МЕТОДИКА ОБОСНОВАНИЯ РАЦИОНАЛЬНОГО ВАРИАНТА ПРОВЕРКИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Гончаров В. В.[1], Гончаров А. В.[2]

Ключевые слова: *телекоммуникационная система, сеть, информационная безопасность, элемент, множество, подмножество элементов, устройство, объект, система контроля, методы интерполирования, сплайн-интерполяция.*

Аннотация

Цель работы: совершенствование научно-методических основ повышения качества контроля выполнения функций по предназначению элементами и устройствами телекоммуникационных систем и сетей.

Методы: системный анализ и экспертное прагматическое формирование подмножеств контролируемых элементов сложных технических систем в условиях ограниченного времени проведения проверок.

Результаты: разработана математическая методика обоснования рационального варианта проверки телекоммуникационных систем и сетей на основе формального разбиения множества элементов, подлежащих проверке, на три непересекающихся подмножества, обеспечивающих локальный максимум достоверности контроля выполнения задекларированных функций как самих исследуемых элементов, так и системы в целом; обоснован алгоритм, доказана возможность и целесообразность коррекции рассматриваемых подмножеств в процессе эксплуатации системы.

Полученные результаты являются основой для создания соответствующего эффективного информационно-математического обеспечения контроля достоверности функционирования сложных телекоммуникационных систем и сетей по предназначению.

DOI: 10.21681/1994-1404-2022-4-39-48

Введение

Быстрое развитие информационных технологий, телекоммуникационных сетей и систем привело к формированию *информационной среды*, оказывающей влияние на все сферы человеческой деятельности. Важнейшим условием существования и развития подобных систем является их *информационная безопасность*, под которой понимается *защищенность* корпоративной информации от случайных и преднамеренных воздействий, которые могут нанести существенный ущерб ее владельцам и пользователям [7].

В настоящее время особое место занимают преднамеренные деструктивные воздействия, связанные с хищением, разрушением, нарушением целостности информации. Так, согласно данным информационного ресурса «Ведомости», только за 2014 г. правоохранительными органами было зарегистрировано более 11 000 подобных преступлений в Российской Федерации. По данным *Group-IB*, ущерб от компьютерных преступлений в РФ увеличивается с каждым годом: в 2015 г. ущерб увеличился на 2,649 *млрд руб*. по сравнению с 2014 г., а в 2016 г. — на 3,811 *млрд руб*. по сравнению с 2015 г. В 2017 г. ущерб составил более 6 *млрд руб*.[3] [16].

Принципиально меняются характер, стиль и методы подобных преступлений. С расширением спектра информационных и сетевых услуг, развитием киберфизических систем, Интернета вещей возникают и новые виды преступлений. Хорошо организованные преступные группы и сообщества для достижения корыстных целей активно и высокопрофессионально применяют в своей деятельности новые методы, подходы, специальные программно-аппаратные средства и технику. При этом преступные группировки не имеют национальности и принадлежности к какой-либо стране, часто работая в разных странах и имея в своем арсенале не только широкий спектр инструментов для планиро-

[3] Hi-tech crime trends 2017. URL: http://files.runet-id. com/2017/csf17/07feb.csf17-3.2-sachkov.pdf

[1] ***Гончаров Владимир Васильевич,*** *доктор технических наук, профессор, заслуженный работник высшей школы Российской Федерации, заведующий кафедрой математики Военной академии имени Петра Великого, г. Москва, Российская Федерация.*
E-mail: v_v_goncharov@mail.ru

[2] ***Гончаров Александр Владимирович,*** *соискатель Военной академии имени Петра Великого, г. Москва, Российская Федерация.*
E-mail: dinozavp@inbox.ru

вания преступления, «взлома» информационного ресурса и сокрытия (уничтожения) следов преступлений, но и пользуются при взаимодействии собственными системами связи.

Часто коммерческие структуры (финансовые, банковские, кредитные и др.) стремятся не афишировать успешные атаки злоумышленников с целью сохранения бизнеса и нежелательного массового оттока клиентов. По данным «Лаборатории Касперского», раскрываемость таких преступлений составляет не более 5%. Вместе с тем ущерб от нарушения информационной безопасности может привести к крупным финансовым потерям, а иногда и к краху компании.

Многие исследователи уделяют внимание только частным подходам: особенностям экспертизы систем на сетевом уровне, созданию корректного образа взломанной системы для дальнейшего исследования и др., не затрагивая при этом общих принципов и подходов к проведению анализа и выработке соответствующих решений [1, 6]. Исходя из этого, проблемы обеспечения информационной безопасности привлекают внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей. Задачи обеспечения безопасности информационных систем решаются путем построения комплексной системы информационной безопасности [7, 9].

Знание и квалифицированное применение современных информационных технологий, стандартов, протоколов и средств защиты информации позволяют достигнуть требуемого уровня информационной безопасности рассматриваемых систем [2, 7]. Вместе с тем обеспечение требуемого уровня информационной безопасности системы предполагает наличие должного контроля ее основных аппаратно-программных элементов и устройств [10]. Исходя из этого, выбор рационального варианта проведения проверки по существующим методикам является актуальным и своевременным.

Однако в результате проведения регламентов, доработок или каких-либо деструктивных операций первоначально заданные функции могут быть изменены. Как правило, *модификация* заключается в расширении функциональных возможностей, не всегда оговоренных в технической документации по проведенным доработкам. Особую значимость приобретает подобная модификация при ведении технической разведки.

В этом случае проверка элементов и устройств системы проводится на предмет выполнения ими незадекларированных функций при строго оговоренном лимите времени и использовании допустимого оборудования. Это связано с тем, что подобные проверки требуют не только понижения готовности объектов системы, но и контроль специального *программно-математического обеспечения* [8] как отдельных элементов, так и всей системы в целом. Получение требуемой *достоверности* контроля отсутствия незадекларированных функций как элементов, так и системы является актуальной научно-технической задачей, направленной на обеспечение требуемого уровня информационной безопасности телекоммуникационной системы и сети.

Формальная постановка задачи исследования

Формальная *математическая постановка задачи* исследования заключается в синтезе модели системы, состоящей из счетного множества элементов различного назначения, объединенных в единую структуру, работающих по алгоритмам, составляющим единый процесс функционирования, направленный на выполнение задач по предназначению. Из определения следует, что система включает в себя ряд подсистем, одной из которых является подсистема контроля. Важнейшей задачей данной подсистемы является проверка задекларированных функций элементов и узлов системы. Основным *показателем* в данном случае является достоверность контроля выполнения функции по предназначению. Однако на практике проведение полной проверки всех элементов системы не представляется возможным из-за их колоссального количества. Для решения поставленной задачи все множество элементов, подлежащих проверке, формально разобьем на три подмножества: проверяемые постоянно, проверяемые по демаскирующим признакам, непроверяемые (проверка является нецелесообразной из-за слишком малой составляющей, вносимой в общий показатель достоверности контроля системы).

Очевидно, что подобное деление на подмножества условно и призвано обеспечить применение математического аппарата *теории вероятностей и математической статистики* [3]. Рассматриваемые события в подмножествах являются независимыми. Переход элементов из одного подмножества в другое и обратно возможен и должен быть строго оговорен перед началом проведения проверки системы. Предполагается также, что время проведения проверки системы строго регламентировано.

Алгоритм решения

Пусть система состоит из N (*рис.* 1) основных элементов, из которых l_1 — проверяются постоянно, l_2 — проверяются по демаскирующим признакам, а остальные $N - l_1 - l_2$ не проверяются [12, 15].

Тогда вероятность отсутствия в системе элементов с незадекларированными функциями будет равна:

$$P = P_{l_1} P_{l_2} P_{N-l_1-l_2}, \quad (1)$$

где P_{l_1} — вероятность отсутствия незадекларированных функций для постоянно проверяемых элементов; P_{l_2} — вероятность отсутствия незадекларированных функций для элементов, проверяемых по демаскирующим признакам; $P_{N-l_1-l_2}$ — вероятность отсутствия элементов с незадекларированными функциями, проверка которых является нецелесообразным.

Очевидно, что вероятность P_i^* отсутствия в i-м проверяемом элементе незадекларированных функций

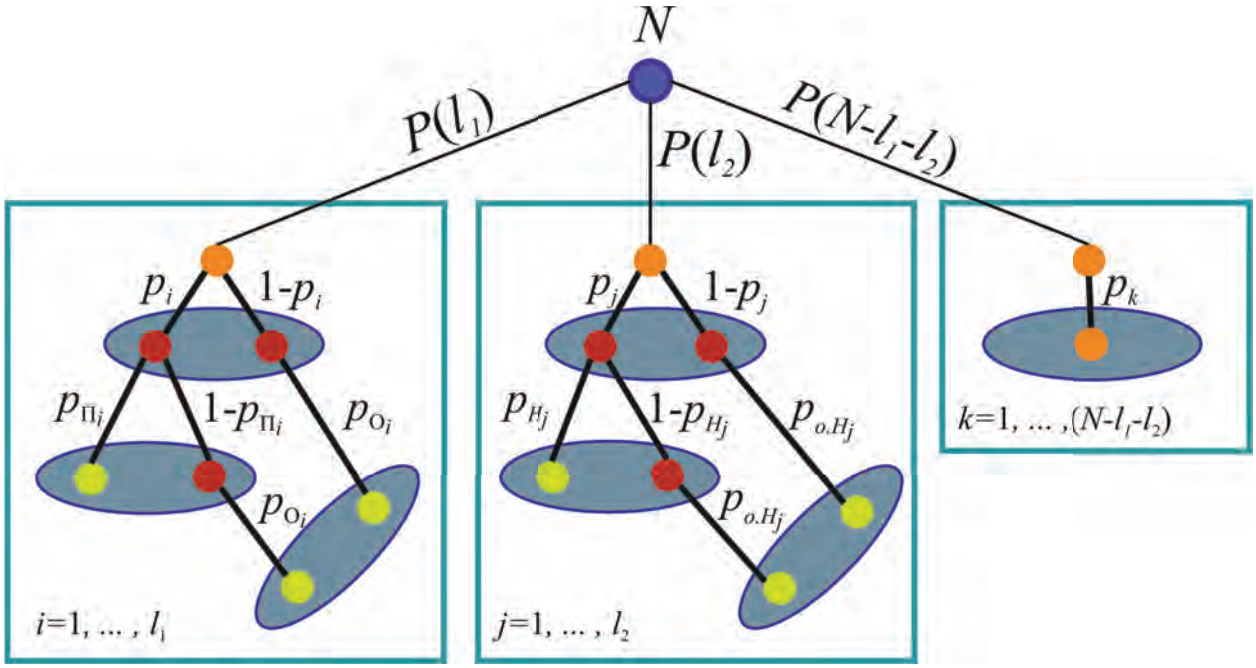

Рис. ***1. Группы элементов при проверке системы***

представляет собой [3] сумму вероятности (достоверности) контроля отсутствия элементов с незадекларированными функциями до проверки (p_i) и при проведении проверки $(p_{п_i})$, вероятности обнаружения (в результате проверки) элементов с незадекларированными функциями $(1-p_{п_i})$, существовавшими до проверки $(1-p_i)$, и вероятности обнаружения (отыскания) данных элементов (p_{o_i}). Следовательно, для i-го проверяемого элемента

$$P_i^* = p_i p_{п_i} + (1-p_i)p_{o_i} + (1-p_{п_i})p_i p_{o_i},$$

где p_i — достоверность i-го элемента до проверки системы; $p_{п_i}$ — достоверность i-го элемента при проверке системы; p_{o_i} — вероятность отыскания незадекларированной функции для i-го проверяемого элемента.

Тогда для l_1 независимых проверяемых элементов

$$P_{l_1} = \prod_{i=1}^{l_1}\left[p_i p_{п_i} + (1-p_i)p_{o_i} + (1-p_{п_i})p_i p_{o_i}\right].$$

В результате преобразования получим:

$$P_{l_1} = \prod_{i=1}^{l_1}\left[p_i p_{п_i} + p_{o_i}(1-p_i p_{п_i})\right]. \quad (2)$$

Аналогичным образом можно определить и P_{l_2}. При этом следует иметь в виду, что достоверность j-го проверяемого элемента по демаскирующим признакам при проверке системы и вероятность отыскания незадекларированных функций в этом случае могут отличаться от рассмотренных выше соответствующих значений для постоянно проверяемого элемента. Следовательно, для j-го элемента, проверяемого по демаскирующим признакам, можно записать

$$P_j^* = p_j p_{H_j} + (1-p_j)p_{o.H_j} + (1-p_{H_j})p_j p_{o.H_j}$$

или

$$P_j^* = p_j p_{H_j} + p_{o.H_j}(1-p_j p_{H_j}),$$

где p_j — достоверность определения j-го элемента, проверяемого по демаскирующим признакам; p_{H_j} — достоверность j-го элемента, проверяемого по демаскирующим признакам при проверке; $p_{o.H_j}$ — вероятность отыскания незадекларированных функций для j-го элемента, проверяемого по демаскирующим признакам.

Тогда

$$P_{l_2} = \prod_{j=1}^{l_2}\left[p_j p_{H_j} + p_{o.H_j}(1-p_j p_{H_j})\right]. \quad (3)$$

Вероятность $P_{N-l_1-l_2}$ представляет произведение достоверных не проверяемых каким-либо способом элементов системы, т. е.

$$P_{N-l_1-l_2} = \prod_{k=1}^{N-l_1-l_2} p_k, \quad (4)$$

где p_k вероятность отсутствия незадекларированных функций для не проверяемого каким-либо способом элемента.

С учетом выражений (2) — (4) выражение (1) примет вид:

$$P = \prod_{i=1}^{l_1}\left[p_i p_{п_i} + p_{o_i}(1-p_i p_{п_i})\right] \times \prod_{j=1}^{l_2}\left[p_j p_{H_j} + p_{o.H_j}(1-p_j p_{H_j})\right] \times \prod_{k=1}^{N-l_1-l_2} p_k. \quad (5)$$

При несовместных по времени проверках выбор метода проверки с целью поиска элементов с незадекларированными функциями состоит в том, чтобы обеспечить максимальное значение выражения (5) при ограниченном времени проверки, т. е. должно быть справедливо неравенство:

$$\sum_{m=1}^{l_1+l_2} t_m \le t_{\text{тр}}, \quad (6)$$

при этом $N - l_1 - l_2$ элементов не участвуют в проверке, следовательно, время на их проверку равно 0.

Учитывая определенные технические трудности оптимизации нелинейной зависимости (5), можно воспользоваться ее линейным эквивалентом, получаемым путем логарифмирования выражения (5) [3, 4]:

$$\log P = \sum_{i=1}^{l_1} \log\left[p_i p_{\text{п}_i} + p_{o_i}(1 - p_i p_{\text{п}_i})\right] + \sum_{j=1}^{l_2} \log\left[p_j p_{H_j} + p_{o.H_j}(1 - p_j p_{H_j})\right] + \sum_{k=1}^{N-l_1-l_2} \log p_k . \quad (7)$$

В процессе проверки контролируемых элементов системы получают информацию о смежных (функционально связанных с проверяемым) элементах, несмотря на то что не все они подвергаются проверке. Поэтому можно предположить, что последнее слагаемое в формуле (7) равно нулю [3]. Кроме этого, выражение (7) можно записать в общем виде, приписав каждому из первых двух слагаемых весовые коэффициенты α_i и $(1 - \alpha_i)$ соответственно. Весовой коэффициент α_i может принимать значение 1 или 0. Единица соответствует проверяемому при проверке элементу, а ноль — непроверяемому [4]. С учетом изложенного

$$\log P = \sum_{i=1}^{l} \left\{\alpha_i \log\left[p_i p_{\text{п}_i} + p_{o_i}(1 - p_i p_{\text{п}_i})\right] + (1 - \alpha_i) \log\left[p_j p_{H_j} + p_{o.H_j}(1 - p_j p_{H_j})\right]\right\}. \quad (8)$$

Или:

$$\log P = \sum_{\substack{i=1 \\ j=1}}^{l} \left\{\alpha_i \log \frac{\left[p_i p_{\text{п}_i} + p_{o_i}(1 - p_i p_{\text{п}_i})\right]}{\left[p_j p_{H_j} + p_{oH_j}(1 - p_j p_{H_j})\right]} + \log\left[p_j p_{H_j} + p_{o.H_j}(1 - p_j p_{H_j})\right]\right\},$$

где $l = l_1 + l_2$ (в обоих последних выражениях).

Первое слагаемое в (8) может служить *критерием* необходимости проверки отдельных элементов [10]. Если будет выполняться условие:

$$\frac{p_i p_{\text{п}_i} + p_{o_i}(1 - p_i p_{\text{п}_i})}{p_j p_{H_j} + p_{oH_j}(1 - p_j p_{H_j})} \le 1, \quad (9)$$

то контроль рассматриваемых элементов при проверке системы нецелесообразен. Однако неравенство (9) является лишь необходимым условием, так как оно не учитывает время, затрачиваемое на проверку. Поэтому второй этап решения задачи состоит в определении множества проверяемых элементов системы для организации поиска элементов с незадекларированными функциями, дающего наибольший эффект.

Необходимо заметить, что рассмотренный вариант проверок справедлив только при *последовательной* схеме организации проверки элементов системы [12], т. е. один проверяющий орган и множество исследуемых элементов. Однако такой подход не всегда целесообразен, так как, прежде всего, время общей проверки объекта существенно увеличивается. При параллельной схеме — несколько проверяющих органов и заданное множество элементов — все приведенные выше рассуждения остаются справедливыми, но с необходимыми ограничениями и допущениями. В связи с этим:

Первое. Так как формула (6) становится неактуальной, целесообразно разработать сетевой график проведения работ, позволяющий определять не только очередность проверяемых элементов, но и порядок работы проверяющих органов.

Второе. Для каждого из не разветвляющихся фрагментов (для конкретного участка, состоящего из счетного множества элементов) применимы вышеприведенные рассуждения, исключая (6). На основе полученных значений для не разветвляющихся фрагментов имеется возможность рассчитать достоверность контроля заданного множества элементов системы [5].

Таким образом, представленный алгоритм позволяет получить локальный максимум достоверности контроля элементов системы. Для нахождения глобального максимума необходима оптимизация порядка расположения элементов как в структуре организации выполнения работ при проверке, так и в структуре органов проверки. В свою очередь, исследование пары «элемент — проверяющий орган» (с учетом времени выполнения самой операции и ее расположения в сетевом графике выполнения работ) также может вносить свой вклад в расчет общей достоверности проверки элементов. В этом случае сформулированная задача является *многокритериальной* задачей [3, 4, 8, 12], а поиск максимального значения функции возможен методами вычислительной математики.

Коррекция подмножеств проверяемых элементов

Особый интерес представляет исследование множества элементов, проверка которых является нецелесообразной из-за слишком малой составляющей, вносимой в общий показатель достоверности контроля системы. Очевидно, что лимит времени не позволяет проводить соответствующие расчеты в рамках выполнения методики. Однако нельзя отрицать того факта, что элементы третьего множества в перспективе не станут элементами первого [11]. Это обусловлено рядом причин, обусловленных:

- недостаточным знанием о существе незадекларированных физических процессов как в отдельных элементах, так и в системе в целом;
- использованием злоумышленниками новых методов и специальных программно-аппаратных средств «взлома» систем и сокрытия (уничтожения) следов инцидента;
- отсутствием технической возможности выявления, идентификации и классификации «перспективных» угроз нарушения информационной безопасности и противодействия им и др.

Допустим, что косвенное проявление деструктивного воздействия на элемент системы заключается в изменении состояния одного из его параметров, который можно наблюдать и при необходимости зафиксировать. Таким параметром может быть напряжение, ток, температура элемента и др.

В этом случае *математическая постановка задачи* заключается в следующем. В дискретные моменты времени $x_1, x_2, \ldots, x_n$ наблюдается значение функции $f(x)$. Требуется восстановить ее значение при других x. Довольно часто $f(x)$ задается таблицей. Значения x_i $(i = 0, 1, 2, \ldots, n)$ называются «узлами таблицы». Они могут не быть равноотстоящими. Необходимо составить многочлен $P_n(x)$ степени не выше n, такой чтобы в узлах его значение было бы в точности равно значению табличной функции, т. е. $P_n(x_i) = f(x_i)$.

Смысл задачи в том, чтобы подобрать аналитическое выражение для функции, заданной таблично. Такой способ приближения называется интерполяцией или интерполированием (от латин. *interpolare* «ремонтировать») [4].

Если такой полином существует, он является единственным. В самом деле, пусть существуют два таких полинома: $P_n(x)$ и $Q_n(x)$. Тогда уравнение $P_n(x) - Q_n(x) = 0$ степени не выше n имеет $n+1$ корень: $x_1, x_2, \ldots, x_n$ что невозможно. Следовательно, $P_n(x) = Q_n(x)$.

Однако при решении задач подобного типа возникают некоторые особенности.

1. Часто бывает известно, что функция хорошо приближается функциями определенного вида, например, многочленами, но неясно, как лучше выбрать степень приближающего многочлена. Проблема усложняется, когда заданные значения функции содержат ошибки.

2. Известен вид хорошего приближения функции, например, функция хорошо приближается многочленом второй степени. В то же время измеряемые значения функции содержат ошибки. Требуется получить наилучшее в определенной норме приближение при минимальном числе измеряемых значений функции.

3. Рассматриваются все функции, такие, что некоторая норма погрешности не превосходит заданную величину. Среди таких функций нужно выбрать ту, вычисление которой требует минимальных затрат времени.

Среди способов интерполирования наиболее распространенными являются: интерполяционные многочлены Лагранжа, Ньютона, Ньютона-Грегори; полиномы по нисходящим разностям, по восходящим разностям и др.

Иногда требуется, чтобы в узлах интерполяции обеспечивалось не только равенство полинома и интерполируемой функции, но и совпадали производные полинома и функции до некоторого порядка. Можно показать существование и единственность такого полинома, который конструируется подобно полиному Лагранжа, но в общем случае имеет, естественно, весьма громоздкий вид[4]. Такие полиномы называют *полиномами с кратными узлами,* а число значений, заданных в узле, называют *кратностью* узла.

Интересен важный *частный случай*. Если имеется только два узла (нулевой и первый) и требуется, чтобы в узлах совпадали полином с функцией и первая производная полинома с первой производной функции, соответствующий полином имеет третий порядок. Он был предложен Ш. Эрмитом[5] в следующем виде:

$$P_3(x) = f_0 \frac{(x_1 - x)^2(2(x - x_0) + h)}{h^3} + f_0' \frac{(x_1 - x)^2(x - x_0)}{h^2} + f_1 \frac{(x - x_0)^2(2(x_1 - x) + h)}{h^3} + f_0' \frac{(x - x_0)^2(x - x_1)}{h^2}. \quad (10)$$

Кратность его узлов равна двум (заданы значения функции и ее первой производной). Прямой подстановкой узловых значений переменной x легко убедиться, что этот полином удовлетворяет предъявленным требованиям.

Погрешность полиномов с кратными узлами оценивается выражением, подобным погрешности полинома Лагранжа, с той разницей, что сомножители произведения $\omega(x)$ имеют степени, равные кратности соответствующего узла[6] [4]. В частности, для кубического полинома Эрмита имеет место равенство $\omega_4(x) = (x - x_0)^2(x - x_1)^2$, максимум которого достигается в точке $(x_0 + x_1)/2$ и равен $h^4/16$. С учетом этого факта приходим к следующей оценке погрешности кубического полинома Эрмита на интервале:

$$\max_{[x_0, x_1]} |f(x) - P_3(x)| \le \frac{M_4}{384} h^4$$

Это означает, что приближение функции кубическим полиномом Эрмита имеет четвертый порядок точности (с уменьшением шага вдвое погрешность уменьшается в 16 раз).

Формула (10) является фундаментом современного *метода сплайн-интерполяции* (интерполяции с помощью сплайнов), ориентированного на применение ЭВМ, впервые появившегося в 1946 г., а с 60-х годов получившего широкое распространение. Этот метод лишен недостатка, например, кусочно-полиномиальной интерполяции (с помощью полиномов Лагранжа или Ньютона-Грегори), состоящего в том, что на стыках интервалов имеет место излом графика полинома, т. е. разрыв первой производной. Пренебречь этим иногда можно, но далеко не всегда.

Термин «сплайн» (от англ. *spline* — стержень, гибкая стальная линейка) обозначает чертежное лекало пере-

[4] Вержбицкий В.М. Основы численных методов : учебник для вузов. М. : Высшая школа, 2009. 840 с.

[5] Бахвалов Н. С. Численные методы (анализ, алгебра, обыкновенные дифференциальные уравнения. М. : Наука, 1975. 632 с.

[6] Блаженков В. В. Элементы вычислительной математики. М. : МО РФ, 2004. 172 с.

менной кривизны. Из курса сопротивления материалов известно, что уравнение статического равновесия балки таково: $S^{\prime\prime\prime\prime} = 0$. Но четвертые производные равны нулю у полиномов третьего порядка. Следовательно, через каждые два соседние узла должен быть проведен график кубического полинома. А чтобы у графика, как и у реальной линейки, не было изломов и скачков кривизны, необходимо обеспечить равенство в узлах производных слева и справа. Непрерывность производных первого порядка обеспечивает отсутствие изломов графика, а непрерывность вторых производных обеспечивает отсутствие скачкообразного изменения кривизны графика. Этого достаточно, чтобы обеспечить приемлемую глобальную гладкость интерполирующей кривой и хорошую точность интерполяции.

На i-м интервале (от x_{i-1} до x_i) парабола 3-го порядка задается формулой

$$S_i(x) = a_i(x - x_{i-1})^3 + b_i(x - x_{i-1})^2 + \\ + c_i(x - x_{i-1})^1 + d_i \,. \quad (11)$$

Поскольку всего интервалов n, имеем $4n$ неизвестных (a_i, b_i, c_i, d_i для $i = 1, \ldots, n$).

Условия $S_i(x_{i-1}) = f(x_{i-1})$ в левых концах интервалов дают n уравнений. Аналогично, условия $S_i(x_i) = f(x_i)$ в правых концах дают еще n уравнений. Условия $S_i^{\prime}(x_i) = S_{i+1}^{\prime}(x_i)$ во внутренних узлах добавляют $n - 1$ уравнение. Аналогично, условие непрерывности вторых производных во внутренних узлах добавляют еще $n - 1$ уравнение: $S_i^{\prime\prime}(x_i) = S_{i+1}^{\prime\prime}(x_i)$. Отсюда имеется всего $4n - 2$ уравнения. Два параметра могут быть выбраны из дополнительных граничных условий (значения в концевых узлах). Задача получается определенной: система линейных (относительно коэффициентов) уравнений (11) включает столько уравнений, сколько в них неизвестных.

Если брать за основу общее выражение кубической параболы (11), уравнения не будут однотипными (для функции первой и второй производных они будут иметь разный вид). Это осложнит решение задачи. Целесообразнее взять за исходную формулу *кубический полином Эрмита* (10). Он уже автоматически обеспечивает заданные значения функции и ее производной на концах интервалов, и остается обеспечить лишь *непрерывность* вторых производных. Это сделает систему уравнений однотипной. Кроме того, эти уравнения будут трехчленными, т. е. матрица системы будет трехдиагональной, что позволит применить для решения этой системы высокоэффективные *методы прогонки*[7] [4].

Необходимо заметить, что учет граничных условий для нулевого и последнего узлов существенно влияет на решение задачи в целом. В [4] отмечается, что существует по крайней мере 5 вариантов их учета (а, следовательно, и задания *требований* к их определению):

1. Если в граничных точках известны значения первых производных, то учитывают их. Получается так называемый «фундаментальный кубический сплайн».

2. Если в граничных точках известны значения вторых производных, то учитывают их. В этом случае решение задачи существенно упрощается.

3. Если в граничных точках принять вторые производные равными нулю (независимо от того, имеет ли это место для интерполируемой функции), получим так называемый «естественный кубический сплайн», точность которого понижается до второго порядка за счет такого допущения.

Под термином «естественный» понимается, что вторая производная, равная нулю, означает отсутствие у приборов фиксации инструментальных погрешностей. В ряде случаев такое допущение может быть неверным и весьма искусственным. Однако благозвучие термина «естественный» в сочетании с простотой уравнений для этого случая приводит к неоправданно широкому применению этого не самого лучшего варианта.

4. Если интерполируемая функция периодична, и ее период совпадает с интервалом интерполяции, естественно потребовать, чтобы первые и вторые производные сплайна в нулевом и последнем узле совпадали.

5. Если, как часто бывает, нет никакой информации о производных на концах интервала интерполяции, накладывают условия непрерывности третьих производных в первом (не в нулевом!) и в предпоследнем узлах. Это эквивалентно попарному объединению первой и последней пар интервалов, откуда и происходит название этого способа — «условие отсутствия узла». Это, по-видимому, наилучший способ поведения при отсутствии информации о граничных условиях.

Учитывая сказанное, при проверке для каждого элемента и системы в целом задается порог срабатывания по деструктивному воздействию, т. е. задается $f_{\text{пор}}(x)$. В ряде случаев это обстоятельство является основанием для деления элементов системы на три подмножества. С учетом важности решаемых задач, конструктивных особенностей и др. проводится уточнение состава подмножеств. По результатам проверки делается научно обоснованное заключение и формируются *рекомендации* по дальнейшей эксплуатации системы. Именно в межпроверочный период на основе априорной информации, получаемой в процессе работы системы, а также учитывая ее текущее состояние, определяются элементы для углубленной проверки с целью уточнения их места в соответствующем множестве. Варианты исследования могут быть различными, начиная от теоретических исследований и заканчивая стендовыми испытания. При этом в обязательном порядке разрабатывается техническое задание и другая необходимая документация.

В качестве примера, не останавливаясь на физической сущности переменных и функции, проиллюстрируем возможность исследования функционирования элемента системы с помощью сплайн-интерполяции,

[7] Демидович Б. П., Марон И. А. Основы вычислительной математики : учеб. пособие. СПб. : Лань, 2011. 672 с.

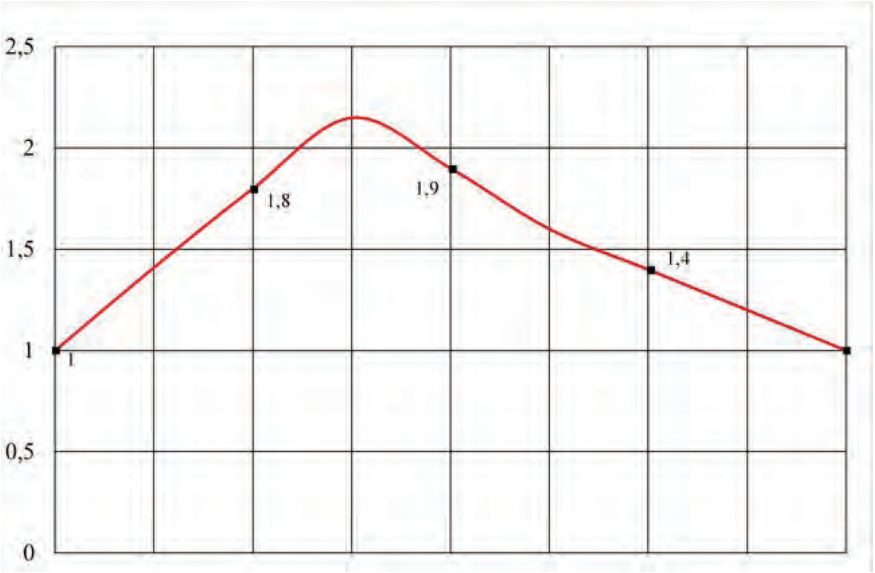

Рис. 2. «Естественный» кубический сплайн

где $f_{\text{пор}}(x) = 2$[8]. Как видно из *рис.* 2, в моменты проверки значение $f(x)$ не превышает $f_{\text{пор}}(x)$, заданного эксплуатационно-технической документацией. Однако в межпроверочный период утверждать это не представляется возможным.

Достаточно удобным и точным методом аппроксимации данных является также *метод наименьших квадратов*, рассматриваемый в регрессионном анализе. Однако формирование матрицы наблюдений не всегда возможно в связи с ограниченным временем проверки элементов системы.

Правовые аспекты формирования экспертного заключения

Решая вопросы (по существу, проводя частную экспертизу) обеспечения безопасности телекоммуникационных систем и сетей связи, необходимо неукоснительное соблюдение *требований* законодательства, определяемых УПК РФ в отношении судебной экспертизы и Федеральным законом № 73 от 31 мая 2001 г. (ред. 08.03.15) «О государственной судебно-экспертной деятельности в Российской Федерации».

Российское судопроизводство выдвигает следующий перечень *требований* к экспертному заключению:

- *полнота* — указание всех признаков; исследование в отношении всех поставленных вопросов; ответ на все поставленные вопросы; исследование всех объектов, предоставленных на исследование; исследование всех материалов, относящихся к предмету экспертизы; использование необходимых методик, обеспечивающих полноту исследования;
- *объективность* — применение объективно существующих специальных знаний; объективный подход к исследованию; использование научно обоснованных методик;
- *всесторонность* — изучение объекта со всех сторон, в том числе экспертная инициатива;
- *достоверность* — возможность проверки экспертного заключения на относимость (относимость установленного факта к предмету доказывания);
- *допустимость* (возможность допущения экспертного заключения как средства доказывания — соблюдение процессуальных требований);
- *доказательность* — установление доказательного значения как факта.

Приведенный перечень требований к экспертному заключению определяет перечень требований к *экспертной методике*, с использованием которой оно дается. Экспертная методика должна обеспечивать полноту исследования, быть научно обоснованной, всесторонне исследовать объект и обеспечивать достоверность экспертного заключения, отвечать требованиям законности, быть безопасной, эффективной, экономичной, этичной, допустимой [13].

Законодательство не ограничивает эксперта в выборе методов исследования. Определяющим фактором при оценке того или иного метода на допустимость является *научная обоснованность* и соответствие метода новейшим достижениям в области современных научных технологий[9].

В мире информационных технологий, в отличие от многих видов классических экспертиз, развитие науки и техники происходит очень быстро, что делает применение методик десятилетней давности лишь ограниченно, частично, а порой и вовсе непригодными в связи с появлением новых объектов, новых вопросов, новых способов совершения преступлений. В этой си-

[8] Блаженков В. В. Элементы вычислительной математики. М. : МО РФ, 2004. 172 с.

[9] Курс лекций по учебной дисциплине «Судебная экспертиза». URL: http://distance.rpa-mu.ru/files/2_vys_bak/sudeb_expertiza.pdf

туации приобретает большое значение научная специализация, профессиональный уровень и личный опыт эксперта. Допустимость методов для эксперта зависит также от их безопасности, характера воздействия на объект исследования, времени получения результатов[10]. Методы должны быть эффективны, рентабельны и обеспечивать решение задач исследования в оптимальные сроки с наибольшей продуктивностью. Ценность полученных результатов должна быть соизмерима с затраченными силами и ресурсами.

Анализ технологии экспертного заключения показал, что исследование, проводимое с использованием рассматриваемой методики, состоит из следующих этапов.

Подготовительный — основной целью этого этапа является уяснение задачи, для чего рассматриваются поставленные вопросы, формируется общее представление о состоянии и признаках исследуемых объектов системы. На данном этапе выдвигаются рабочие гипотезы, определяются необходимые методы, приемы и средства исследования, а также алгоритм их применения, составляется план работы. В случае необходимости запрашиваются дополнительные материалы, изучается специальная и справочная литература.

Аналитический — на этом этапе выполняется тщательное исследование объектов. На аналитическом этапе используются рабочие инструментальные методы и технические средства. Ход проведения исследования и используемые методы фиксируются. В завершении этапа даются предварительные выводы. Сделанные на аналитическом этапе выводы дополняются на последующих этапах исследования.

Эксперимент (наличие этого этапа зависит от каждой конкретной ситуации). Эксперимент проводится в целях выявления механизма взаимодействия объектов экспертного исследования и (или) механизма последствия, его отдельных параметров. В ходе эксперимента изучаются интересующие процессы и условия. Наличие/отсутствие этой стадии определяется задачами и целями экспертного исследования. Результаты эксперимента оформляются в виде предварительных выводов по данному этапу.

Синтезирующий — заключается в синтезе информации на основе проведенного анализа.

Результативный — на этом этапе происходит подведение итогов, оцениваются результаты проведенных исследований.

Формирование выводов — на этом заключительном этапе оформляются выводы по экспертизе.

На основе проведенных этапов экспертного исследования формируется экспертное заключение, состоящее из трех обязательных частей[11]:

вводная — описание и результаты подготовительного этапа;

исследовательская — описание и результаты анализирующей части эксперимента, синтезирующей и результативной частей;

выводы — формирование выводов (этап «формирование выводов»).

В общем случае под экспертной методикой (методикой экспертного исследования) понимается последовательность изучения свойств объекта экспертизы с целью решения экспертной задачи путем упорядоченного применения научно разработанной системы методов экспертного познания, включающего в себя:

всеобщие методы познания — материалистическая диалектика;

общенаучные методы — к ним относятся наблюдение, измерение, описание, эксперимент, моделирование;

частные методы — инструментальные методы, применимые для экспертизы определённого рода;

специальные методы — частные методы, адаптированные под выполнение конкретной экспертизы.

Методы делятся на *простые* (описывают способ выполнения одного действия) и *комплексные* (описывают способ выполнения нескольких действий). Некоторые методы, примененные на одной стадии, могут быть использованы и на другой стадии (например, *наглядно-образный метод* представления информации используется для фиксации результатов на всех этапах исследования), т. е. существуют методы, общие для нескольких этапов исследования.

Заключение

Таким образом, рассмотренные в статье научно-методологические и математические аспекты обоснования рационального варианта проверки системы с целью отыскания максимума достоверности контроля отсутствия в их работе незадекларированных функций не противоречат основным процессуальным нормам и федеральному законодательству о государственной судебно-экспертной деятельности и имеют существенное практическое значение. Перспективным направлением решения рассмотренной задачи является разработка соответствующего специального математического и программного обеспечения имитационно-моделирующего комплекса (ИМК) [8], позволяющего не только рассчитывать по приведенным соотношениям значения рассмотренных показателей, но и учитывать возможности по наращиванию дополнительных функций для каждого элемента. Это, в свою очередь, позволит более точно проводить анализ и определять подмножества элементов проверки, основные характеристики процесса их контроля (математическое ожидание, дисперсию и др.), а также вырабатывать рекомендации для времени начала проведения проверки в зависимости от требуемой достоверности контроля. Тем самым в перспективе ИМК

[10] Концептуальные основы судебной компьютерно-технической экспертизы. URL: http://www.dslib.net/kriminal-process/konceptualnye -osnovy - sudebnoj-kompjuterno -tehnicheskoj-jekspertizy.html

[11] Демидович Б. П., Марон И. А. Основы вычислительной математики : учеб. пособие. СПб. : Лань, 2011. 672 с.

может стать интеллектуальной системой выработки, поддержки и принятия решения. Быстро развивающийся аппарат теории нейронных сетей [17] позволит создавать такие ИМК, которые по имеющейся выборке (результатам) проведут самообучение, а затем сформулируют рекомендации по совершенствованию проверки при заданных показателях элементов рассматриваемой системы.

Рецензент: ***Омельченко Виктор Валентинович,*** *доктор технических наук, профессор, заслуженный деятель науки и техники РСФСР, советник секретариата научно-технического совета ВПК «НПО Машиностроения», г. Москва, Российская Федерация.*
E-mail: omvv@yandex.ru

Литература

1. Анин Б.Ю. Защита компьютерной информации. СПб. : БХВ-Санкт-Петербург, 2016. 384 с.
2. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. М. : Нолидж, 2014. 496 с.
3. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М. : Высшая школа, 2007. 479 с.
4. Демидович Б.П., Марон И.А., Шувалова Э.З. Методы приближенных вычислений. М. : Наука, 2015. 400 с.
5. Додонов А.Г., Ландэ Д.В. Живучесть информационных систем. К. : Наукова думка, 2011. 256 с.
6. Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. М. : Синтег, 2004. 496 с.
7. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
8. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2020. 314 с. ISBN: 978-5-93916-887-8.
9. Ловцов Д.А. Информационная теория эргасистем: Тезаурус. М. : Наука, 2005. 248 с.
10. Ловцов Д.А. Информационная безопасность и нетрадиционные угрозы // Федеральный справочник. Т. 8. Оборонно-промышленный комплекс России. М. : Центр стратег. исследований, 2013. С. 507—512.
11. Попков В.К. Математические модели связности : монография. Новосибирск : Изд-во ИВМиМГ СО РАН, 2006. 490 с.
12. Труханов В.М. Надежность технических систем. М. : Машиностроение-1, 2008. 585 с.
13. Федосеев С.В. Применение математических методов теории нечетких множеств при проведении судебно-экспертных исследований // Правовая информатика. 2020. № 4. С. 38—45. DOI: 10.21681/1994-1404-2020-4-38-45 .
14. Шелупанов А.А., Смолина А.Р. Форензика. Теория и практика расследования киберпреступлений. М. : Горячая линия — Телеком, 2019. 104 с.
15. Шувалов В.П., Егунов М.М., Минина Е.А. Обеспечение показателей надежности телекоммуникационных систем и сетей. М. : Горячая линия — Телеком, 2016. 168 с.
16. Goncharov V.V., Goncharov A.V., Shavrin S.S., Shishova N.A. The cyber-attack on the corporate network models theoretical aspects. Proceedings of the International Scientific Conference "2021 Systems of Signals Generating and Processing in the Field of On-Board Communications". Moscow, Media Publisher, 2021, pp. 188.
17. Gavrilov D.A., Lovtsov D.A. Automated visual information processing using artificial intelligence // Scientific and technical information processing. 2021. Vol. 48. No. 6. Pp. 436–445. DOI: 10.3103/S0147688221060034 .

METHODOLOGY FOR JUSTIFYING THE RATIONAL VARIANT OF TESTING THE FUNCTIONING OF TELECOMMUNICATION SYSTEMS AND NETWORKS

Vladimir Goncharov, *Dr.Sc. (Technology), Professor, Honoured Figure of Higher School of the Russian Federation, Head of the Department of Mathematics of the Peter the Great Military Academy, Moscow, Russian Federation.*
E-mail: v_v_goncharov@mail.ru

Aleksandr Goncharov, *external Ph.D. student at the Peter the Great Military Academy, Moscow, Russian Federation.*
E-mail: dinozavp@inbox.ru

Keywords: *telecommunication system, network, information security, element, set, subset of elements, device, object, control system, interpolation methods, spline interpolation.*

Abstract

Purpose of the paper: improving the research and methodological basis for enhancing the quality of testing the correct functioning of elements and devices of telecommunication systems and networks.

Methods: system analysis and pragmatic expert formation of subsets of tested elements of complex technical systems under the conditions of limited time for carrying out the tests.

Findings. A methodology for justifying the rational variant of testing telecommunication systems and networks was developed based on the formal separation of the set of elements to be tested into three non-overlapping subsets providing a local maximum for the reliability of controlling the performance of declared functions of both the studied elements themselves and the system as a whole. A justification for the algorithm is given, the feasibility and advisability of correcting the considered subsets during operating the system are proven.

The obtained results are the basis for setting up appropriate efficient information and mathematical support for testing the reliability of correct functioning of complex telecommunication systems and networks.

References

1. Anin B.Iu. Zashchita komp'iuternoi informatsii. SPb. : BKhV-Sankt-Peterburg, 2016. 384 pp.
2. Barsukov V.S., Vodolaznii V.V. Sovremennye tekhnologii bezopasnosti. M. : Nolidzh, 2014. 496 pp.
3. Venttsel' E.S., Ovcharov L.A. Teoriia sluchainykh protsessov i ee inzhenernye prilozheniia. M. : Vysshaia shkola, 2007. 479 pp.
4. Demidovich B.P., Maron I.A., Shuvalova E.Z. Metody priblizhennykh vychislenii. M. : Nauka, 2015. 400 pp.
5. Dodonov A.G., Lande D.V. Zhivuchest' informatsionnykh sistem. K. : Naukova dumka, 2011. 256 pp.
6. Kul'ba V.V., Kovalevskii S.S., Shelkov A.B. Dostovernost' i sokhrannost' informatsii v ASU. M. : Sinteg, 2004. 496 pp.
7. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
8. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2020. 314 pp. ISBN 978-5-93916-887-8.
9. Lovtsov D.A. Informatsionnaia teoriia ergasistem: Tezaurus. M. : Nauka, 2005. 248 pp.
10. Lovtsov D.A. Informatsionnaia bezopasnost' i netraditsionnye ugrozy. Federal'nyi spravochnik. T. 8. Oboronno-promyshlennyi kompleks Rossii. M. : Tsentr strateg. issledovanii, 2013, pp. 507–512.
11. Popkov V.K. Matematicheskie modeli sviaznosti : monografiia. Novosibirsk : Izd-vo IVMiMG SO RAN, 2006. 490 pp.
12. Trukhanov V.M. Nadezhnost' tekhnicheskikh sistem. M. : Mashinostroenie-1, 2008. 585 pp.
13. Fedoseev S.V. Primenenie matematicheskikh metodov teorii nechetkikh mnozhestv pri provedenii sudebno-ekspertnykh issledovanii. Pravovaia informatika, 2020, No. 4, pp. 38–45. DOI: 10.21681/1994-1404-2020-4-38-45 .
14. Shelupanov A.A., Smolina A.R. Forenzika. Teoriia i praktika rassledovaniia kiberprestuplenii. M. : Goriachaia liniia – Telekom, 2019. 104 pp.
15. Shuvalov V.P., Egunov M.M., Minina E.A. Obespechenie pokazatelei nadezhnosti telekommunikatsionnykh sistem i setei. M. : Goriachaia liniia – Telekom, 2016. 168 pp.
16. Goncharov V.V., Goncharov A.V., Shavrin S.S., Shishova N.A. The cyber-attack on the corporate network models theoretical aspects. Proceedings of the International Scientific Conference "2021 Systems of Signals Generating and Processing in the Field of On-Board Communications". Moscow, Media Publisher, 2021, pp. 188.
17. Gavrilov D.A., Lovtsov D.A. Automated visual information processing using artificial intelligence. Scientific and technical information processing, 2021. Vol. 48. No. 6. Pp. 436–445. DOI: 10.3103/S0147688221060034 .