. Н.* Рефлектометрия оптических волокон. — М.: ВЭЛКОМ, 2005. — 208 с.

20. *Калинин В. А., Пресленев Л. Н.* Оптические волокна и пассивные компоненты волоконно-оптических линий связи: Учеб. пособие. — СПб: ГУАП, 2008. — 80 с.

21. Тестер волоконно-оптический "Рубин-021". Руководство по эксплуатации РВПИ.204125.001 РЭ. — С.-Петербург, 2005. — 21 с.

22. *Рудницкий В. Б., Сумкин В. Р.* Современные волоконно-оптические телефоны.— М.: Фотон-Экспресс, 2005. № 8(48). С. 42—44.

Quantitative estimation of efficiency convert channel on technical parameters of communication channels

V.V. Grishachev, O. A. Kosenko

The Institute of Information Sciences and Security Technologies, RSUH, Moscow, Russia

On the basis of standard characteristics by definition of channels functioning quality of an information transfer the parameters set on estimations of effective convert channel is offered. Calculation methods of parameters for practical use are offered at the description of a various kind and the nature covert channel.

Keywords: data object protection, covert channel, and effective convert channel.

Гришачев Владимир Васильевич, доцент.
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