3 Технічні засоби системи захисту інформації. Стандартизація та метрологічне забезпечення систем ТЗІ. Визначення відповідності засобів ТЗІ

УДК: 519.95

КОНТРОЛЬ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В КОМПЬЮТЕРНЫХ СЕТЯХ И СИСТЕМАХ

Юлий Савченко, Георгий Розоринов, Сергей Толюпа*
*НТУУ "КПИ",*ГУИКТ*

Анотація: **Запропонована методика визначення реальної вірогідності невиявлення помилок в умовах застосування групових кодів.**
Summary: **The method of determination of the real probability of undetection of errors is offered in the conditions of application of group kodas.**
Ключові слова: **Надійність, груповий код, достовірність, безпека, надмірність.**

I Введение

В связи с использованием компьютерных сетей в качестве средства информационного обмена в системах управления реальными процессами в промышленности, банках и оборонных объектах особое внимание уделяется их безопасности и надежности. Уже на интуитивном уровне понятия безопасности и надежности – почти синонимы. Очевидно, что безопасность связана с надежностью не только аппаратных средств, но и программного обеспечения, реализующего обработку и передачу информации между рабочими станциями (абонентами) компьютерной сети.

В большинстве случаев надежность как показатель качества технического объекта определяют во временной области, чаще всего как вероятность безотказной работы (выполнения рабочего алгоритма) за заданное время. Как правило, этот период достаточно большой – десятки и тысячи часов. С другой стороны, с точки зрения безопасности этот показатель во многих практически важных случаях не является критичным. Например, если компьютер является звеном управления блоком АЭС, то такой показатель надежности как среднее время безотказной работы T (тысячи часов) вряд ли можно считать самым важным. Скорее нас будет интересовать значение вероятности выдачи ошибочного управляющего воздействия (команды) на объект управления, т. е. достоверность полученной в результате компьютерной обработки и передачи по каналу связи информации. Иными словами, безопасность будет зависеть, в первую очередь, от эффективности процедур контроля, используемых при обработке и передаче информации. Здесь уместно процитировать одну из работ, посвященных безопасности: "Контроль призван защитить нас от аварий в тех случаях, когда из-за недостаточной надежности появляются отказы" [1]. Это высказывание основано на практическом опыте создания и эксплуатации систем контроля объектов оборонной техники и отражает значение контроля в проблеме обеспечения безопасности.

Цель работы – показать возможности использования естественной информационной избыточности, которая практически всегда присутствует в реальных сигналах и сообщениях, для организации эффективного контроля достоверности, а также дать точную оценку достигаемой достоверности передачи в случае применения кодов с обнаружением ошибок.

II Основная часть

Рассмотрим задачи контроля, ограничившись представлением сигнальной информации (например, команд и сообщений, поступающих на объект управления) в цифровом виде. Пусть сигналы, достоверность которых необходимо контролировать, представлены двоичными n – разрядными словами $X_i = (x_1, x_2, ..., x_n)$

Используя терминологию теории кодов, контролирующих ошибки, множество всех возможных n – разрядных слов X^0 можно представить объединением $X^0 = X^p \cup X^3$, где X^p – подмножество разрешенных (кодовых) слов, а X^3 – подмножество запрещенных слов. Очевидно, если все слова являются разрешенными, то возможность контроля достоверности полностью отсутствует. С другой стороны, в первом приближении,

можно утверждать, что количество обнаруживаемых ошибок будет тем больше, чем больше объем подмножества запрещенных слов $m\left(X^3\right)$. Долю или часть, например, в процентном соотношении ошибок, которые обнаруживаются при заданном $m\left(X^3\right)$, можно определить с помощью простого выражения [2]:

$$\delta = \frac{m\left(X^3\right)}{2^m - 1}. \qquad (1)$$

Ясно, что когда все возможные сигналы (сообщения) являются разрешенными, т. е. $m\left(X^3\right) = 0$, то определить, содержит или нет конкретное сообщение ошибку, не представляется возможным. Исходя из фундаментальных положений теории информации, можно утверждать, что этот случай является примером отсутствия информационной избыточности (ИИ).

Традиционно ИИ связывают с использованием помехозащищенных кодов для передачи и хранения информации. Уровень ИИ определяется превышением максимально возможной энтропии $H_{\max}$ над реальной энтропией H_p источника информации при использовании конкретного способа кодирования $D = 1 - \frac{H_p}{H_{\max}}$, или в абсолютном исчислении, т. е. в битах $D^a = H_{\max} - H_p$, где $H_{\max} = \log_2 N$ и $H_p = \sum_{i=1}^{N} p_i \log_2 p_i$, а N - количество возможных сообщений, p_i - вероятность появления *i*-го сообщения.

Такое превышение возникает при любом отклонении распределения вероятностей появления отдельных сообщений от равномерного. В частном случае, когда отдельные сообщения при нормальной работе источником не используются (вероятность их появления равна 0), именно эти сообщения образуют подмножество запрещенных слов X^3. Этот случай с практической точки зрения наиболее интересен, поэтому далее рассмотрим его подробнее.

Если рассматривать ИИ менее формально, то можно отметить, что ее присутствие проявляется в специфичности (индивидуальности) источника сообщений. При использовании помехозащищенных кодов эта индивидуальность достигается добавлением проверочных символов, образованных в соответствии с определенными правилами. Выполнение именно этих правил и делает источник индивидуальным, т. е. каждое кодовое (разрешенное) слово можно отличить от других, если при этом были использованы другие способы кодирования. Проверка искусственно введенных правил позволяет обнаружить и (или) исправить ошибки, которые возникли при передаче или хранении информации.

Однако наличие ИИ не является обязательным для того, чтобы источник был индивидуальным (отличимым от других). Даже в случае, когда все сообщения равновероятны, источник остается специфичным. Эта индивидуальность именно в том и состоит, что все сообщения равновероятны, а отклонения от равновероятности будут свидетельствовать о возникновении ошибок при передаче или хранении информации. Такую ситуацию можно рассматривать даже как парадоксальную – никакой избыточности нет, а ошибки, по крайней мере некоторые, можно обнаружить.

Таким образом, можно утверждать, что любой источник с известной и стационарной статистикой появления (генерации) сообщений (даже генератор белого шума) является специфичным. И если эту специфику можно описать с помощью некоторых формальных правил, то можно и обнаружить ошибки. Отсюда следует, что контроль достоверности произвольного источника можно осуществить без введения искусственной ИИ. Такое утверждение не является результатом строго формального доказательства. Это, скорее, гипотеза, в доказательство которой можно привести большое количество примеров. Приведем некоторые из них.

Пример 1. Сообщения генерируются источником и имеют произвольное распределение вероятностей, задаваемое спектрограммой, полученной, например, в результате длительного наблюдения за этими сообщениями. Такая спектрограмма отображает относительные частоты появления того или иного сообщения (символа, отсчета оцифрованного аналогового сигнала и т. п.). Известно, например, что а английском тексте символ (буква) E встречается с относительной частотой (вероятностью) 0,12, символ *W* – 0,02 и т. д. В украинском языке распределение иное. Наибольшую частоту имеют символы О (0,08), А (0,07), а наименьшую – символы Ц (0,0044) и Є (0,0037). Именно распределение частот появления символов характеризует индивидуальность конкретного источника.

Проверку частотного распределения можно рассматривать как процедуру контроля в качестве соответствующего критерия достоверности информации: любое существенное отклонение от зафиксированной за значительное время наблюдений зависимости является признаком возникновения

ошибки. Однако, одиночные отклонения (однократные ошибки) вряд ли приведут к изменению распределения и потому не могут быть надежно обнаружены. Ясно, что это является принципиальным ограничением всех без исключения статистических методов контроля. Более того, даже если ошибки регулярны, их можно обнаружить лишь с запаздыванием, и вновь после значительного времени наблюдения. Поэтому статистический метод контроля не может быть оперативным (обнаружение ошибки в момент ее возникновения) и не может быть использован в случаях, когда полученная информация сразу же используется для управления реальними объектами и даже одиночные ошибки могут привести к серьезным последствям с точки зрения безопасности.

Пример 2. В частотном распределении есть “провалы” - они образуются за счет запрещенных слов, которые имеют нулевую вероятность появления. Появление любого слова из X^3 является признаком ошибки, которая может быть практически мгновенно выявлена аппаратными или программными средствами.

С теоретической точки зрения между примерами 1 и 2 нет принципиальной разницы. И в одном, и в другом случае свойства источника описываются одинаково – произвольным частотным распределением, и это распределение можно использовать как эталон для обнаружения ошибок. Но с практической точки зрения и эффективности контроля по критерию безопасности (минимума времени, за которое ошибка может быть обнаружена) второй пример принципиально отличается от первого. Именно наличие слов с нулевой вероятностью появления дает возможность обнаружить соответствующие ошибки практически в момент их появления.

Поэтому решение примера 1 выглядит достаточно простым и прозрачным. Если рассматривать частотное распределение, образованное парами слов, которые поступают в смежные моменты времени, то почти наверняка обнаружится, что некоторые пары имеют нулевую вероятность появления. А это свидетельствует об автоматическом переходе к примеру 2. Если же рассматривать частотное распределение „троек”, „четверок” и др. смежных во времени сообщений, то количество таких искусственно объединенных сообщений, имеющих нулевую вероятность появления, будет возрастать в геометрической прогрессии.

Для иллюстрации рассмотрим пример сообщения на русском или украинском языках. На уровне отдельных букв в частотном распределении нет „провалов” - в текстах используются все символы, но с разной вероятностью. Но уже в распределении пар такие „провалы” появляются: в русском языке мягкий знак никогда не используется после гласных, в украинском языке не используются пары „кє”, „дє” и др.

Это были, условно говоря лингвистические примеры, которые, на первый взгляд, не имеют отношения к контролю электронной аппаратуры и компьютерных систем. Однако, если внимательно проанализировать, например, сообщения, поступающие от конкретного датчика в систему управления технологическим объектом, то можно заметить определенные закономерности, характерные для статистической структуры таких сообщений. Например, если это значения температуры жидкости, которую нагревают, то эти значения будут возрастать, и каждое значение в момент времени t_1 будет не меньше, чем в момент $(t_1 - 1)$. Или, например, давление в замкнутом объеме, который уменьшается, не может также уменьшаться, поскольку в соответствии с законом Бойля-Мариотта, произведение давления на объем остается постоянным. Отметим, что именно эта закономерность в ответственных случаях может быть использована для контроля достоверности сигналов, которые поступают в систему управления от объекта. Во многих других случаях именно „связанность” (коррелированность) некоторых параметров физическими закономерностями может оказаться наиболее полезной и эффективной для контроля достоверности.

Например, известно, что в компьютерных системах управления реальными объектами большая часть информации поступает в систему путем регулярного опроса датчиков и первичных преобразователей в соответствии с фиксированным временным регламентом. Как следствие, сообщения от отдельных датчиков, которые характеризуют один физический (технологический) процесс, будут обязательно коррелированны (взаимозависимы) уже хотя бы потому, что параметры процесса не могут выходить за границы соответствующих физических (химических) законов. Поэтому, как и в предыдущем примере, проверка выполнения этих законов может быть эффективно использована для контроля достоверности. Коррелированность сигналов свидетельствует о присутствии ИИ, поэтому введение дополнительной избыточности путем специального кодирования не является обязательным. И, самое важное, контроль на основе уже присутствующей избыточности, которую логично назвать естественной ИИ, охватывает не только ошибки средств передачи данных, а и нарушения нормальной („правильной”) работы объекта управления и неисправности средств автоматизации. А именно это обстоятельство наиболее существенно с точки зрения безопасности и предупреждения аварийных ситуаций.

На сегодняшний день применение кодов, контролирующих ошибки в телекоммуникационных системах, давно уже не исключение, а норма. Это связано, прежде всего, с непредсказуемым уровнем помех даже в стационарных каналах информационного обмена и, с другой стороны, относительно небольшими затратами

на реализацию процедур кодирования и декодирования. Поэтому преобладающее большинство стандартов и протоколов межкомпьютерного обмена предусматривают как обязательное помехозащищенное кодирование.

Оценка эффективности применения кодирования проводится, как правило, на основе известных соотношений, связывающих кратность t ошибок, которые могут быть обнаружены или исправлены, с минимальным кодовым расстоянием $t_{\text{îáí}} = d_{\min} - 1$ и $t_{\text{èñ}} = \frac{d_{\min} - 1}{2}$. Но эти простые соотношения определяют лишь минимальный гарантированный эффект от применения кодирования (по крайней мере, это справедливо для обнаружения ошибок). На самом деле, любой код обладает существенно более высокой обнаруживающей способностью. Например, один из самых простых кодов с обнаружением однократных ошибок (одной проверкой на четность и $d_{\min}$ =2) обнаруживает все ошибки нечетной кратности t =3,5,7,…, т. е. практически 50% всех возможных ошибок. Можно показать, что большинство кодов имеет более высокую способность к обнаружению ошибок по сравнению с теоретической, определяемой минимальным кодовым расстоянием.

Точную оценку количества обнаруживаемых ошибок дает соотношение (1). Для максимального количества векторов ошибок, которые могут быть исправлены, справедливо неравенство [2]:

$$m(E) \le \frac{m\left(X^3\right)}{2^m - m\left(X^3\right)}. \qquad (2)$$

Эти соотношения дают точную оценку количества обнаруживаемых ошибок и ошибок, которые потенциально могут быть исправлены соответствующей процедурой кодирования. Однако конкретный состав таких ошибок остается неизвестным. С практической точки зрения пользователя услугами связи и компьютерной сети в целом интересует реальная достоверность информационного обмена, т. е. вероятность того, что полученное сообщение не содержит ошибок.

Ограничимся здесь анализом реальной обнаруживающей способности некоторых используемых на практике кодов с обнаружением ошибок. Такие коды получили наибольшее распространение, так как не требуют введения значительной ИИ и при наличии обратного канала для передачи команды на повторную передачу блока, содержащего ошибку, обеспечивают требуемую достоверность в целом.

В условиях независимости ошибок в отдельных символах битового потока с увеличением длины блока (пакета) n суммарная вероятность возникновения ошибки более высокой кратности также увеличивается в соответствии с биномиальным законом $P(t) = \sum_{i=1}^{t} C_n^i q^i (1-q)^{n-i}$. Из всей совокупности возможных ошибок кратности t, количество которых определяется комбинаторным числом C_n^t любой конкретный код обнаруживает лишь некоторую часть, а именно N_t ошибок (при $C_n^t = N_t$ код обнаруживает все ошибки соответствующей кратности).

Вероятность отсутствия ошибок в блоке длиной n можно записать в виде

$$P_0 = \sum_{t=1}^{n} (C_n^t - N_t)\, q^t (1-q)^{n-t} \qquad (3)$$

где q – вероятность ошибки в одном бите последовательности.

Таким образом, исходя из (3), для оценки реальной способности конкретного кода обеспечить заданный уровень достоверности необходимо рассчитать ряд значений N_t, $t = 1, 2...n$. Очевидно, эти значения могут бать получены только на основе свойств проверочной матрицы группового кода или порождающего полинома циклического кода.

Для кодов с количеством проверочных разрядов больше 1 такая оценка может оказаться достаточно трудоемкой. В частности, необходимо путем перебора сочетаний столбцов проверочной матрицы выявить такие сочетания, поразрядная сумма по модулю 2 которых не равна нулю – это те векторы кратных ошибок, которые действительно обнаруживаются кодом [3].

Рассмотрим для иллюстрации такого подхода проверочную матрицу классического (7, 4) - кода Хемминга

$$P = \begin{bmatrix} 1101100 \\ 1011010 \\ 1110001 \end{bmatrix}.$$

В табл. 1 приведены результаты вычислений для всех возможных кратных ошибок.

Таблица 1 – Кратные ошибки (7, 4)-кода Хэмминга

t	1	2	3	4	5	6	7
C_7^t	7	21	35	35	21	7	1
N_t	7	21	28	28	21	7	0
$C_7^t - N_t$	0	0	7	7	0	0	1

Из табл. 1 видно, что обнаруживаются все ошибки кратности 1, 2, 5, 6, и не обнаруживаются некоторое количество ошибок кратности 3, 4 и 7. Непосредственный подсчет показывает, что код обнаруживает 88,2% всех возможных ошибок. Полученное значение совпадает со значением, рассчитанным на основе (1):

$$\delta = \frac{2^n - 2^k}{2^n - 1} = \frac{128 - 16}{127} = 0{,}882 .$$

Аналогично можно рассчитать способность (7, 4)–кода обнаруживать пакеты ошибок длиной b (табл. 2).

Таблица 2 – Обнаруживающая способность (7, 4)-кода Хэмминга

b	2	3	4	5	6	7
M	6	5	4	3	2	1
N	6	4	2	3	2	0
$M - N$	0	1	2	0	0	1

В таблице символами M и N обозначены, соответственно, комбинаторное число теоретически возможных ошибок в пакете и таких ошибок, которые реально обнаруживаются.

Рассмотрим теперь популярный (8, 4)-код, имеющий такую проверочную матрицу

$$P = \begin{bmatrix} 10110000 \\ 11001100 \\ 11101010 \\ 11111111 \end{bmatrix}$$

Как и можно было ожидать, способность к обнаружению ошибок по сравнению с предыдущим кодом возрастает, что видно из табл. 3.

Таблица 3 – Кратные ошибки (8, 4)-кода

t	1	2	3	4	5	6	7	8
C_7^t	8	28	56	70	56	28	8	1
N_t	8	28	56	56	56	28	8	0
$C_7^t - N_t$	0	0	0	14	0	0	0	1

(8, 4)-код обнаруживает 94% ошибок. Можно было бы привести большое число других кодов, которые используются в телекоммуникационных системах. В частности, такой анализ выполнен для кода ASCII, (11, 7-кода, международного телеграфного (15, 11)-кода МТК-2 и многих циклических кодов.

Задаваясь вероятностью q возникновения ошибки в одном бите цифрового потока (численное значение

определяется физическими свойствами реального канала) и законом распределения вероятностей возникновения ошибок в группах символов можно рассчитать реальную достоверность информационного обмена. Так, например, при использовании (7, 4)-кода Хэмминга и $q=10^{-8}$ вероятность необнаружения составляет 7×10^{-24} при независимых искажениях отдельных битов.

III Заключение

Предлагаемый подход позволяет точно рассчитать обнаруживающую способность заданного кода по отношению к конкретным ошибкам. Это создает предпосылки для реализации сетей с гарантированной безопасностью информационного обмена путем выбора соответствующего кода, где безопасность, по сути, является вероятностью отсутствия ошибок в сообщении.

*Литература:***1.** *Крохин Я А. Фактометрия. Техногенные катастрофы. Между прошлым и будущим / Я. А. Крохин. – К.: Логос, 2004. – 92 с.* **2.** *Локазюк В. М., Савченко Ю. Г. Надійність, контроль, діагностика і модернізація ПК / В. М. Локазюк, Ю. Г. Савченко. - К.: Видавничий центр „Академія", 2004. – 373 с.* **3.** *Теоретичні основи завадостійкого кодування. Ч. 1 / П. Ф. Олексенко, В. В. Коваль, Г. М. Розорінов, Г. О. Сукач. – К.: Наукова думка, 2010. - 192 с.*

УДК.621.791

МЕТОДИКА КОНТРОЛЯ РАБОТОСПОСОБНОСТИ ВИБРОИЗЛУЧАТЕЛЕЙ ДЛЯ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Михаил Кузнецов, Игорь Порошин, Михаил Прокофьев
НИЦ "ТЕЗИС" НТУУ "КПИ"

Анотація: **Пропонується методика вхідного/вихідного контролю віброперетворювачів, яка враховує виробничий розкид їх параметрів. Реалізація методики дозволить розподіляти віброперетворювачі по групам залежно від рівня віброприскорення, яке вони створюють на стандартній масі, і таким чином знизити трудозатрати при створенні комплексів ТЗІ.**
Summary: **The method of enter/exit control of vibroemitters, taking into account production variation of their parameters, is offered. Its realization will allow to distribute vibroemitters on groups depending on the level of vibroacceleration, developed by them on standard mass, and thus to reduce creation expenditures of protection complexes.**
Ключевые слова: **Захист мовної інформації, комплекс ТЗІ.**

I Введение

Контроль работоспособности виброизлучателей (ВИ), используемых в системах активной виброакустической защиты (АВЗ) речевой информации, обычно производится по рекомендациям, изложенным в нормативных документах по технической защите информации (НД ТЗИ). Однако нормативные требования, согласно которым характеристики ВИ проверяются на стандартной стальной массе [1], не учитывают всё разнообразие строительных конструкций, на которые ВИ устанавливаются.

Как показывает практика, некоторые из этих конструкций ("тяжелые" - стены, потолки, полы и т. п.) для эффективного зашумления требуют высокие уровни шумового виброускорения. Другим же, «лёгким» конструкциям (окнам, сантехническим системам, воздуховодам и т. п.) вполне достаточны существенно меньшие уровни виброускорения, которые создаются в них ВИ. Учитывая производственный разброс параметров ВИ целесообразно при входном/выходном контроле ВИ распределять их по группам применения в зависимости от уровня виброускорения, развиваемого ими на стандартной массе. Специалисты, занимающиеся установкой и настройкой систем АВЗ, по опыту знают, какая именно группа ВИ пригодна для эффективного зашумления той или иной конкретной конструкции, не создавая при этом значительного уровня паразитного акустического шума. Не исключено, что некоторые ВИ, не обеспечивающие требуемых уровней виброускорения для "тяжелых" конструкций, могут достаточно эффективно зашумлять «лёгкие» виды конструкций. Для этого в ходе проверки эти ВИ выделяются в группу с наиболее низким уровнем виброускорения. Подобный дифференцированный подход к проверке ВИ позволяет в ряде случаев при создании комплекса ТЗИ существенно уменьшить временные и стоимостные затраты на его создание.

Проверка ВИ и их распределение по группам в зависимости от уровня виброускорения требует наличия