та коэффициентов ОПС для СП с постепенно деградируемой структурой. Показано, что применение разработанной математической модели позволяет эффективно реализовать процедуры обнаружения и коррекции ошибок, а также осуществлять перевод из непозиционного кода в ПСС.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Бережной В.В.* Математическая модель нейронных сетей для исследования ортогональных преобразований сигналов в расширенных полях Галуа // Нейрокомпьютеры: разработка и применение. 2003. №6.С.61-68.

2. *Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Бережной В.В.* Математическая модель нейронной сети для коррекции ошибок в непозиционном коде расширенного поля Галуа// Нейрокомпьютеры: разработка и применение. 2003. №8-9. С.10-16.

3. *Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А., Бережной В.В.* Нейросетевая реализация в ПСКВ операций ЦОС повышенной разрядности/Нейрокомпьютеры: разработка, применение. №5-6 2004. С. .94 -100.

4. *Калмыков И.А., Щелкунова Ю.О., Гахов В.Р.* Применение ПСКВ для повышения отказоустойчивости биометрических систем аутентификации. – Известия ТРТУ. Тематический выпуск. Материалы V Международной научно-практической конференции «Информационная безопасность». Таганрог: 2003. №4. . С.151-155.

5. *Калмыков И.А.* Математическая модель нейронной сети для исправления ошибок непозиционного кода расширенного поля Галуа в частотной области/Нейрокомпьютеры: разработка, применение. №5-6. 2004. С.71-78.

6. *Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А., Бережной В.В.* Архитектура отказоустойчивой нейронной сети для цифровой обработки сигналов/Нейрокомпьютеры: разработка, применение. № 12. 2004. С.51-60.

7. *Калмыков И.А., Щелкунова Ю.О.* Математическая модель вычисления коэффициентов обобщенной полиадической системы $GF(p^v)$ на основе нейронной сети. – Тезисы докладов и сообщений II Международной научно-технической конференции «Физика и технические приложения волновых процессов». Самара, 2003. С.146.

8. Элементы компьютерной математики и нейроноинфроматики */Червяков Н.И., Калмыков И.А., Галкина В.А., Щелкунова Ю.О., Шилов А.А.*; *Под ред. Н.И. Червякова*. - М.: Физматлит, 2003. - 216 с.

9. *Калмыков И.А., Чипига А.А.* Методика пересчета коэффициентов обобщенной полиадической системы для живучих систем биометрической аутентификации пользователя - Материалы VI Международной научно-практической конференции «Информационная безопасность». Таганрог: 2004. С.144-146.

В.В. Котенко
Россия, г. Таганрог, ТРТУ

ОЦЕНКА ИНФОРМАЦИОННОГО ОБРАЗА ИССЛЕДУЕМОГО ОБЪЕКТА С ПОЗИЦИЙ ТЕОРИИ ВИРТУАЛЬНОГО ПОЗНАНИЯ

Постоянно возрастающая роль информационных технологий в современном мире объективно определяет актуальность поиска новых подходов, позволяющих повысить эффективность процессов обработки и передачи информации. Это тем более важно для научных исследований, учитывая явно наметившуюся тенденцию неуклонного увеличения объемов требуемой в их целях информации.

Так как понятие «информация» свойственно только процессу коммуникации, объект исследования и исследователь в данном случае могут рассматриваться как элементы некоторой схемы коммуникации (рис.1).

Объект исследования здесь выступает в роли источника информации, а исследователь – в роли ее получателя. При этом в качестве канала коммуникации может выступать или окружающая среда, что соответствует непосредственной

коммуникации, или технические средства, что определяют техническую коммуникацию.

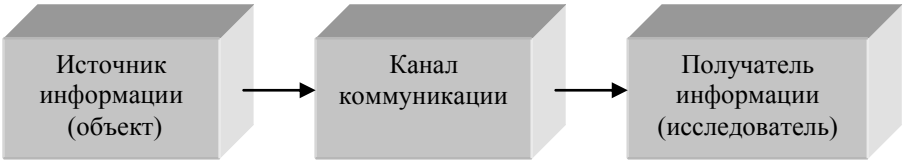

Рис.1. Схема коммуникации процесса научных исследований

С этих позиций можно считать, что основной задачей получателя информации в ходе исследования объекта является создание некоего информационного образа источника информации. В терминах теории информации основу этого образа составляет понятие «ансамбль», составляющими которого являются выборочное пространство и его вероятностная мера. При этом, если выборочное пространство дискретное, то вероятностная мера представляет собой совокупность вероятностей. Если же оно непрерывное, то вероятностная мера соответствует плотности вероятностей непрерывного случайного процесса, составляющего выборочное пространство.

Необходимо подчеркнуть, что абсолютное большинство рассматриваемых объектов при их включении в ходе исследования в схему коммуникации представляют собой непрерывные источники информации. Таким источникам соответствует непрерывный ансамбль, основу которого составляет непрерывное выборочное пространство. Вследствие этого, количество собственной информации об объекте во времени может рассматриваться как некий векторный непрерывный случайный процесс *J(t)* с математическим ожиданием, равным вектору дифференциальных энтропий исследуемых параметров объекта.

Главной особенностью реальной коммуникации (как непосредственной, так и технической) является то, что этот процесс воспринимается получателем информации об объекте (исследователем) квантами. Это объясняется целым рядом причин, к которым, прежде всего, следует отнести специфику функционирования органов чувств человека, а также всегда существующие ограничения на точность и надежность синхронизации измерительных приборов. Образно говоря, исследователь объекта анализирует (наблюдает) не сам процесс *J(t)*, а результат его своеобразного цифрового представления J_{ψ} *(i).* Эта ситуация является типичной для современных подходов к обработке информации об объектах исследования практически во всех областях знаний. Вполне понятно, что в данном случае происходит искажение истинной информации об объекте, вызванное ошибками квантования и дискретизации исходного процесса *J(t)* при коммуникации. Последствия этого вполне очевидны: это неточности в теоретических построениях, а иногда и полная их несостоятельность. К сожалению, эти последствия обычно проявляются только через некоторое время, по мере развития научного знания. Причем, как показывает история, формы этого проявления могут оказаться весьма негативными и даже трагическими. Учитывая вполне прогнозируемое увеличение возможных масштабов этих последствий в условиях научно-технического прогресса, становится понятной опасность сложившейся ситуации. Эта опасность еще более усиливается тем, что вплоть до настоящего времени отмеченная ситуация фактически остается без должного внимания.

Ставится задача определения подхода, позволяющего получить оценку *J*(t)* исходного процесса *J(t)*, обеспечивающего минимально допустимую величину информационных потерь $e(t) = J(t) - J^*(t)$.

Сразу отметим, что решение данной задачи в прямой постановке не представляется возможным. Это связано с особенностью определения компонент $J_n(t)$ вектора $J(t)$, основу которого составляют информационные характеристики параметров исследуемого объекта. Особенность в данном случае заключается в том, что основу определения случайного значения $J_n(t)$ составляет вероятностная характеристика $P_n(t)$ другого случайного значения – значения n-го параметра исследуемого объекта. Образно говоря, понятие количества собственной информации выступает здесь в роли некоего виртуального понятия. Под виртуальным (от средневекового латинского virtualis) понимается возможное при определенных условиях. Нельзя не заметить, что это образное сравнение подсказывает выход из рассмотренной выше ситуации, а именно: применение для решения поставленной задачи теории виртуального познания.

Согласно общему принципу виртуальности этой теории, любой реальный объект (явление) может рассматриваться как проекция некоторого объекта (явления) виртуальной области. При этом несколько реальных объектов (явлений) могут являться различными проекциями одного и того же виртуального объекта (явления). То есть один и тот же объект в виртуальной области может иметь множество различных реальных проекций.

Применив общий принцип виртуальности к поставленной задаче и рассматривая систему коммуникации (рис.1) как реальную проекцию можно получить следующее определение соответствующей ей виртуальной схемы: виртуальный объект (источник) формирует некоторую непрерывную субстанцию, которая квантуется и передается другому виртуальному объекту (получателю).

С этих позиций поставленную задачу можно рассматривать как реальную проекцию некоторого виртуального образа в виде задачи определения подхода, позволяющего получателю свести к минимуму потери от квантования субстанции, формируемой источником.

Среди возможных реальных проекций данного виртуального образа наибольший интерес в нашем случае представляет собой задача минимизации ошибки квантования в цифровых системах связи [1]. Трансформация апробированных решений этой задачи через виртуальную область применительно к реальной проекции, составляющей поставленную задачу, позволяет получать достаточно оригинальный подход к ее решению.

Для простоты изложения данного подхода воспользуемся представлением процесса $J(t)$ в скалярном виде, учитывая при этом возможность последующего обобщения полученных результатов на его векторное представление. Скалярное представление $J(t)$, с учетом отмеченной выше трансформации через виртуальную область, может быть определено как

$$J(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} S_J(\omega) \mathrm{e}^{j[\omega t - \varphi(\omega)]} d\omega \ , \qquad (1)$$

где $J(t)$ – количество собственной информации некоторого определяющего параметра объекта; $S_J(\omega)$ – спектральная плотность $J(t)$; $\omega = 2nf$ – частота; $\varphi(\omega)$ - фаза.

Необходимо подчеркнуть, что представление (1) отражает реализации стационарного процесса, удовлетворяющие условиям Дирихле.

Преобразовав (1) в тригонометрическую форму, имеем

$$J(t) = j\frac{1}{2\pi} \int_{-\infty}^{\infty} S_J(\omega) \cos[\omega t - \varphi(\omega)] d\omega + j\frac{1}{2\pi} \int_{-\infty}^{\infty} S_J(\omega) \sin[\omega t - \varphi(\omega)] d\omega \, . \qquad (2)$$

Спектральная плотность *Sj(ω)* в выражениях (1) и (2) показывает плотность распределения значений количества информации, приходящихся на бесконечно малый частотный интервал. В случае стационарности *J(t)* эта спектральная плотность не зависит от времени, и ее, так называемая энергетическая форма представления $G(f) = 2S^2(f)$ может быть определена как

$$G_J(f) = \int_{-\infty}^{\infty} R_J(\tau)\cos(2\pi f\tau)d\tau - j\int_{-\infty}^{\infty} R_J(\tau)\sin(2\pi f\tau)d\tau, \qquad (3)$$

где $R_J(\tau)$ – корреляционная функция *J(t).*

Это свойство вполне логично позволяет рассматривать спектральную плотность как некий информационный образ исследуемого объекта. Причем логичность такого представления сохраняется и при нестационарности *J(t),* так как вызванное этим изменение данного информационного образа во времени будет незначительным по сравнению с *J(t).*

В случае, когда *J(t)* присущи элементы квантового периодического изменения во времени, выражение (2) может быть приведено к виду

$$J(t) = \frac{1}{2}h_0 + \sum_{k=1}^{\infty} \bar{J}_k \cos(k\Omega t - \Psi_k) + j\sum_{k=1}^{\infty} \tilde{J}_k \sin(k\Omega t - \Psi_k), \qquad (4)$$

где h_0 – энтропия источника; $k\Omega = k2\pi/T$ – частоты, вблизи которых сосредоточен спектр процесса *J(t);* Ψ_k – $arctg(\tilde{J}_k / \bar{J}_k)$ – фаза; $\tilde{J}_k$ и $\bar{J}_k$ - ортогональные - случайные компоненты процесса:

$$\bar{J}_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} J(t)\cos k\Omega t dt \ ,$$

$$\tilde{J}_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} J(t)\sin k\Omega t dt \ .$$

Из (4) видно, что *J(t)* может быть представлена как совокупность информационных квазигармонических колебаний с частотами, кратными частоте Ω, соответствующей периоду *T*. Если каждую из этих гармоник условно считать информационным каналом, то информационный анализ объекта исследователем предстает как многоканальная схема коммуникации. Отсюда следует , что в данном случае наиболее полное представление об определенном параметре объекта дает его исследование по некоторому множеству параллельно используемых информационных каналов. Этот вывод остается справедливым и при переходе к случаю непериодического изменения *J(t),* т.е. при переходе от (4) к (2) путем устремления значения периода *T* к бесконечности. При этом, как следует из (2), в роли информационного канала будет выступать полоса информационных частот $d\omega$.

Необходимо подчеркнуть, что полученный выше вывод в принципе не является новым. Сама природа пришла к нему гораздо раньше. Примером этому может служить процесс восприятия человеком звуков, когда их спектр разбивается в его слуховом аппарате приблизительно на 6 000 полос (каналов) и информация о значениях средних интенсивностей сигналов в этих каналах параллельно поступает в мозг. Отсюда можно считать, что восприятие звуков и придание им определенных

образов осуществляется мыслительным аппаратом человека путем параллельного анализа множества информационных каналов, соответствующего каждому звуку.

Обращает внимание еще одна особенность, которую можно заметить при анализе приведенных выражений. Информационный образ любого реального объекта, как следует из (3), может иметь две явно выраженные составляющие – действительную и мнимую, т. е.

$$G_J(f) = G_{Jd}(f) + jG_{Jm}(f), \tag{5}$$

где

$$G_{Jd}(f) = \int_{-\infty}^{\infty} R(\tau)\cos(2\pi f\tau)d\tau, \tag{6}$$

$$G_{Jm}(f) = \int_{-\infty}^{\infty} R(\tau)\sin(2\pi f\tau)d\tau. \tag{7}$$

Данная особенность присуща и самому процессу *J(t)*, который, как видно из выражений (2) и (4), тоже имеет две явно выраженные действительную и мнимую составляющие.

При этом, для реальной проекции, взятой за исходную, установлено, что мнимая часть спектра сигнала обращается в ноль ввиду наблюдаемой в данном случае четности корреляционной функции. Согласно общему принципу виртуальности, можно считать, что этот результат будет справедлив и для других реальных проекций, в том числе и для проекции, определенной выражениями (1) - (4). Отсюда следует, что при традиционном изучении и анализе реальных объектов (явлений) исследователю доступна только действительная часть их информационного образа, т.е.

$$G_{Jd}(f) = 2\int_{0}^{\infty} R_J(\tau)\cos 2\pi f\tau d\tau. \tag{8}$$

Полученный вывод порождает целый ряд вопросов, выводящих в принципиально новую область научного познания. Прежде всего, что собой представляет мнимая часть информационного образа реальных объектов? Не является ли ее существование подтверждением положений различного рода эмпирических теорий и верований о существовании неких информационных и духовных субстанций, соответствующих реальным объектам? Например, чем это не подтверждение теории эгрегоров, которая утверждает, что каждому реальному объекту соответствует некоторая информационная сущность, так называемый эгрегор, которая для человека выступает в роли «ангела-хранителя»? А если пойти еще дальше, может быть, эта часть информационного образа отражает еще одну область существования определений части реальных объектов, так называемый потусторонний мир и т.п.? Почему мнимую часть информационного образа невозможно измерить в реальных проекциях? Что надо предпринять, чтобы нарушить четность корреляционной функции в (7)? Ответы на эти и производные от них вопросы, несомненно, могут составить основу отдельных фундаментальных исследований. Пока же, можно с достаточной долей уверенности утверждать, что само существование мнимой (духовной) части информационного образа реальных объектов закладывает основу дальнейшего совершенствования процесса их научного исследования.

Выражения (1) - (8) определяют математическую модель информационного образа объекта исследований как источника информации в схеме коммуникации (рис.1). Однако, как уже отмечалось, исследователь, выступая с этих позиций в роли получателя информации, имеет возможность работать только с квантовыми

представлениями об объекте. Образно говоря, исследователь, применяя известные подходы, получает, как правило, информацию, искаженную так называемыми шумами квантового представления, что, естественно, приводит к формулированию им искаженного информационного образа объекта исследования. Вполне понятно, что эти искажения будут влиять на научную достоверность результатов исследования. Это влияние может характеризоваться ошибкой $e(t) = J(t) - J^*(t)$. Среди возможных критериев минимизации данной ошибки наиболее предпочтительным по результатам апробации является критерий минимума среднего квадрата ошибки (СКО). С позиций этого критерия общий алгоритм определения оптимальной оценки *J**, минимизирующей ошибку, определяется посредством

$$J^* = \int_{-\infty}^{\infty} JP_{ps}(J)dJ\ , \qquad (9)$$

где $P_{ps}(J)$ - апостериорная плотность вероятностей.

Для интервалов квантования во времени $t\ (t_i < t < t_{i+1})$ апостериорная плотность вероятностей может быть определена дифференциальным уравнением Фоккера-Планка-Колмогорова [1]:

$$\frac{dP(J(t),t)}{dt} = \alpha \frac{d}{dJ}\{[J(t) - h_0]P(J(t),t)\} + \frac{g^2}{4} N_J \frac{d^2}{dJ^2} P(J(t),t)\,, \qquad (10)$$

где α, g, N_J определяются из дифференциального уравнения состояния источника

$$\frac{dJ(t)}{dt} = -\alpha(t, J(t)) + g(t)n_J(t) \qquad (11)$$

в предположении его стационарности, гауссовости и марковости, когда (11) принимает вид

$$\frac{dJ(t)}{dt} = -\alpha(J(t) - h_0) + gn_J(t)\,. \qquad (12)$$

Здесь $n_J(t)$ - стационарный гауссовский белый шум со спектральной плотностью N_J.

Таким образом, при получении наблюдения $J_\psi(t_i) = J_\psi(i)$ апостериорная плотность вероятностей скачком устанавливается равной $P_{ps}(J(i))$, а затем экстраполируется по закону (10). Исходя из этого, задача определения оценки $J^*(t)$ по квантовой последовательности $J_\psi(i)$ разделяется на две задачи: задачу определения последовательности оценок $J^*(t_i) = J^*(i)$ и задачу сглаживания полученной последовательности $J^*(i)$. Если эта оценка формируется на полуинтервале наблюдения $[t_i, t_{i+1})$ по одному наблюдению $J_\psi(i)$, то справедливо выражение

$$J^*(t) = J^*(i)\mathrm{e}^{-\alpha(t-t_i)}. \qquad (13)$$

Задача определения оценки $J^*(i)$ в общем случае является нелинейной задачей, которая может быть решена на основании (9) путем определения рекуррентного выражения для апостериорной плотности вероятностей [2]. Результатом этого решения является рекуррентный алгоритм вида

$$J^*(i) = \mathrm{e}^{-\alpha T} J^*(i-1) + K_i^{(k)}\left[J_\psi(i) - \mathrm{e}^{-\alpha T} J^*(i-1) - h_0\right] + h_0\,, \qquad (14)$$

где *k* - индекс области квантования, к которой относятся $J_\psi(i)$; $K_i^{(k)}$ - коэффициент усиления.

Определение оценки $J^*(t)$ является основой для дальнейшего формирования оценки информационного образа:

$$S_J^*(\omega) = \int_0^\infty J^*(t) e^{-j\omega t} dt . \qquad (15)$$

Выражения (13) - (15) представляют собой математическую модель оценки информационного образа исследуемого объекта. Реализация данной модели и создание на ее основе программных и программно-аппаратных комплексов позволит выйти на новый качественный уровень решения задач информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Величкин А.И*. Передача аналоговых сообщений по цифровым каналам. - М.: Радио и связь, 1983. – 240 с.

2. *Величкин А.И., Котенко В.В*. Сглаживание непрерывного сообщения на выходе системы связи с кодоимпульсной модуляцией // Радиотехника, 1980, Т. 35. № 3. С..38-41.

О.Р. Маликов
Россия, г. Москва, МГУ им. М.В.Ломоносова

АВТОМАТИЧЕСКОЕ ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ В ИСХОДНОМ КОДЕ ПРОГРАММ

В настоящее время развитие коммуникационных технологий привело к новым требованиям по безопасности программного обеспечения. Необходимым условием обеспечения безопасности программы является её корректная работа на всех возможных наборах входных данных (как допустимых, так и недопустимых). Наиболее важным классом ошибок, приводящих к нарушению этого условия, являются так называемые уязвимости защиты (security vulnerabilities). Наличие ошибки этого типа в программе означает, что существует возможность преодолеть ограничения защиты всей системы, частью которой является эта программа.

По данным сайта SecurityFocus.com, отслеживающего найденные уязвимости защиты в программах, за период в полтора года с января 2000 г. было найдено более трех тысяч уязвимостей. Наиболее частыми ошибками являются ошибки переполнения буфера (в разные периоды от 23 % до 50 %) и форматной строки.

В процессе тестирования и отладки программы обнаружить уязвимости защиты чрезвычайно трудно, так как в большинстве случаев для того, чтобы уязвимость себя проявила, программе необходимо передать нетривиальные входные данные, обработка которых была плохо продумана или реализована. Поэтому на стадии тестирования и отладки находятся лишь самые простые уязвимости. Другой подход к предотвращению использования уязвимостей защиты представляют собой утилиты, предназначенные для обнаружения попыток взлома защиты в реальном времени. Однако часто такие программы влекут неприемлемые временные затраты, при этом они фиксируют лишь попытку взлома, не указывая собственно на место ошибки. Поэтому наиболее полным с точки зрения безопасности решением является аудит исходного кода программы с привлечением автоматических или полуавтоматических инструментальных средств (так как исследование кода, проводимое вручную, является дорогостоящим и длительным).

К сожалению, существующие на данный момент утилиты либо не предназначены для поиска именно уязвимостей защиты, либо выдают слишком большое количество ложных срабатываний (до 90%), когда фрагмент программы, не содержащий таких ошибок, отмечается как опасный. Применение методов глубокого