

УДК 004.056.53

МЕТОДИКА ЗАЩИТЫ ПОМЕЩЕНИЙ ОТ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Е.П. Аншакова, А.К. Чернышов

В статье описана методика организации защиты речевой информации от утечки по техническим каналам для помещений, в которых эта информация циркулирует. При проведении подобных работ по защите информации могут возникнуть проблемы выбора из множества альтернативных методов решения этой задачи. В статье предлагается использовать инструментально-расчетный метод измерения разборчивости речи Н.Б. Покровского и метод анализа иерархии.

Ключевые слова: речевая информация, технический канал утечки информации, разборчивость речи, метод анализа иерархий, методы защиты, оценка эффективности

Key words: speech information, technical channel of information leakage, speech intelligibility, hierarchy analysis method, protection methods, efficiency evaluation.

В настоящее время актуальность защиты речевой информации от утечки по техническим каналам неоспорима. Особенно это касается обсуждения информации ограниченного доступа при проведении совещаний, переговоров и т.п. в коммерческих и государственных структурах. Однако при многообразии и широком ассортименте на российском и международном рынках технических средств защиты, различных по качеству, сложности и стоимости, единых методик по выбору оптимального комплекса средств защиты и оценке эффективности реализованных мер не существует.

В данной статье предлагается методика организации защиты речевой информации от утечки по техническим каналам для помещений, в которых эта информация циркулирует.

Первым этапом методики проведения мероприятий по защите помещений от утечки речевой информации по техническим каналам является определение риска утечки информации. Оценка рисков и выражение их в денежной форме необходимы, прежде всего, для принятия решения о целесообразности внедрения мер по обеспечению безопасности, их состава и направленности.

Вероятность реализации угрозы может быть оценена по статистическим данным, если на предприятии ведется статистика по нарушениям информационной безопасности. При отсутствии статистических данных зачастую трудно определить вероятности того или иного события. Большинство предприятий не ведет учета нарушений безопасности и не имеет данных, характеризующих эти нарушения. Поэтому при оценке вероятности нарушения безопасности целесообразно использовать косвенные методы оценки. В качестве таких оценок могут выступать, например, метод ALE (Annualized Loss Expectancy), метод компании IBM [2] и т.п.

На втором этапе необходимо оценить вероятность использования злоумышленником того или иного технического канала утечки информации (ТКУИ). Она может быть оценена по статистическим данным (если таковые имеются) либо с применением одного из методов оценки с привлечением экспертов. В данной методике предлагается использовать метод анализа иерархий.

ПРИКАСПИЙСКИЙ ЖУРНАЛ:

управление и высокие технологии № 1 (9) 2010

Метод анализа иерархий (МАИ) – математический инструмент системного подхода к сложным проблемам принятия решений [1]. МАИ не предписывает лицу, принимающему решение, какого-либо «правильного» решения, а позволяет ему в интерактивном режиме найти такой вариант (альтернативу), который наилучшим образом согласуется с его пониманием сути проблемы и требованиями к ее решению. МАИ позволяет понятным и рациональным образом структурировать сложную проблему принятия решений в виде иерархии, сравнить и выполнить количественную оценку альтернативных вариантов решения.

Простейшая иерархия содержит три уровня: цель, критерии и альтернативы. Числа на рис. показывают приоритеты элементов иерархии с точки зрения цели, которые вычисляются в МАИ на основе парных сравнений элементов каждого уровня относительно связанных с ними элементами вышерасположенного уровня. Приоритеты альтернатив относительно цели (глобальные приоритеты) вычисляются на заключительном этапе метода путем линейной свертки локальных приоритетов всех элементов. Лучшей считается альтернатива с максимальным значением приоритета.

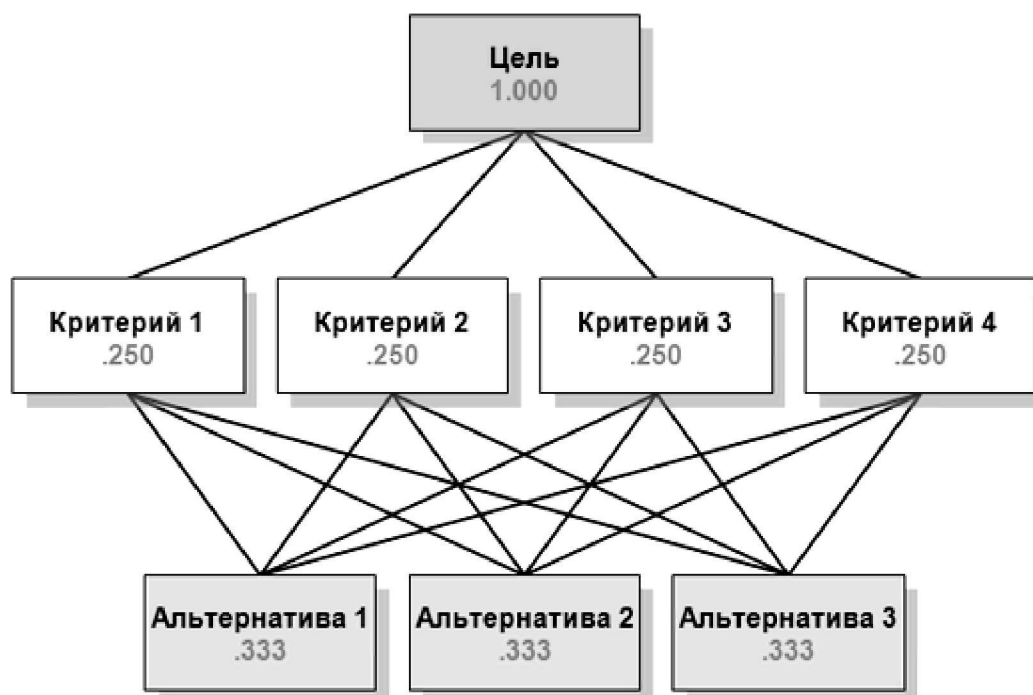


Рис. Схема простейшей иерархии с приоритетами, определенными по умолчанию

Наиболее важной частью МАИ является формирование критериев оценки. В данном случае, например, для малых предприятий, могут быть предложены следующие критерии по оценке вероятности реализации ТКУИ: дешевизна аппаратуры снятия информации; помехоустойчивость ТКУИ; простота изготовления аппаратуры кустарным способом; простота настройки аппаратуры снятия информации и т.п.

В данном случае альтернативами являются каналы утечки речевой информации, которые в зависимости от физической природы возникновения информационных сигналов, среды их распространения и способов перехвата разделяются на прямой акустический, виброакустический, акустооптический (лазерный), акустоэлектрический и акустоэлектромагнитный (параметрический).

ЗАЩИТА ИНФОРМАЦИИ

Если $A_1 \dots A_n$ – множество из n элементов, в качестве которых будут выступать критерии сравнений или ресурсов, тогда $W_1 \dots W_n$ – их взаимные оценки, которые соотносятся следующим образом:

$$W = \begin{matrix} & A_1 & \dots & A_n \\ \begin{matrix} A_1 \\ \dots \\ A_n \end{matrix} & \begin{pmatrix} 1 & \dots & W_1/W_n \\ \dots & 1 & \dots \\ W_n/W_1 & \dots & 1 \end{pmatrix} \end{matrix}$$

Оценка компонент вектора приоритетов производится по схеме:

$$X_1 = \left(1 \cdot \frac{W_1}{W_2} \cdot \dots \cdot \frac{W_1}{W_n}\right)^{\frac{1}{n}}$$

...

$$X_n = \left(\frac{W_n}{W_1} \cdot \dots \cdot \frac{W_n}{W_{n-1}} \cdot 1\right)^{\frac{1}{n}}$$

Веса по отдельным критериям рассчитываются по формуле:

$$W(A_i) = \frac{X_i}{\sum_i X_i}$$

Сравнения вероятностей влияния основных критериев на возможность снятия информации по соответствующему ТКУИ, производится по шкале:

- 1 – равная важность;
- 3 – умеренное превосходство;
- 5 – существенное превосходство;
- 7 – значительное превосходство;
- 9 – очень сильное превосходство;
- 2, 4, 6, 8 – промежуточные значения.

После получения весовых коэффициентов, которые в данном случае могут рассматриваться как вероятности использования ТКУИ, следует определить допустимый уровень вероятности, ниже которого угрозу утечки по данному каналу следует считать несущественной. Для всех существенных угроз необходимо выбрать средства защиты.

При осуществлении третьего этапа проводится оценка разборчивости речи в местах вероятного расположения средств съема речевой информации. Для этого используется инструментально-расчетный метод, основанный на результатах экспериментальных исследований [5], проведенных Н.Б. Покровским: числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала и шума в местах предполагаемого расположения датчиков аппаратуры акустической разведки.

Суть метода заключается в следующем. Спектр речи разбивается на пять октавных частотных полос. Для каждой i -й частотной полосы на среднегеометрической частоте

$$f_{с.і} = \sqrt{f_{г.і} \cdot f_{н.і}}$$

определяется формантный параметр ΔA_i , характеризующий энергетическую избыточность дискретной составляющей речевого сигнала (дБ):

$$\Delta A_i = L_{ср.і} - A_i = \Delta A(f_{ср.і}).$$

где $L_{cp,i}$ – средний спектральный уровень речевого сигнала в месте измерения в i -той спектральной полосе, дБ; A_i – средний спектральный модальный уровень формант в i -той спектральной полосе, дБ;

Значения формантных параметров определяются из соотношения:

$$\Delta A(f) = \begin{cases} \frac{200}{f^{0,37}} - 0,37, \text{ если } f \leq 1000 \text{ Гц} \\ 1,37 + \frac{1000}{f^{0,69}}, \text{ если } f > 1000 \text{ Гц} \end{cases}$$

Для каждой i -й частотной полосы определяется весовой коэффициент k_i , характеризующий вероятность наличия формант речи в данной полосе:

$$k_i = k(f_{\bar{e},i}) - k(f_{\bar{n},i}),$$

где $k(f_{\bar{e},i})$ и $k(f_{\bar{n},i})$ – значения весового коэффициента для верхней и нижней граничной частот i -й частотной полосы спектра речевого сигнала.

Значения весовых коэффициентов могут быть определены из следующего соотношения при условии, что $f = f_{\bar{e},i}$ и $f = f_{\bar{n},i}$:

$$\Delta k(f) = \begin{cases} 2,57 \cdot 10^{-8} \cdot f^{2,4}, & \text{для полосы } 100 \leq f \leq 400 \text{ Гц,} \\ 1 - 1,074 \cdot e^{-10^{-4} \cdot f^{1,18}}, & \text{для полосы } 400 \leq f \leq 10000 \text{ Гц} \end{cases}$$

Для каждой частотной полосы на среднегеометрической частоте из соотношения определяется коэффициент восприятия форманта слуховым аппаратом человека, представляющий собой вероятное относительное количество формантных составляющих речи, которые будут иметь уровни интенсивности выше порогового значения:

$$\Delta p_i = \begin{cases} \frac{0,78 + 5,46 \cdot \exp(-4,3 \cdot 10^{-3} \cdot (27,3 - |Q_i|)^2)}{1 + 10^{0,1 \cdot |Q_i|}}, & \text{для } Q_i \leq 0 \\ 1 - \frac{0,78 + 5,46 \cdot \exp(-4,3 \cdot 10^{-3} \cdot (27,3 - |Q_i|)^2)}{1 + 10^{0,1 \cdot |Q_i|}}, & \text{для } Q_i > 0 \end{cases}$$

где

$$Q_i = A_i - L_{ш,i} = (L_{c,i} - \Delta A_i) - L_{ш,i} = q_{ш,i} - \Delta A_i;$$

$q_i = L_{c,i} - L_{ш,i}$ – отношение «уровень речевого сигнала/уровень шума», дБ. Далее определяется спектральный индекс артикуляции (понимаемости) речи (информационный вес i -й спектральной полосы частотного диапазона речи):

$$R_i = p_i \cdot k_i$$

Тогда интегральный индекс артикуляции речи:

$$R = \sum_i R_i$$

Зависимости словесной разборчивости W от интегрального индекса артикуляции речи R определяется:

$$W = \begin{cases} 1,54 \cdot R^{0,25} \cdot (1 - \exp(-11 \cdot R)), & \text{для } R \leq 0,15 \\ 1 - \exp\left(-\frac{11 \cdot R}{1 + 0,7 \cdot R}\right), & \text{для } R > 0,15 \end{cases}$$

Считается, что перехват речевой информации возможен, если рассчитанное по результатам измерения значение словесной разборчивости речи W превышает 10–20 %.

ЗАЩИТА ИНФОРМАЦИИ

На четвертом этапе формируется множество методов защиты. В качестве примера предлагается использовать методы защиты [4], [5], которые указаны в таблице.

Таблица

**Список средств и способов перехвата и мер противодействия
для каждого из возможных каналов утечки информации**

Канал	Средство или способ перехвата	Меры противодействия
Прямой акустический ТКУИ	Человеческое ухо (прямое подслушивание)	1. Улучшение звукоизоляции. 2. Использование шумления
	Диктофон	1. Мероприятия по обнаружению диктофонов. 2. Применение блокираторов (подавителей) диктофонов и сотовых телефонов. 3. Использование шумления
	Акустические закладные устройства	1. Постановка радиопомех. 2. Использование интерференционного метода подавления предусилителя РЗУ. 3. Мероприятия по отысканию РЗУ
Вибрационный ТКУИ	Электронный стетоскоп	1. Улучшение звукоизоляции. 2. Использование вибрационных генераторов
	Радиостетоскоп	1. Улучшение звукоизоляции. 2. Использование вибрационных генераторов. 3. Постановка радиопомех
Пассивный акустостатический ТКУИ	Микрофонный эффект	1. Отключение источников опасных сигналов. 2. Фильтрация опасных сигналов. 3. Ограничение опасных сигналов. 4. Применение буферных устройств. 5. Линейное шумление. 6. Пространственное шумление
Активный акустостатический ТКУИ	Высокочастотное навязывание	
Пассивный акустостатический ТКУИ	Побочные электромагнитные излучения	1. Экранирование помещений. 2. Экранирование компонентов. Энергетическая и неэнергетическая радиотехническая маскировка (постановка шумовой или заградительной помехи)
Активный акустостатический ТКУИ	Высокочастотное облучение помещения	
Акустооптический (лазерный) ТКУИ	Лазерные акустические системы разведки (ЛАСР)	1. Использование средств, увеличивающих амплитуду вибраций тонких поверхностей

Пятый этап осуществления методики предполагает выбор оптимальных средств защиты и осуществляется изложенным выше методом анализа иерархий. В этом случае в роли альтернатив выступают средства защиты, которые оцениваются по набору критериев, определенных для этой задачи.

Критериями выбора средств защиты могут быть: стоимость; эффективность; наличие сертификации ФСТЭК; совместимость; удобство установки и использования и т.п.

Заключительный, шестой этап предполагает, что после интегрирования системы защиты для оценки эффективности реализованных мер, проводится повторная оценка вероятности утечки речевой информации. Для акустических каналов проводится расчет вероятности утечки речевой информации путем измерения разборчивости речи. Для оценки вероятности использования других ТКУИ может использоваться один из методов экспертных оценок, например ALE. Далее может быть оценен уровень снижения вероятности утечки и снижение уровня рисков, связанных с утечкой речевой информации.

В работе описана последовательность действий по организации защиты речевой информации от утечки по техническим каналам. Методика состоит из следующих этапов:

- оценки вероятного ущерба в случае реализации угрозы;
- определения наиболее вероятных каналов утечки информации;
- оценки разборчивости речевой информации;
- определения мер и способов защиты речевой информации;
- выбора оптимальных средств защиты;
- оценки вероятности утечки речевой информации после внедрения выбранных средств защиты.

Предложенные в статье рекомендации разработаны на основе анализа многочисленных известных методов и могут найти практическое применение в области защиты информации, а также быть полезны руководителям коммерческих организаций, которых волнуют вопросы защиты коммерческой тайны при проведении переговоров.

Библиографический список

1. *Саати, Т.* Принятие решений: метод анализа иерархий : пер. с англ. / Т. Саати. – М. : Радио и связь, 1993. – 278 с.
2. *Семкин, С. Н.* Основы организационного обеспечения информационной безопасности объектов информатизации / С. Н. Семкин, Э. В. Беляков, С. В. Гребенев, В. И. Казачок. – М. : Гелиос АРВ, 2005. – 186 с.
3. *Торокин, А. А.* Основы инженерно-технической защиты информации / А. А. Торокин. – М. : Ось-89, 1998. – 336 с.
4. *Хорев, А. А.* Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А. А. Хорев. – Режим доступа: <http://www.analitika.info/kanalutechki.php>, свободный. – Заглавие с экрана. – Яз. рус.
5. *Хорев, А. А.* К оценке эффективности защиты акустической (речевой) информации / А. А. Хорев, Ю. К. Макаров // Специальная техника. – 2000. – № 5.