ментів й їх легалізацію варто погодити з юридичною службою.

8. Розробляємо й впроваджуємо метод і засоби аналізу захищеності ресурсів, визначаємо інтервали й призначаємо відповідальних серед штатного персоналу за проведення систематичного контролю створеної системи інформаційної безпеки. Для аналізу програмно-технічних засобів можна застосувати програмні сканери безпеки й впровадити їх у корпоративну систему, а розроблену нормативну документацію приводити у відповідність при змінах характеру й складу бізнес-процесів, змінах архітектури мережі й, з іншого боку, регулярно піддавати створену систему захисту інформації аналізу на відповідність вимогам документації, тобто проводити регулярний внутрішній аудит.

Впровадження розроблених мір займе деякий час, як і підготовка персоналу, перш, ніж захист інформації буде забезпечений на належному рівні. Але є ще кілька питань, від вирішення яких залежить досягнутий рівень захисту інформації.

По-перше, розвиток технологій, у тому числі і тих, які використовують зловмисники, це постійний процес, вимагає й удосконалювання засобів захисту.

По-друге, ніхто не гарантує, що при впровадженні навіть незначних змін і наступної експлуатації корпоративної інформаційної системи в ній не зявляться нові вразливості. На жаль, але, на відміну від розвинених країн, у нашій країні практика страхування інформаційних ризиків поки ще відсутня.

По-третє, неможливо якісно перевірити самого себе.

Висновоки. Єдине рішення – в проведенні періодичного зовнішнього аудиту для підтвердження й підтримки заданого рівня захищеності. Поява "слабкої" ланки в побудованій системі призведе до послаблення системи в цілому. Регламент і регулярність проведення зовнішнього аудита можуть бути визначені в процесі розробки організаційних мір і закріплені у відповідних розпорядницьких документах.

Запропонована послідовність дій визначена виходячи з досвіду провідних компаній, які займаються інформаційною безпекою підприємств із різними формами власності, різних сфер діяльності й різної величини – від декількох робочих місць в одному приміщенні до територіально розподіленої структури з багатотисячним колективом.

Безумовно, даний підхід має деякі недоліки з погляду побудови комплексної системи керування інформаційною безпекою, але це вже інше завдання,

Перевагами запропонованого підходу є:

досягнуто поставлену мету – конфіденційна інформація захищена;

значна частина робіт виконана штатним зацікавленим персоналом;

документовано поточний стан інформаційної системи підприємства;

запропонований підхід дозволив уникнути невиправданої бюрократичної тяганини з розподілом обовязків при виконанні робіт;

гранично знижені витрати на досягнення мети;

створена логічно повязана система захисту інформації;

створено базу для побудови системи інформаційної безпеки;

істотно підвищений рівень безпеки підприємства та держави.

Таким чином, запропонований підхід є раціональним, щодо захисту конфіденційної інформації на підприємствах при застосуванні принципу доцільності витрат на забезпечення даного захисту.

1. Даллес А. Великие шпионы / А. Далес; [пер. с англ. Б.Г. Любарцева]. – Ростов н/Д: Феникс, 1998. – 511 с. 2. Ленков С.В. Методы и средства защиты информации / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с. 3. Петраков А. Информационная безопасность и защита информации / Петраков А., Мельников В, Клейменов С. – М.: Academia, 2008. – 336 с. 4. Курбатов В. Руководство по защите от внутренних угроз информационной безопасности / Курбатов В., Скиба В. – С.Петербург.: Питер, 2008. – 320 с.

Надійшла до редколегії 21.08.09р

УДК 519.676:681.51

С.В. Ленков, д-р техн. наук, проф.,
О.В. Рыбальский, д-р техн. наук, проф.,
В.А. Хорошко, д-р техн. наук, проф.,
Л.П. Крючкова, канд. техн. наук, доц.

ПРИНЦИПЫ БЛОКИРОВАНИЯ СЪЕМА ИНФОРМАЦИИ СПОСОБАМИ ВЧ-НАВЯЗЫВАНИЯ

Запропонована нова концепція захосту акустичної інформації від збору із застосуванням ВЧ-навязування, основана на зміні якостей зондуючого сигналу.

Ключові слова: защита информации, зондирующий сигнал, блокирование.

The new concept of protection of the acoustic information from gathering with application high frequency-imposing based on change of qualities of probing signal is offered.

Keywords: the information protection, probing signal, blocking.

Вступ. Большинству специалистов в области защиты информации известно, что способ снятия акустической информации, получивший название "ВЧ-навязывание", был изобретен в 1945 г. и впервые реализован в "подарке" советских пионеров послу США в СССР А. Гарриману. "Бесценный дар" был выполнен в виде гипсового герба США, принят с благодарностью растроганным послом и размещен на стене его кабинета, где благополучно провисел до 1950 г., поставляя оперативную и стратегическую информацию советскому руководству [1].

С тех пор прошло много лет и способ, изобретенный выдающимся ученым Л.С. Терменом, получил дальнейшее развитие. Были разработаны методы его применения в токопроводящей среде с использованием в качестве пассивной закладки отдельных электрорадиоэлементов (ЭРЭ) электронной техники. В настоящее время такие методы съема акустической информации являются одними из самых перспективных беззаходовых способов ее добывания и имеют тенденцию к дальнейшему развитию.

Однако методы защиты информации от снятия этими способами в концептуальном плане развивались не столь интенсивно. Часть из них основана на обнаружении сигнала внешнего облучения и попытках либо обнаружения и уничтожения резонаторов, либо, если их обнаружение или уничтожение проблематично, постановке активной электромагнитной или акустической помехи. В токопроводящей среде широкое распространение получили фильтры нижних частот, препятствующие попаданию зондирующих ВЧ-сигналов на ЭРЭ технических устройств, способных выполнять роль резонаторов [1]. Но акустическая помеха создает ряд неудобств и не всегда эффективна.

Иногда применяют сплошное экранирование охраняемого помещения [1]. Однако этот метод достаточно дорогой, а его эффективность в ряде случаев также вызывает сомнения.

Казалось бы, что оптимальным, с точки зрения соотношения эффективность/стоимость, было бы применение активной ВЧ-помехи, блокирующей съем информации. Однако здесь возникает ряд сложностей, поскольку зондирующие сигналы ВЧ-навязывания, как правило, излучаются с большой мощностью, имеют узкую полосу частот и острую направленность, а постановщики активной помехи излучают широкополосный шум, позволяющий перекрыть большой диапазон частот. Естественно, что при таких условиях выделение полезного сигнала из шума не является задачей высокой технической сложности.

Использование тех или иных методов и средств защиты определяется характеристиками объекта защиты и аппаратуры разведки, а также требованиями, предъявляемыми к эффективности защиты акустической информации. В качестве показателя для оценки защищенности наиболее часто используют словесную разборчивость речи W.

Для оценки разборчивости речи целесообразно использовать инструментально-расчетный метод, основанный на результатах экспериментальных исследований, проведенных Н.Б. Покровским [2]. Суть этого метода заключается в следующем [2, 3, 4].

Энергетический спектр речи разбивается на N частотных полос, в общем случае произвольной ширины $f = f_{Bi} - f_{Hi}$, (f_{Bi} – верхнее значение частоты i-й полосы; f_{Hi} – нижнее значение частоты i-й полосы).

Для каждой i-й (i = 1, …, N) частотной полосы инструментальным методом измеряются уровень сигнала L_{ci}, дБ и уровень шума (помехи) $L_{\omega i}$, дБ.

Далее для каждой i-й частотной полосы расчетным методом определяется:

1. Отношение "уровень речевого сигнала / уровень шума (помехи)" по формуле

$$g_i = L_{ci} - L_{\omega i}. \qquad (1)$$

2. Формантный параметр A_i, на среднегеометрической частоте полосы характеризующий энергетическую избыточность дискретной составляющей речевого сигнала в полосе, по формуле

$$\Delta A(f_{cpi}) = \begin{cases} 200 / f_{cpi}^{0,43} - 0,37, \\ \text{если } f_{cpi} \le 1000 \text{ Гц} \\ 1,37 + 1000 / f_{cpi}^{0,69}, \\ \text{если } f_{cpi} > 1000 \text{ Гц} \end{cases}. \qquad (2)$$

3. Весовой коэффициент полосы k_i, характеризующий вероятность наличия формант речи в данной полосе, по формуле

$$k_i = k(f_{Bi}) - k(f_{Hi}), \qquad (3)$$

где $k(f_{Bi})$ и $k(f_{Hi})$ – значения весового коэффициента для верхней f_{Bi} и нижней f_{Hi} граничных частот, рассчитанные по формуле

$$k(f) = \begin{cases} 2,57 \cdot 10^{-8} \cdot f^{2,4}, \\ \text{если } 100 < f \le 400 \text{ Гц} \\ 1 - 1,074 \cdot \exp(-10^{-4} \cdot f^{1,18}), \\ \text{если } 400 < f \le 10000 \text{ Гц} \end{cases}. \qquad (4)$$

4. Спектральный индекс артикуляции (понимаемости) речи R_i (информационный вес i-й спектральной полосы частотного диапазона речи), по формуле

$$R_i = p_i \cdot k_i, \qquad (5)$$

где коэффициент p_i определяется по формуле

$$p_i = \begin{cases} \dfrac{0,78 + 5,46 \cdot \exp\left[-4,3 \cdot 10^{-3}\left(27,3 - |\theta_i|^2\right)\right]^2}{1 + 10^{0,1|\theta_i|}}, \\ \text{если} \quad \theta \le 0; \\ 1 - \dfrac{0,78 + 5,46 \cdot \exp\left[-4,3 \cdot 10^{-3}\left(27,3 - |\theta_i|^2\right)\right]^2}{1 + 10^{0,1|\theta_i|}}, \\ \text{если} \quad \theta > 0 \end{cases} \qquad (6)$$

где $\theta_i = g_i - A_i$.

Далее для общей частотной полосы спектра речевого сигнала рассчитываются:

5. Интегральный индекс артикуляции речи R, по формуле

$$R = \sum_{i=1}^{N} R_i. \qquad (7)$$

6. Слоговая разборчивость S, по формуле

$$S = \begin{cases} 4 \cdot R^{1,43}, \quad \text{если R} \le 0,15; \\ 1,1 \cdot \left[1 - 1,17 \cdot \exp(-2,9 \cdot R)\right], \\ \quad \text{если } 0,15 \le \text{R} \le 0,7 \\ 1,01 - \left[1 - 9,1 \cdot \exp(-6,9 \cdot \text{R})\right], \\ \quad \text{если R} > 0,7 \end{cases}. \qquad (8)$$

7. Словесная разборчивость W, по формуле

$$W = 1,05\left[1 - \exp\left(-\frac{6,15 \cdot S}{1 + S}\right)\right]. \qquad (9)$$

Зависимости $A(f)$, $\Delta k(f)$, $p_i(g_i)$, $S(R)$ и $W(S)$ определены Покровским Н.Б. экспериментально и представлены в виде графиков в [2]. С учетом (8) и (9) легко

получить зависимость словесной разборчивости от интегрального индекса артикуляции речи:

$$W = \begin{cases} 1{,}54 \cdot R^{1{,}4}\left[\exp\left(-1{,}1R\right)\right] \\ \quad \text{если } R < 0{,}15; \\ 1 - \exp\left(-\dfrac{1{,}1R}{1+0{,}7R}\right) \\ \quad \text{если } R \geq 0{,}15; \end{cases} . \qquad (10)$$

Критерии эффективности защиты акустической (речевой) информации во многом зависят от целей, преследуемых при организации защиты, например:

- скрыть смысловое содержание ведущегося разговора;
- скрыть тематику ведущегося разговора и т.д.

Процесс восприятия речи в шуме сопровождается потерями составных элементов речевого сообщения. Понятность речевого сообщения характеризуется количеством правильно принятых слов, отражающих качественную область понятности, которая выражена в категориях подробности о перехваченном разговоре, составляемой злоумышленником.

Исходя из этого, нами предлагается новая концепция разработки методов защиты акустической информации от ее съема способами ВЧ-навязывания – преобразование зондирующего сигнала, делающее его непригодным для применения.

В радиотехнике давно известно [5] явление возникновения биений между двумя близкими по частоте гармоническими колебаниями, описываемое известной формулой

$$s_{\Sigma}(t) = s_1(t) + s_2(t) = A_{m1}\sin\omega_1 t + A_{m2}\sin\omega_2 t = 2A_{m1}A_{m2}\cos\frac{\omega_1-\omega_2}{2}t \cdot \sin\frac{\omega_1+\omega_2}{2}t . \qquad (11)$$

В результате взаимодействия двух таких колебаний возникают новые колебания с частотой

$$\omega = \frac{\omega_1+\omega_2}{2} \qquad (12)$$

и переменной амплитудой, максимальные значения которой повторяются с частотой

$$\Omega = \omega_1 - \omega_2 . \qquad (13)$$

Мы полагаем, что это явление можно использовать для защиты от ВЧ-навязывания. Действительно, если измерить частоту зондирующего колебания, то всегда можно излучить в эфир (или направить в токопроводящую среду) колебания с частотой, близкой к частоте зондирующего сигнала ВЧ-навязывания. В результате их взаимодействия образуются биения, одним из свойств которых является изменение фазы результирующего колебания при переходе огибающей через нуль.

Поскольку при съеме информации данным способом могут возникать как амплитудная, так частотная и фазовая модуляция переизлученного сигнала, то необходимо принять меры к блокированию возможности получения информации при использовании любой из этих модуляций. Помехой для сигналов с фазовой модуляцией будет изменение фазы результирующего колебания в момент перехода его амплитуды через нуль. Но если такие моменты сохранить постоянными (т.е. выбрать постоянную частоту вводимого колебания), то систему съема информации можно легко адаптировать к такой помехе. Поэтому имеет смысл частоту вводимого колебания сделать качающейся в каких-то небольших пределах, обеспечивающих возникновение явления биений. Для этого можно качать частоту влево и вправо от среднего значения, например, по линейному закону. А для внесения хаотичности в процесс перестройки частоты, основной (задающий) линейный управляющий сигнал можно сложить со случайным низкочастотным сигналом, что обеспечит защиту и от частотно- и амплитудно-модулированного снятия информации.

Для окончательного зашумления снимаемой акустической информации, излучаемый вводимый сигнал можно сложить с другим случайным сигналом малого уровня (чтобы сохранить основную частоту вводимого гармонического сигнала), перекрывающим звуковой диапазон частот.

Рассмотрим модель происходящих при этом процессов. Для удобства воспользуемся методом суперпозиции, используя в качестве исходного соотношение (11).

Обозначим вводимый сигнал как $s_1(t)$, а зондирующий сигнал как $s_2(t)$ и рассмотрим их взаимодействие.

Сначала запишем вводимый сигнал, излучаемый в среду распространения зондирующего сигнала, как

$$s_1(t) = \left[A_{m1} + \eta(t)\right]\sin\left(\omega_1 + \omega_{\mu} + \omega_P\right)t \qquad (14)$$

где

A_{m1} – амплитуда вводимого колебания,

$\eta(t)$ – случайный сигнал, суммируемый с выходным вводимым колебанием,

ω_{μ} – мгновенное значение частоты случайного сигнала, суммируемого с линейным сигналом управления смещением частоты генератора вводимого колебания,

ω_P – частота первой гармоники линейного управляющего сигнала.

Исходя из соотношений (12) и (14) можно записать частоту колебания, образующегося в результате взаимодействия сигналов $s_1(t)$ и $s_2(t)$, как

$$\omega = \frac{\omega_3+\omega_2}{2} , \qquad (15)$$

где

$$\omega_3 = \omega_1 + \omega_{\mu} + \omega_P ,$$

а частоту повторения максимальных значений амплитуды результирующего колебания как

$$\Omega = \omega_3 - \omega_2 . \qquad (16)$$

При этом амплитуда результирующего колебания запишется как

$$A_{\Sigma} = 2\left[A_{m1} + \eta(t)\right]\cdot A_{m2} , \qquad (17)$$

а само результирующее колебание как

$$s_{\Sigma}(t) = A_{\Sigma}\cos\frac{\omega_3-\omega_2}{2}t \cdot \sin\frac{\omega_3+\omega_2}{2}t . \qquad (18)$$

Таким образом, в среду, используемую для подачи зондирующего колебания, будет введена активная помеха, преобразующая сигнал ВЧ-навязывания в сигнал с фазой, частотой и амплитудой, носящими случайный характер, что сделает его непригодным для работы на резонатор.

Заметим, что при определенном выборе средней частоты вводимого колебания и диапазона ее изменения можно достичь захвата этой частоты генератором ВЧ-навязывания.

Выводы.

1. Предложенный метод защиты акустической информации от ее съема с использованием способов ВЧ-навязывания изменяет свойства зондирующего сигнала и преобразует его в непригодный для использования по назначению.

2. Метод позволяет обеспечить постановку активной помехи, изменяющей свойства зондирующих сигналов и препятствующей получению переизлучаемых сигналов, модулированных по частоте, фазе и амплитуде, и, как следствие, снятию информации.

3. Проверка предлагаемого метода защиты акустической информации на словесную и слоговую разборчивость показала, что срыв несанкционированного получения информации наблюдается при словесной разборчивости менее 71%. Практически доказано, что составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 60-70%, а краткой справки – аннотации – при словесной разборчивости менее 40-50%. При словесной разборчивости менее 20-30% значительно затруднено установление даже предмета ведущегося разговора, а при словесной разборчивости менее 10% это практически невозможно даже при использовании современной техники фильтрации помех.

1. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб.: ООО "Издательство Полигон", 2000. – 896 с. 2. Анин Б.Ю., Петрович А.И. Радиошпионаж. – М.: Международные отношения, 1996. – 448 с. 3. Андрианов В.И., Бородин В.А., Соколов А.В. "Шпионские штучки" и устройства для защиты объектов информации. Справочное пособие. – СПб: Лань, 1996. – 272с. 4. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. – К.: Арий, 2008. В двух томах. 5. Изюмов Н.М., Линде Д.П. Основы радиотехники. – М.: Энергия, 1964. – 479 с.

Надійшла до редколегії 23.06.09

УДК 621: 658.56 (075.8)

Л.А. Пономаренко, д-р техн. наук, проф.
Н.В. Касаткіна, здобувач

ШЛЯХИ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В АТЕСТАЦІЇ НАУКОВИХ КАДРІВ

Розглянута актуальна проблема підвищення якості підготовки та атестації наукових кадрів вищої кваліфікації за допомогою застосування прогресивних інформаційних технологій. Запропоновано низку конкретних заходів, які сприятимуть розв'язанню названої проблеми.

Ключові слова: інформаційна технологія, база даних, атестація наукових кадрів

The actual problem of improvement of quality of preparation and certification of scientific manpower of the top skills by means of application of progressive information technologies is considered. A number of concrete actions which will promote the decision of the named problem is offered.

Keywords: information technology, database, certification of scientific manpower

Вступ. Модернізація українського суспільства, орієнтація на інноваційний тип суспільного розвитку вимагає різкого підвищення якості підготовки фахівців вищої кваліфікації. Будь-яке нове актуальне й складне завдання неможливо розв'язати без ефективної участі вчених. Можна сміливо стверджувати: у сучасному світі рівень розвитку науки визначає і рівень розвитку даного суспільства. Тому наша молода держава життєво зацікавлена у зростанні як кількості наукових кадрів, так і їх якості. І, навпаки, псевдонаукові роботи і "баласт бездарів" різко гальмують розвиток нашої науки і понижують її рейтинг на фоні інших світових наукових шкіл. Ситуація у цій сфері зараз досить тривожна. Відбувається поступова, але неухильна девальвація наукових ступенів. У середовищі службовців державних органів влади, керівників підприємств і фінансово-кредитних установ спостерігається своєрідне змагання за володіння правом нанести на візитну картку науковий "титул", який би засвідчив приналежність хазяїна до інтелектуальної еліти. Як відповідь на згадані проблеми ВАК України підвищує вимоги до порядку підготовки і проходження атестації дисертаційних робіт. Проблеми підготовки наукових кадрів вищої кваліфікації досить часто обговорюються на сторінках періодичних видань, часто-густо із протилежними оцінками і суперечливими пропозиціями, які, на наш погляд, є малоефективними.

Основна частина. Ефективність внеску вченого у розв'язання найскладніших, злободенних і нестандартних завдань, які висуваються практикою, у всіх галузях економіки, в освіті й духовному житті нашого суспільства визначається рівнем та якістю дисертацій, які захищаються в наукових установах та навчальних закладах. Першочергове завдання, поставлене самим життям, – підвищення вимогливості до наукових досліджень, актуальності й новизни розробок, їх практичної значущості.

При вирішенні цього завдання надзвичайно важливим є забезпечення об'єктивності й незалежності експертизи дисертаційних робіт. З цією метою ВАК планомірно здійснює низку заходів. На думку багатьох фахівців, ключовими напрямками, які мають забезпечити удосконалення системи атестації науково-педагогічних кадрів, є

1. Система вимог до докторських і кандидатських дисертацій.
2. Порядок комплектування спеціалізованих вчених рад.
3. Порядок проходження дисертацій.
4. Публікація результатів дисертаційних досліджень.
5. Призначення офіційних опонентів.
6. Порядок комплектування експертних рад ВАК.

Реалізація названих вище ключових положень неможлива без широкого застосування сучасних досягнень інформатики і обчислювальної техніки. Багато із цих проблем у суто технічному плані зводиться до створення, наповнення та організації експлуатації інтегрованих баз даних із відповідними системами управління базами даних (СУБД). До таких баз даних повинна, зокрема, входити інформація про фахівців за різ-