ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВОЗМОЖНОЙ УТЕЧКИ ИНФОРМАЦИИ

УДК 004.056

Методика оценки параметров технического канала утечки информации

В. В. Гришачев, канд. физ.-мат. наук
Российский государственный геологоразведочный университет (РГГРУ), Москва, Россия

Предложен метод оценки эффективности технического канала утечки информации на основе расчета вероятности прохождения бита информации для различных видов представления информации при передаче.

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

Построение защиты объекта информатизации связано с решением многих задач, одной из которых является выявление технических каналов утечки информации и применение инженерно-технических средств защиты для их подавления [1–3]. Эффективное решение подобной задачи требует разделения обнаруженных каналов утечки по уровню угроз, невозможное без теоретической оценки опасности каналов утечки. Как правило, для оценки используются вероятностные методы, в которых на основе специально введенных коэффициентов определяется уровень защищенности объекта. Разработка простых и понятных техническим специалистам методов по оценке опасности каналов утечки является важной задачей, которой и посвящена данная работа.

Технический канал утечки информации представляет собой совокупность объекта технической разведки, физической среды и средства технической разведки, которыми добываются разведывательные данные [1–3]. Обобщенная структурная схема функциональных связей элементов канала (рис. 1) показывает, каким образом информация передается от источника 1, обладателя конфиденциальной информации, к адресату 6, получателю информации, злоумышленнику. Принципы функционирования канала зависят от формы представления информации, как правило, это физическое поле, в котором содержится информация (оптическое изображение объекта, речь человека, данные в коммуникациях). Для передачи информации от источника к адресату требуется передатчик 2, устройство, с помощью которого информация преобразуется в вид, необходимый для ввода в канал утечки. Преобразование в сигнал осуществляется посредством генерации или модуляции физических полей, существующих в канале связи 3, среде, через которую происходит передача. В качестве таковой выступает окружающая среда, естественный или искусственный волновод и т. д., проходя который сигнал поступает в приемник 5. Устройством вывода информации из канала связи является демодулятор, преобразующий принятый сигнал в информацию для получателя.

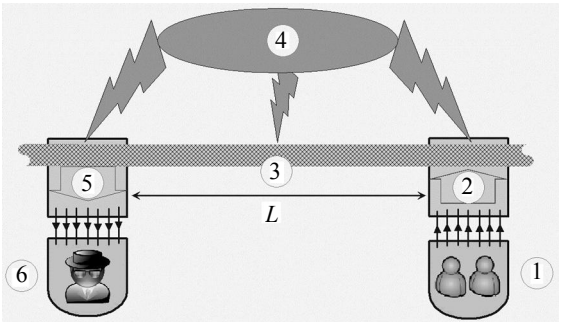

Рис. 1. Обобщенная структура канала утечки информации

Функционирование канала утечки сопровождается помехами 4 — случайными воздействиями на передатчик, канал связи и приемник, связанные с преобразованием, передачей и регистрацией информации и создающие зашумление полезного сигнала [4–6]. Помехи приводят к изменениям условий прохождения сигнала и, как следствие, к его искажению, разрушению, в результате доля полезной информации, дошедшей до получателя, сокращается, а доля потерянной растет. На основании подобных рассуждений можно ввести понятие эффективность технического канала утечки информации как доли, дошедшей до получателя полезной информации от всей поступившей. Тогда основным элементом, влияющим на эффективность, будет воздействие помех.

Характеристики технических каналов утечки информации

Все каналы утечки в общем случае по форме передаваемой информации можно разделить на два вида — вещественный и полевой канал. Каждый из видов имеет свои методы оценки эффективности канала утечки информации и защиты от формирования [1—3]. К первому виду утечки относится такой способ, как вынос за пределы охраняемой зоны бумажных, электронных носителей конфиденциальной информации, устный пересказ человеком важных сведений и т. д. Особенностью информации для подобных каналов утечки является вещественность существования, стабильность во времени и пространстве, передача от источника к получателю через подвижные объекты. Основной способ противодействия таким утечкам — организационно-технические меры. Ко второму виду относится утечка информации в виде физических полей, таких как аудио- и видеоинформация в форме акустического и оптического полей, информация в виде электромагнитного, акустического, гравитационного полей, радиационных излучений и т. д., как правило, это технические каналы утечки информации.

Особенность информации для каналов утечки в форме физических полей — изменяемость во времени, непрерывность движения (распространения), связанное с ним рассеяние энергии и зашумление. У этого вида каналов утечки существует время (t_0) начала передачи, продолжительность (τ) передачи и время достижения пункта назначения (t_1), за промежуток времени инфор-мация оказывается на расстоянии $L = c\cdot(t_1-t_0)$, где c — скорость распространения сигнала в среде. В полевой форме информация связана с параметрами поля, основной характеристикой которого является мощность сигнала P и шума N, что определяется необходимостью регистрации информации получателем в реальном времени. Исходные параметры сигнала играют важную роль для оценки эффективности канала утечки. В первую очередь это отношение сигнал/шум (SNR_{in}), характеризующее соотношение между информационной и шумовой составляющими в сигнале: чем выше отношение, тем надежнее выделение полезной информации, и, наоборот, уменьшение SNR_{in} (менее единицы) делает выделение трудно выполнимым [4]. Другой характеристикой исходного сигнала является динамический диапазон (SDR). Он показывает, с какими ограничениями связана передача сигнала для его приема без искажений. При распространении сигнала через среду канала утечки и при регистрации искажения не должны превышать некоторых значений, определяемых возможностью надежного, без искажений и потерь, выделения полезного сигнала.

Эффективность канала утечки информации зависит от модуляции или генерации под действием исходного сигнала потоков энергии в среде канала, от свойств среды, через которую проходит сигнал, так что основные параметры сигнала на выходе изменяются [5]. Мощность и динамический диапазон сигнала на выходе влияют на разрешающую способность регистрирующей аппаратуры технических средств разведки, поэтому основным параметром для оценки эффективности канала утечки информации является отношение сигнал/шум на выходе канала SNR_{out}. Его значение определяется коэффициентом шума CNL = (SNR_{in}/SNR_{out}), показывающим, во сколько раз увеличилась доля шума в сигнале при прохождении через канал утечки. Другими параметрами, определяемыми техническими средствами разведки, являются коэффициенты модуляции (CML) и потерь (CLL) в канале утечки. При воздействии исходного сигнала на среду канала утечки происходит либо генерация (преобразование) сигнала с CML = 1, либо модуляция проходящих потоков энергий по параметрам поля с CML ≤ 1. Уровень потерь задает, во сколько раз мощность сигнала на выходе уменьшилась по отношению к сигналу на входе. Значения CML и CLL влияют на параметры приемной аппаратуры, разрешающая способность которой должна быть таковой, чтобы разрешить мощность по уровню не более

$$\sigma = P_{in}\frac{\mathrm{CML}}{\mathrm{CLL}\cdot\mathrm{SDR}}, \qquad (1)$$

где P_{in} — мощность сигнала на входе канала утечки, т. е. генерируемая или проходящая мощность потока, σ — разрешающая способность по мощности приемного оборудования, коэффициенты SDR, CML и CLL выражаются в безразмерных единицах.

Выбранные параметры SNR_{in}, SNR_{out}, SDR, CNL, CML и CLL достаточно полно характеризуют свойства канала утечки, но более информативно описание дается некоторым оценочным коэффициентом, который будет связывать между собой все или практически все приведенные параметры. Эффективность функционирования можно задать по вероятности прохождения отдельного бита информации через канал утечки [6], который назовем коэффициентом эффективности канала утечки информации (CEL) и определим как

$$\mathrm{CEL} = \frac{H_x}{H_0} = 1 - \frac{\Delta H}{H_0}, \qquad (2)$$

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.

Вычисление CEL зависит от формы предоставления информации. Это может быть цифровая кодировка с бинарным представлением сигнала, применяемая для передачи данных, имеющим два уровня мощности сигнала — нижним (0) и верхним (1) уровнями. Случайный сигнал от измерительных приборов, различных преобразователей, где уровень сигнала произвольно меняется в широких пределах, определяется динамическим диапазоном SDR. Другой тип — чисто аналоговый сигнал — является промежуточным между случайным и цифровым, имеющими разные вероятности изменения уровня сигнала в сообщении. Например, к аналоговым сигналам относится речь человека, изображения предметов и т. д. Для каждой формы представления сигнала требуется ввести свое оценочное выражение.

Описание работы цифрового канала утечки дается по принципам функционирования цифровых линий связи [5], в которых одним из основных параметров является вероятность появления ошибочного бита (BER). Учитывая определение для CEL, можно получить CEL = 1−BER, и тогда для цифрового представления сигнала утечки будем иметь оценочную формулу

$$\mathrm{CEL} = 0{,}5 \cdot \left[1 + \mathrm{erf}\left(0{,}35 \cdot \mathrm{SNR}_{out}\right)\right], \qquad (3)$$

которая находится по методам определения BER для цифрового канала связи. Эффективность канала утечки с цифровым представлением сигнала не может быть меньше 0,5, что связано с необходимостью выбора только между двумя уровнями, соответствующими либо нулю, либо единице.

Случайный сигнал утечки характеризуется амплитудой в данный момент времени. Пусть на входе имеем полный сигнал вместе с шумами $P_{in}+N_{in}$ с отношением сигнал/шум SNR_{in}, а на выходе — $P_{out}+N_{out}$ с отношением сигнал/шум SNR_{out}. В уровне сигнала содержится информация, выраженная в двоичном коде объемом $\log_2\left((P_{in}+N_{in})/\sigma\right)$, а шумы создают неопределенность с объемом информации $\log_2\left(N_{in}/\sigma\right)$, где σ — разрешающая способность регистрирующего оборудования. Таким образом, объем полезной информации на входе канала утечки можно определить по формуле $H_0 = \log_2\left(1+\mathrm{SNR}_{in}\right)$. Аналогично объем информации, регистрируемый на выходе канала утечки, составит $H_x = \log_2\left(1+\mathrm{SNR}_{out}\right)$.

Таким образом, эффективность канала утечки информации для случайного сигнала утечки можем определить по формуле

$$\mathrm{CEL} = \frac{\ln\left(1+\mathrm{SNR}_{out}\right)}{\ln\left(1+\mathrm{SNR}_{in}\right)} = \frac{\ln\left(1+\mathrm{SNR}_{in}/\mathrm{CNL}\right)}{\ln\left(1+\mathrm{SNR}_{in}\right)}, \qquad (4)$$

где переход к натуральным логарифмам произведен на основании свойств отношения логарифмов.

Промежуточный между цифровым и случайным сигналами канала утечки аналоговый сигнал не может корректно описываться ни одной из предложенных формул, что связано с отмеченными выше его особенностями [6]. Но по своей сути он ближе к цифровому сигналу, так как в обоих случаях существует предопределенность регистрируемого уровня. Если в цифровом — это только два уровня, то в аналоговом — предопределенность вытекает из связанности между собой всех и в первую очередь соседних уровней. В аналоговом сигнале неопределенность удваивается из-за выбора не между двух уровней, а трех — находясь на исходном уровне, следующий по времени уровень может быть как меньше, так и больше. В этом случае можно предложить следующую формулу для оценки эффективности канала со связями внутри сигнала

$$\mathrm{CEL} = 1 - 2 \cdot \mathrm{BER} = \mathrm{erf}\left(0{,}35 \cdot \mathrm{SNR}_{out}\right). \qquad (5)$$

Из приведенных формул по оценке эффективности функционирования каналов утечки информации следует зависимость всех видов каналов утечки от отношения сигнала к шуму на выходе SNR_{out} или от отношения сигнала к шуму на входе SNR_{in} и коэффициента шума канала CNL.

Сравнение коэффициентов эффективности каналов утечки информации

Выражение для коэффициента эффективности канала с цифровым сигналом утечки является прямым следствием расчетов вероятности появления ошибочного бита в обычной цифровой системе связи. В обычном канале связи SNR_{out} больше 5, а коэффициент шума близок к 1, для канала утечки отличие сводится к более близкому к единице значению SNR_{out}.

Выражения для случайного и аналогового сигналов каналов утечки менее очевидны и требуют сравнительного анализа. На рис. 2 представлены графики зависимостей коэффициента эффективности от отношения сигнал/шум на выходе для разных видов каналов утечки, а на рис. 3 — графики зависимостей коэффициента эффективности от коэффициента шума для аналогового сигнала канала утечки. Из графиков на рис. 2 видно, что для аналогового сигнала канала утечки зависимость имеет пороговый вид, определяется отношением сигнал/шум на выходе канала и не зависит от свойств исходного сигнала и среды распространения. Эффективность канала утечки быстро растет от 38 до 87 % при увеличении SNR_{out} от 1 до 3 независимо от предыстории сигнала. Превышение отношения сигнал/шум более 5 позволяет получить более 99 % информации, а уменьшение ниже 0,5 — менее 20 %. В области SNR_{out} менее 1 получение достоверной информации затруднено, так как связи между отдельными частями нарушаются.

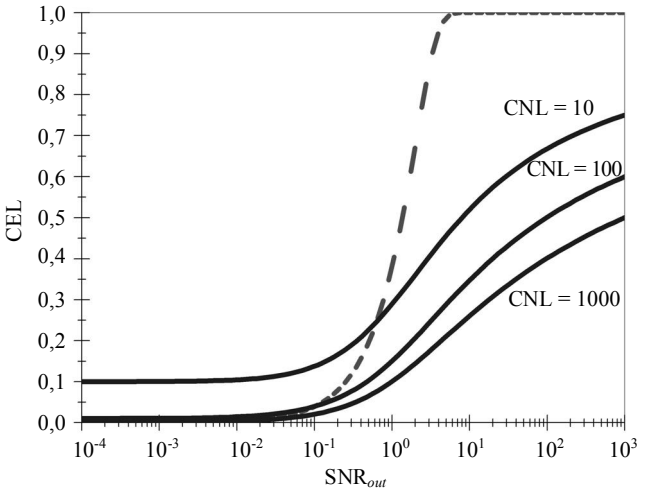

Рис. 2. Сравнение приближений для вычисления коэффициента эффективности случайного (сплошная линия) и аналогового (пунктирная линия) сигналов каналов утечки информации в зависимости от выходного отношения сигнал/шум

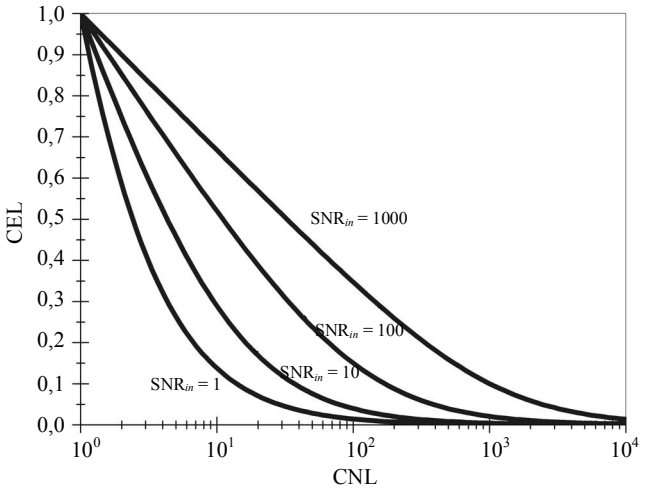

Рис. 3. Зависимость коэффициента эффективности от коэффициента шума случайного сигнала канала утечки информации при фиксированном входном отношении сигнал/шум

Эффективность канала со случайным сигналом утечки имеет похожий ход зависимости от отношения сигнал/шум — с ростом отношения растет эффективность, но при этом на зависимость сильное влияние оказывает предыстория сигнала, зашумление при прохождении канала утечки. Это можно объяснить тем, что нахождение неизвестного уровня сигнала определяется влиянием не только аддитивного шума, который добавляется к сигналу по пути распространения, но и мультипликативным шумом, состоящим из потерь и вносимых искажений в сам сигнал при его распространении из-за взаимодействия со средой канала. В аналоговом сигнале мультипликативная составляющая шума уменьшается связями внутри сообщения, а в случайном сигнале утечки такие связи отсутствуют, так как имеет значение абсолютная величина сигнала в данный момент времени, никак не связанная с другими измерениями в другие моменты времени. Это приводит к сильной зависимости эффективности канала со случайным сигналом утечки от коэффициента шума, что показано на графике рис. 3. Отличительной особенностью случайного сигнала канала утечки является значительно меньший рост эффективности при увеличении отношения сигнал/шум на выходе, чем у канала с аналоговым сигналом утечки. Еще одно отличие состоит в том, что чем больше коэффициент шума, тем меньше рост коэффициента эффективности. Даже при отношении сигнал/шум на выходе канала утечки SNR_{out} = 30 дБ, но при сильно шумящем канале с коэффициентом шума CNL = 30 дБ получаем коэффициент эффективности CEL < 50 %. В этом примере отношение сигнала к шуму на входе составляет 60 дБ, т. е. имеем высококачественный сигнал, но в неэффективном канале утечки с большими шумами сигнал теряет 50 % своей информативности, которую невозможно восстановить.

Обсудим применение всех трех приближений к получению акустической информации при прослушивании комнаты с людьми, ведущими переговоры [1—3]. Выберем три вида информации, соответствующей трем приближениям:

цифровой сигнал канала утечки — шаги, вход или выход переговорщиков с открыванием и закрыванием двери, перемещение предметов и другие действия малой продолжительности и высокого уровня звукового давления;

аналоговый сигнал канала утечки — речь переговорщиков;

случайный сигнал канала утечки — посторонние по отношению к разговору звуки, такие как сопровождающие работу вентиляции, приборов и другие, не имеющие смысловой нагрузки, но с изменяющейся тональностью, продолжительностью, уровнем звукового давления.

Как видно из представленного анализа возможного подслушивания, для каждого вида звуков требуется применение своей формулы для оценки эффективности.

Проведенные исследования позволяют задать некоторый алгоритм оценки технического канала утечки информации на эффективность для последующей выработки мер по организационной и инженерно-технической защите информации [1—3]. Алгоритм включает следующие процедуры:

определение вида и возможных параметров сигнала утечки: отношение сигнал/шум (SNR_{in}), динамический диапазон сигнала (SDR);

определение возможных параметров технических средств разведки: средняя мощность зондирующего энергетического потока (P), разрешающая способность приемника (σ);

определение параметров канала утечки: коэффициент модуляции (CML), коэффициент потерь (CLL), коэффициент шума (CNL);

определение интегральных характеристик канала утечки: длина (L), отношение сигнал/шум на выходе (SNR_{out}), коэффициент эффективности (CEL).

В предложенной схеме учитывается минимальное число параметров технических средств разведки, так как их увеличение значительно усложнит оценку. Итоговых характеристик канала утечки вполне достаточно для оценки общих угроз системе защиты информации. Понижение уровня опасности можно произвести по третьему пункту алгоритма, т. е. путем изменения параметров канала утечки с помощью инженерно-технических средств защиты.

Заключение

На основе анализа цифровых каналов связи предложены оценочные формулы для вычисления эффективности канала утечки информации по вероятности прохождения бита информации. Выражения адаптированы для различного вида представления информации при передаче в форме цифрового, аналогового и случайного сигналов канала утечки.

Литература

1. *Хорев А. А.* Техническая защита информации: Том 1. Технические каналы утечки информации. — М.: НПЦ "Аналитика", 2008. — 436 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. *Шереметьев А. Г.* Когерентная волоконно-оптическая связь. — М.: Радио и связь, 1991. — 192 с.
5. *Скляр Бернард.* Цифровая связь. Теоретические основы и практическое применение. — М.: ВИЛЬЯМС, 2003. — 1104 с.
6. *Гришачев В. В., Косенко О. А.* Практическая оценка эффективности канала утечки акустической (речевой) информации через волоконно-оптические коммуникации // Вопросы защиты информации. 2010. № 2. С. 18—25.

Estimation method of technical convert channel characteristic

V. V. Grishachev

Russian State Geological Prospecting University (RSGPU), Moscow, Russia

In the work is proposed evaluation procedure of efficient factor of technical convert channel on basis of propagation information bit probability calculation for any kind of data representation during transmission.

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

Гришачев Владимир Васильевич, доцент.
E-mail: grishachev@mail.ru