Объединив нейроны можно получить нейронную сеть. Совокупность подобных сетей представляет собой идеальный нейрокомпьютер.

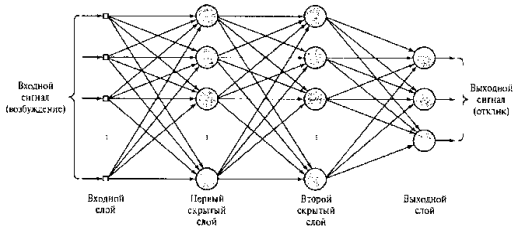

Рис. 2 – Нейронная сеть

Нейронные компьютеры обладают рядом преимуществ: повышенное быстродействие, устойчивость к помехам. Недостатком является использование параллелизма, который устраняется путём построения максимально параллельных алгоритмов для различных классов задач.

Наряду с бимолекулярными и квантовыми ЭВМ, компьютеры, использующие нейронные сети, являются одним из самых перспективных направлений развития в современной электронике и будут широко востребованы в медицине, для прогнозирования различных процессов и событий, для обеспечения информационной безопасности. [2]

ЛИТЕРАТУРА

1. Журнал «Нейрокомпьютеры: разработка, применение», ИПРЖР Радиотехника

2. Нейрокомпьютерная парадигма и общество. / Под ред. Ю. Ю. Петрунина. — М.: Издательство Московского университета, 2012. — 304 с.

В.К.ЖЕЛЕЗНЯК[1], Д.С.РЯБЕНКО[1], И.Б.БУРАЧЕНОК[1]

ОЦЕНКА НОРМАТИВНЫХ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ РЕЧЕВОГО СИГНАЛА В АНАЛОГОВОЙ И ЦИФРОВОЙ ФОРМЕ

[1]*Учреждение образования «Полоцкий государственный университет», г. Новополоцк, Республика Беларусь*

Для оценки защищенности речевой информации в каналах утечки широко применяется в качестве измерительного гармонический сигнал, обоснованный корреляционной теорией разборчивости речи [1]. Метод гармонического измерительного сигнала обладает рядом преимуществ по сравнению с другими и обусловлен рядом положительных свойств. Однако при наложении ограничения на время воздействия гармонического сигнала, его параметры ухудшаются.

С целью обоснования сложного сигнала с большой базой [1] в качестве измерительного установим математическую зависимость между нормированным показателем защищенности гармоническим измерительным сигналом и показателем, устанавливающим защищенность сложным сигналом с большой базой. Нормированный показатель защищенности речевого сигнала, установленный для метода гармонического сигнала [2], подтверждает возможность однозначно оценивать защищенность речевого сигнала, а также с учетом повышенных возможностей аппаратуры перехвата и обработки позволяет установить обоснованный нормированный показатель для метода сложного сигнала с большой базой.

Для оценки нормативного показателя защищенности речевого сигнала используем k измерительных сигналов с большой базой в k -полосах равной разборчивости. Исходя из того, что для детерминированного сигнала отношение сигнал/шум (ОСШ) в диапазоне $0 \le t \le T_c$ определяют как $q^2 = 2E / N_0$, где N_0 – спектральная плотность мощности шума [3], то отношение сигнал/шум для сложного сигнала с большой базой можно представить:

$$q^2_{вых\_сл} = \frac{2U_0^2 T_c^2}{BN_0} 2\Box f = \frac{2U_0^2 T_c^2 2\Box f}{T_c 2\Box fN_0} = \frac{2U_0^2 B}{2\ fN_0} = \frac{P_c}{P_ш} 2B, \qquad (1)$$

где $P_ш$ мощность шума в заданной полосе равной разборчивости $2\Delta f$ равная $P_ш = N_0 2\Delta f$, а P_c – мощность сигнала равная $P_c = U_0^2$. Задаваемые значения ОСШ на входе и получаемые на выходе приемника согласно (1) взаимозависимы на величину размера базы сложного сигнала.

Нормативный показатель, устанавливающий математическую зависимость между нормированным показателем защищенности гармоническим измерительным сигналом и показателем, устанавливающим защищенность сложным сигналом с большой базой, определяют как ОСШ на выходе, оцененное при помощи сложного сигнала с большой базой $q^2_{вых\_сл}$ к нормативному показателю $q^2_{вых\_гар}$ защищенности речевого сигнала в виде численного значения ОСШ гармонического измерительного сигнала:

$$\delta_{сл} = \frac{q^2_{вых\_сл}}{q^2_{вых\_гар}}. \qquad (2)$$

Если нормативный показатель защищенности речевого сигнала гармоническим измерительным сигналом определяется как: $q^2_{вых\_гар} = \left(P_c / P_ш\right)_{норм}$, то при равенстве отношений сигнал/шум выходных сигналов измерительного гармонического и сложного с большой базой $\left(P_c / P_ш\right)_{сл} = \left(P_c / P_ш\right)_{норм}$ имеем:

$$\delta = \frac{q^2_{вых\_сл}}{\left(P_c / P_ш\right)_{норм}} = \frac{2B\left(P_c / P_ш\right)_{сл}}{\left(P_c / P_ш\right)_{норм}} = 2B \qquad (3)$$

С помощью математической модели (3), устанавливающей однозначную связь метода оценки разборчивости речи сложным сигналом с большой базой с методом гармонического сигнала оценки разборчивости речи установлены однозначные преимущества первого метода перед вторым, определяемое величиной базы первого сигнала равное произведению времени существования сигнала на полную девиацию частоты в пределах полосы равной разборчивости.

Таким образом, чем больше значение базы измерительного сложного сигнала, тем выше возможность его обнаружения на фоне шумов высокого уровня относительно измерительного гармонического сигнала. Преимуществом сложных сигналов с большей базой является то, что с их помощью возможно получить большие значения ОСШ на выходе канала утечки речевой информации. Использование сложных измерительных сигналов с большой базой для оценки защищенности каналов утечки речевой информации позволяет улучшить ОСШ на $\approx$ 12 дБ при длительности сигналов T_c=1 с и на $\approx$ 16 дБ при T_c=4 с в k -полосах равной разборчивости.

При преобразовании электрических аналоговых речевых сигналов в речевые сигналы в цифровой форме с постоянными параметрами и аддитивной помехой типа белого гауссового шума в канале утечки информации возникают сигналы и наводки на несимметричные цепи и паразитная модуляция генераторов [1]. Преобразование речевых сигналов в цифровой форме в аналоговые речевые сигналы сопровождается излучением наведенных манипулированных сигналов на высокочастотные колебания с гармониками частот дискретизации.

Нормативный показатель оценки защищенности речевого сигнала от утечки должен адекватно соответствовать критерию оценки защищенности от утечки речевого сигнала в цифровой форме. Предложено критерий оценки защищенности речевых сигналов в цифровой форме установить по вероятности ошибочного приема бита $р_{ош}$, приведенному к информационному показателю нормированной величины разборчивости речи.

Известно, что при малом отношении сигнал/шум $P_c < P_ш$ для аналогового сигнала из формулы Шеннона значение пропускной способности [2]:

$$C_a = F\log_2 e \cdot \frac{P_с}{P_ш} = 1{,}443 \cdot F \cdot \frac{P_с}{P_ш} = 1{,}443\frac{P_с}{N_0} = 1{,}443\Delta, \qquad (4)$$

где $C_а$ – пропускная способность канала; F – ширина полосы частот; $P_c / P_ш$ – отношение мощности сигнала P_c к мощности шума $P_ш$ для аналогового речевого сигнала; $P_c / N_0 = \Delta$ – нормативное значение отношения мощности речевого сигнала P_c к спектральной плотности мощности шума N_0.

Нормативное значение отношения мощности сигнала P_c к спектральной плотности мощности шума N_0 установлено нормированным показателем разборчивости речи.

Для двоичного симметричного дискретного канала пропускная способность канала $C_ц$ при ее равенстве максимальной скорости передачи информации $C_ц=R_{макс}$ вычисляется [4]:

$$C_ц = 1 + p_{ош} \log_2 p_{ош} + (1 - p_{ош}) \log_2 (1 - p_{ош}). \quad (5)$$

При равенстве $C_ц = C_a$ из формулы (5) вычисляют вероятность ошибочного приема бита $p_{ош}$ в зависимости от нормативного значения отношения Δ мощности сигнала P_c к спектральной плотности мощности шума N_0. Нормативным значением оценки защищенности речевых сигналов в цифровой форме следует принять величину вероятности ошибочного приема бита $p_{ош}$, соответствующую нормированному показателю разборчивости речи.

Научно обоснован критерий оценки защищенности от утечки речевого сигнала в цифровой форме в виде числового значения ошибочного приема бита $p_{ош}$ путем установления математической зависимости с критерием оценки защищенности аналогового речевого сигнала в виде нормированного числового значения разборчивости речи и битовой скорости передачи.

ЛИТЕРАТУРА

1.Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с.

2. Варакин, Л.Е. Теория сложных сигналов / Л.Е. Варакин. – М.: Советское радио, 1970. – 376 с.

3. Линдсей, В.С. Системы синхронизации в связи и управлении: Пер. с англ. /Под ред. Ю.Б. Бакаева и М.В. Капранова. – М. Сов. радио. 1978. –600с.

4. Баскаков, С.И. Радиотехнические цепи и сигналы: учебник для вузов по спец. «радиотехника». – 2-е изд., перераб. и доп. / С.И. Баскаков. – М.: Высш. шк., 1988. – 448 с.

Н.В.ГРИБ[1], Т.Н.ДВОРНИКОВА[1], Е.В.ЖУРОК[1]

HD – SDI ИЛИ CCTV

[1]*Учреждение образования «Высший государственный колледж связи», г. Минск, Республика Беларусь*

Формат цифровой передачи данных HD-SDI пришел в системы видеонаблюдения совсем недавно, как и очень многие технологии до него из телевизионного вещания.

В области телевидения высокой четкости формат HD-SDI получил широкое распространение при переводе телевидения к цифровому сигналу и радикальному улучшению качества картинки. Особенно популярным формат стал в связи с возможностью сохранения каналов передачи сигнала: в большинстве своем используются уже проложенные коаксиальные кабели. Аналогичным преимуществом обладают производители систем безопасности, в частности DiGiVi и Polyvision. Для перехода от аналоговых систем к цифровым достаточно заменить конечные устройства приема и передачи видеосигнала, то есть установить соответствующие видеокамеры и видеорегистраторы.

Очень ценным преимуществом формата HD-SDI перед параллельно развивающейся IP технологией является отсутствие задержки при передаче видеосигнала. При идеальных условиях: линии связи, видеокамеры, маршрутизаторы, при использовании IP-видеонаблюдения задержка при передаче видеопотока с разрешением 1080 p (FullHD) уже в теории достигает 70 мс.

Как показывает практика, в среднем задержка при вышеупомянутых характеристиках сигнала составляет порядка 300 мс. Причем, в зависимости от состояния сети (загруженности) в данный момент, задержка может достигать 1,5 секунд и более.

Всего этого мы избегаем при использовании HD-SDI: 1 кабель - 1 канал.

CCTV, или Close Circuit Television, переводится как «система телевидения замкнутого контура». Технология HD-SDI позволяет без особых усилий добиться невозможности вмешательства в каналы передачи видеосигнала извне. Помимо случая использования оптоволоконного кабеля.

Формат HD-SDI 1.0, имеет следующие характеристики, касающиеся длины канала связи: гарантированная длина передачи видеосигнала в формате HD-SDI 1.0 составляет 100 м при использовании кабеля RG-59 и 150 м при использовании кабеля RG-6.

Для увеличения длины канала передачи возможно использование повторителей, которые способны увеличить линию связи на 200 м. В одной линии связи может использоваться не менее 5 таких повторителей, то есть канал передачи составит уже более 1 км.

Формат HD-SDI 1.0 поддерживает передачу видеосигнала с разрешениями 720 p@30 fps (1280x720), 720 p@60 fps (1280x720) и 1080 p@30 fps (1920x1080). Единственным серьезным ограничением формата HD-SDI на данный момент является невозможность передачи звука.

На рубеже первого десятилетия XXI века был создан Альянс HDcctv, адаптирующий и по сей день технологию HD-SDI применительно к цифровому HD-видеонаблюдению. В то время, как создатели интернет протокола занимались глобальными проблемами, например увеличением максимального возможного количества IP-адресов в сети, разработчики HDcctv Alliance наращивали пропускную способность и длину канала передачи формата.

Уже сегодня ратифицировано множество расширений формата, такие как HD-SDI XR (extended Reach), позволяющие достигать дальности передачи сигнала до 320 м (с использованием специальных приемопередатчиков и кабеля RG-6U). Активно ведутся разработки формата HD-SDI 3.0, который позволит увеличить максимально возможную для передачи частоту кадров видеоряда и будет нести множество дополнений.

Таким образом, технология HD-SDI уже сейчас заняла прочное место на рынке видеонаблюдения. А скорость развития технологии открывает огромные перспективы, даже при сопоставлении с IP наблюдением.

ЛИТЕРАТУРА

1. Журнал «Алгоритм Безопасности», №4, 2013 г., Москва.
2. Журнал «Спецтехника» 2013 Г., Москва.

В.А.ВИШНЯКОВ[1], С.М.ГОНДАГ[2], Ш.М.МОЗДУОАНИ[2]

АНАЛИЗ БЕЗОПАСНОЙ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНЫХ СИСТЕМАХ УПРАВЛЕНИЯ И ОБЛАЧНЫХ СРЕДАХ

[1]Учреждение образования «Высший государственный колледж связи», г. Минск, Республика Беларусь
[2]Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Республика Беларусь

Средства безопасности в корпоративных системах управления (КИС) предусматривают уровни защиты по периметру безопасности, такие как межсетевые экраны, системы предотвращения вторжений (Intrusion Prevention Systems − IPS), зашифрованное сетевое туннелирование [1].

Информационно-ориентированная сеть (Information-Centric Networking − ICN) в последнее время рассматривается как перспективная парадигма для следующего поколения КИС, работающих в Интернете. В ICN контент важнее, чем хост, что дает такие преимущества, как сокращение загрузки сети, низкая задержка распространения, масштабируемость и т. д. Сети, ориентированные на данные (Named Data Networking − NDN) являются представителем ICN архитектуры. В докладе представлены четыре вопроса наиболее важные для безопасности в NDN для защиты информации: от новых форм неизвестных атак, обеспечения конфиденциальности, блокировки вредоносного сетевого трафика, обнаружения аномалий и DoS/DDoS атак [2].

Облачные вычисления (ОВ) используются в КИС из-за экономической эффективности, экономии времени и эффективного использования вычислительных ресурсов. Но вопросы конфиденциальности и безопасности являются одними из основных препятствий, сдерживающих внедрение этой технологии [1].

В докладе представлены также элементы предлагаемого подхода для безопасной работы пользователей в среде облачных вычислений. Участники взаимодействий: пользователь (пользователям могут быть физические лица и организации), аутентификатор подлинности (Trusted Authenticator − TA), облачный провайдер услуг (Cloud Service Provider − CSP),