ОЦЕНКА ЖИВУЧЕСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Искольный Б.Б.[1], Максимов Р.В.[2], Шарифуллин С.Р.[3]

Методика применима при сравнительной оценке распределенных информационно–телекоммуникационных сетей на предмет их способности обеспечивать информационных обмен между корреспондентами в условиях случайных и преднамеренных (компьютерные атаки, использование недекларированных возможностей программного обеспечения) программных помех (деструктивных программных воздействий). Воздействие на сеть случайных и преднамеренных помех, вызывающих цепочки отказов описано в модели деградации сети, основанной на теории перколяции. Результатом использования методики является повышение достоверности оценивания структур распределенных интегрированных информационно–телекоммуникационных сетей при вариации количества узлов и линий связи сети. Методика учитывает безопасность линий связи, которые в отличие от узлов невозможно изолировать от воздействий внешней среды.

Ключевые слова: *информационная безопасность, живучесть, интегрированные информационно–телекоммуникационные сети, преднамеренные помехи, маршрутизация, адаптация.*

DOI: 10.21681/2311-3456-2017-5-72-82

Введение

Случайные и преднамеренные программные помехи – это возмущения, снижающие качество распределенных интегрированных информационно-телекоммуникационных сетей (ИТКС): реальную скорость передачи данных (наличие избыточности служебной информации, содержащейся в каждом из фрагментов пакетов сообщений снижает реальную скорость передачи данных) и доступность средств связи (отказ в обслуживании информационных систем) посредством создания нештатной дополнительной нагрузки на процессы и устройства их реализующие [1, стр. 498-513].

Живучесть системы – это ее способность выполнять основные функции, несмотря на действие возмущений [1, 2].

Информационный обмен между защищенными сегментами ИТКС корреспонденты осуществляют через последовательность транзитных узлов и линий связи сетей связи общего пользования (ССОП). При этом динамически формируется структура ИТКС, включающая в себя все альтернативы маршрутов пакетов сообщений между корреспондирующими абонентами.

Возникает задача интегрированного оценивания качества подсистем, полностью или частично не принадлежащих оценщику. Она обусловлена использованием для информационного обмена больших и динамичных интегрированных ИТКС, практически непредсказуемо включающих в свой состав одни высоконадежные элементы (узлы и связи между ними, функционирующие в штатном режиме) и исключающих другие. То есть задача оценивания должна решаться в процессе структурирования ИТКС – постоянного изменения ее топологии и типологии ее элементов.

Реальные структуры ИТКС достаточно большие, поэтому задача оценки живучести ИТКС аналитическими методами не решается. В связи с этим такие задачи принято [3, 4, 5, 6] решать с помощью имитационного моделирования.

Недостатками известных и внедренных в практику методик оценивания ССОП являются:

- узость области применения, выраженная в том, что используют локальную адаптацию (охват корректировкой отдельных фрагментов) к вариациям структуры и качеству сетевых ресурсов при выборе пути прохождения информационных сообщений;

- недостаточно высокая достоверность результатов оценки структур ИТКС при увеличении количества узлов и линий связи (в то же время методики, не имеющие данного недостатка, применимы только для принятых бесконечными по количеству элементов – узлов и линий связи – структур).

1 Искольный Борис Борисович, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, Краснодар, Россия. E-mail: isk-boris@mail.ru

2 Максимов Роман Викторович, доктор технических наук, профессор, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, Краснодар, Россия. E-mail: rvmaxim@yandex.ru

3 Шарифуллин Сергей Равильевич, кандидат технических наук, доцент, Краснодарское высшее военное училище им. генерала армии С.М. Штеменко, Краснодар, Россия. E-mail: SharifullinSR@mail.ru

Низкая точность методик обусловлены:

- децентрализованной корректировкой маршрутов;

- неприемлемыми временными и ресурсными затратами на получение исходных данных по большому количеству элементов ИТКС;

- комбинаторной сложностью задачи поиска безопасных маршрутов на большом количестве элементов ИТКС;

- неприемлемо низкой чувствительностью показателей безопасности маршрутов, связанное с тем, что увеличение количества элементов ИТКС неизбежно приводит к увеличению количества маршрутов с близким значением показателя безопасности;

- отсутствием учета безопасности линий связи, которые в отличие от узлов невозможно изолировать от воздействий внешней среды, так как они не локализованы в пределах контролируемых зон. Возможна компрометация сети связи размещением пассивных средств злоумышленника на линиях связи или радиоэлектронным подавлением линий связи большой протяженности, что потребует значительных средств для поиска и устранения причин снижения значений комплексных показателей безопасности линий связи.

Цель методики – решение задачи сравнительной оценки живучести ИТКС, обеспечивающей повышение достоверности результатов оценки при вариации количества узлов и линий связи ИТКС от структур, размер которых можно принять конечным по количеству элементов, до больших структур, размер которых можно принять относительно бесконечным, в условиях воздействия на оцениваемые ИТКС преднамеренных и случайных программных помех, а также обеспечение адаптационных возможностей ИТКС в условиях воздействия дестабилизирующих факторов среды.

Повысить достоверность результата сравнительной оценки структур ИТКС можно путем учета перспективного снижения значений показателей безопасности (защищенности) узлов и линий связи, а также за счет учета критической области, занятой интервалом значений критического соотношения «опасных» и «безопасных» узлов и линий связи, полученных в экспериментах с различными случайными последовательностями.

Обеспечение адаптационных возможностей ИТКС в условиях воздействия дестабилизирующих факторов среды достигается выбором наилучшей (из числа допустимых альтернатив) структуры ИТКС, а также выбором наилучших решений для восстановления связи между транзитными узлами. Ассортимент альтернативных структур для этого предварительно находят мониторингом ССОП специализированным программным обеспечением (ПО) типа *Visual Route* или встроенными в операционные системы семейства *Windows* утилитами *tracert* (*traceroute* в *Unix*), *ping* и *pathping*.

Содержательная (физическая) постановка задачи

Маршрутизация пакетов сообщений в ИТКС и передача их по линиям связи для обеспечения информационного обмена между корреспондентами осуществляется в транзитных узлах ССОП.

Определение маршрута движения пакетов сообщений в ССОП является сложной задачей, так как между каждой парой корреспондентов существует большой ассортимент альтернативных маршрутов. Выбор маршрута осуществляют в узлах ССОП (маршрутизаторах операторов связи). Критериями выбора маршрута из числа допустимых альтернатив являются потенциальная пропускная способность и загруженность линий (каналов) связи; вносимые каналами задержки и их надежность; количество транзитных узлов ССОП и их надежность.

Для обеспечения безопасности информационного взаимодействия корреспондентов необходимо осуществлять сравнительную оценку альтернативных структур ИТКС, учитывающую способность обеспечить информационное взаимодействие корреспондентов в условиях преднамеренных и случайных программных помех, приводящих к снижению качества ИТКС и создающих нештатную нагрузку на процессы устройства, реализующие информационное взаимодействие.

Такая постановка задачи позволяет сформулировать следующие противоречия.

Противоречие между необходимостью обеспечить высокую достоверность результатов оценки и увеличением потребного для ее решения ресурса, вызванного вариацией количества линий и узлов связи ИТКС, подверженных влиянию помех.

Противоречие между потребностью дать оценку адаптационным возможностям ИТКС и необходимостью получения этой оценки перспективных значений показателей безопасности узлов и линий связи, учитывающих деструктивное воздействие среды.

Методика направлена на устранение указанных противоречий.

Интегральным показателем живучести ИТКС выбрана вероятность $P^{НС}$ нарушения связи между корреспондентами (абонентами), а показателем

живучести узла ИТКС – коэффициент доступности $K^{Д}_{i}$, где $i = 1, 2, 3, \ldots, n$, характеризующий его возможности по обеспечению абонентов услугами связи с требуемым качеством. Порядок получения значений показателей, частные критерии и их вклад в итоговую оценку изложены ниже по тексту.

Теоретической основой методики являются теории перколяции (от англ. *percolation* – протекание), математической статистики и вероятности. Воздействие на ИТКС преднамеренных и случайных программных помех, вызывающих последовательности отказов, аналогично представленному в работах [7, 8, 9] процессу протекания (перколяции) и дает возможность описать глобально, но простой форме процессы эпидемии на деградирующей структуре ИТКС. В рамках теории перколяции такая задача решается по узлам и по связям [8].

Модель деградации ИТКС, решение перколяционной задачи по узлам

Для достижения цели методики при решении перколяционной задачи по узлам осуществляют следующую последовательность действий. Задают исходные данные: схему связи органов управления; требования к показателям качества ИТКС и минимальное допустимое значение комплексного показателя безопасности Π^{Kmin}; идентификаторы узлов и наличие между ними линий связи. Структура и параметры распределенной ИТКС (типология ее элементов) определяются перечисленными исходными данными. При этом схема связи и требования к показателям качества ИТКС задает система вышестоящего уровня иерархии – система управления ведомства, в интересах которого организуют связь. Если информацию о структуре ССОП невозможно получить как исходные данные от оператора связи, то ее предварительно находят мониторингом ССОП специализированным ПО. Полнота и достоверность результатов мониторинга определяется количеством и взаимным расположением (пространственным размахом) средств мониторинга. Достоверность в данном случае определяется изоморфизмом результатов мониторинга и структуры реальной ССОП. Целесообразно иметь пункты мониторинга в каждом защищаемом сегменте ИТКС, подключенном к ССОП. Такое многоагентное ПО в результате позволит решать задачи подсистемы мониторинга топологии и типологии ИТКС для определения всего ассортимента альтернативных структур ИТКС для информационного обмена между органами управления [10, 11].

Показатель доступности (исправного действия) i-го узла ИТКС – коэффициент доступности, который вычисляют по формуле $К^{Д}_{i} = ((T_i - T^{П}_{i}) / T_i) \cdot 100\%$, где $T^{П}_{i}$ – длительность интервала времени, в течение которого абонентам недоступны с требуемым качеством услуги от узла связи (время «простоя»); T_i – суммарное время работы узла ИТКС. Воздействие на узел ИТКС случайных и преднамеренных помех создает нештатную (дополнительную) нагрузку на связь и устройства, ее реализующие. Как следствие, $T^{П}_{i}$ – длительность интервала времени, в течение которого абонентам недоступны с требуемым качеством услуги от узла связи (время «простоя») – увеличивается, а показатель доступности узла ИТКС – уменьшается. Опыт эксплуатации ИТКС и эксперименты на ее фрагментах показывают, что значение минимального допустимого значения показателя доступности должно быть задано в интервале $0{,}6 < К^{Дmin} < 1$.

Далее необходимо вычислить значения комплексного показателя безопасности для каждого узла ИТКС. Под комплексным показателем i-го узла ИТКС $\Pi^{К}_{i}$, понимают свертку (ее нормированное численное значение) параметров безопасности, характеризующую способность узла ИТКС противостоять реализации угроз безопасности. Расчет $\Pi^{К}_{i}$ можно вычислить разными способами: суммированием, или перемножением, или как среднее арифметическое значение параметров безопасности узла. Кроме этого в предварительно заданные исходные данные в качестве параметров ИТКС дополнительно задают минимальное допустимое значение комплексного показателя безопасности Π^{Kmin} для узлов ИТКС и альтернативные варианты подключения абонентов к ИТКС. Значение Π^{Kmin} задают как требование (то есть директивно) с учетом реализации функций безопасности, обеспечивающих уровень минимального доверия к производителю и эксплуатанту оборудования (регламентируется нормативно).

Опыт эксплуатации ИТКС и эксперименты на ее фрагментах показывают, что значение Π^{Kmin} должно задаваться в интервале $0{,}5 < \Pi^{Kmin} < 1$.

Затем необходимо сравнить значение вычисленного комплексного показателя безопасности $\Pi^{К}_{i}$ i-го узла ИТКС с предварительно заданным минимальным допустимым значением Π^{Kmin}.

При $\Pi^{К}_{i} < \Pi^{Kmin}$ запоминают i-й узел как «опасный», а при $\Pi^{К}_{i} \geq \Pi^{Kmin}$ узел запоминают как «безопасный». При увеличении в структуре ИТКС (до относительно большого количества) узлов связи существуют, как правило, альтернативы вариантов маршрутизации пакетов сообщений. Требуемую

живучесть и надежность систем связи достигают резервированием каналов связи и известными адаптивными способами маршрутизации (реализуемыми локально оборудованием операторов связи).

Пусть, например, j-й вариант идеализированной регулярной структуры ИТКС представляет собой структуру, в узлах которой размещены узлы связи (рис.1), p_j-я доля которых (узлы черного цвета) является «опасными», и возможность прохождения пакетов сообщений между абонентами №1 и №2 исключена. Из таких смежных узлов формируют цепочки (узлы и связи между ними черного цвета) и запоминают их. В приведенном примере видно, что при представленной на (рис.1, *а*), и (рис.1, *б*), p_j-й части «опасных» узлов из общего их количества ($p_j = 0{,}3$) существует большое количество альтернатив маршрутизации сообщений между абонентами ИТКС (узлы белого цвета и связи между ними на (рис.1, *б*), некоторые из которых показаны на рисунке стрелками).

Для учета перспективного снижения значений Π^{K}_{i}, вызванного воздействием случайных и преднамеренных помех на каналы связи и узлы ИТКС, необходимо увеличивать долю «опасных» узлов на величину Δp. Эту величину (Δp) задают в интервале $\Delta p = 0{,}01..0{,}2$ из требуемой точности результатов расчетов. Из рисунка, представленного на (рис.1, *в*), следует, что при p_j-й части «опасных» узлов, представленной на (рис.1, *в* и *г*), где $p_j = 0{,}5$, существует лишь 4 альтернативных варианта маршрутов пакетов сообщений между абонентами, по-

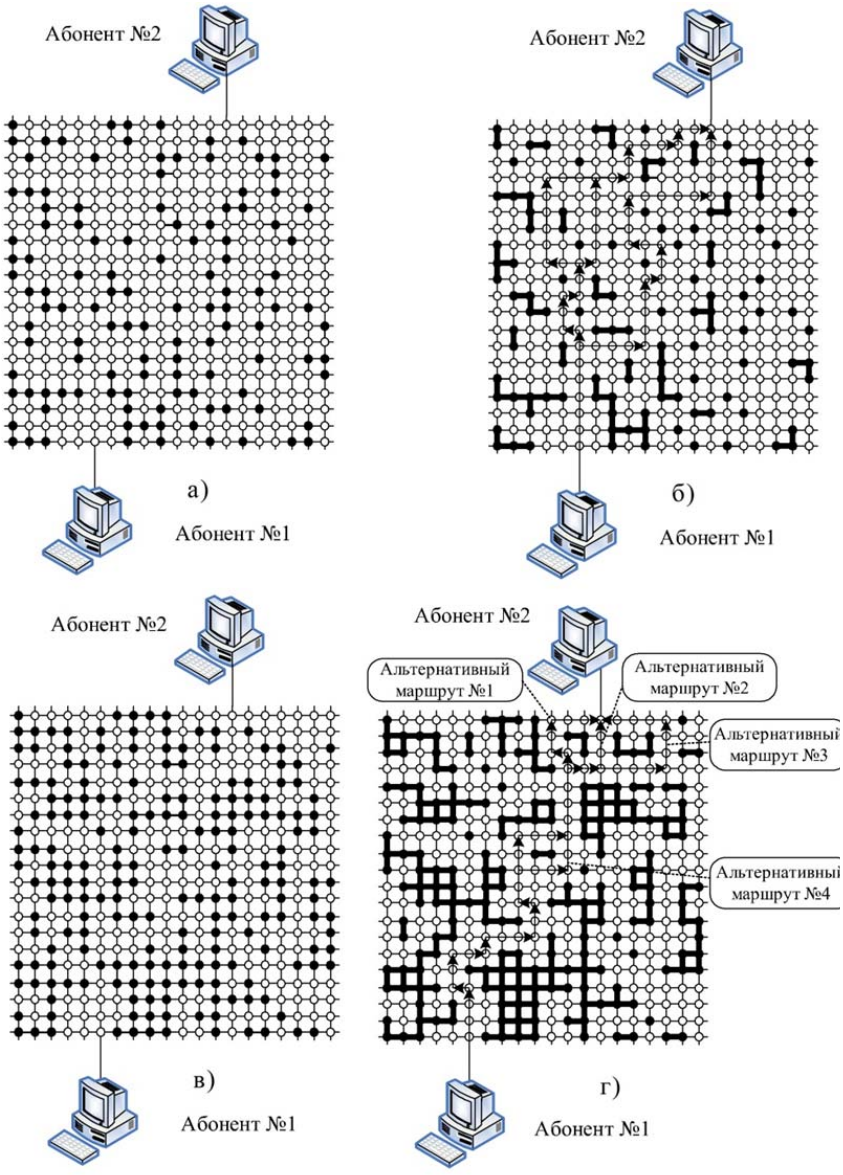

***Рис.1**. Вариант регулярной структуры ИТКС с различным количеством «опасных» узлов*

казанные на рисунке стрелками. Для того вычисления критического соотношения «безопасных» и «опасных» узлов p^k_j для каждого j-го варианта подключения абонентов, необходимо последовательно увеличивать на величину Δp (где, например, Δp = 0,01) долю «опасных» узлов до выполнения условий $p_j = p^k_j$, при котором смежные «опасные» узлы образуют цепочки, исключающие для абонентов возможность информационного обмена.

После вычисления критического соотношения «опасных» и «безопасных» узлов p^k_j для каждой альтернативной структуры ИТКС и ранжирования альтернативных вариантов подключения абонентов к ИТКС в соответствии со значениями p^k_j выбирают из них дополнительно варианты с допустимым значением (допустимые варианты) p^k_j ($p^k_j \geq p^{ДОП}$) и запоминают их [12, 13].

Затем необходимо вычислить показатель доступности каждого «опасного» $К^Д_i$ i-го узла ИТКС и сравнить его значение с предварительно заданным минимально допустимым $К^{Дmin}$. При $К^Д_i \geq К^{Дmin}$ необходимо запомнить i-й узел как «доступный», в противном случае, то есть при $К^Д_i < К^{Дmin}$, запомнить узел как «недоступный».

Затем необходимо последовательно уменьшить значение показателя доступности узла ИТКС $К^Д_i$ на величину Δd до выполнения условий $К^Д_i < К^{Дmin}$. Значение величины Δd задают в интервале Δd = 0,01 ÷ 0,1 из требуемой точности результатов расчетов.

Далее необходимо вычислить длительность интервала времени $Т^Д_i$, в течение которого выполнялось условие $К^Д_i \geq К^{Дmin}$.

Помехи, инжектируемые в одну или несколько точек ИТКС, снижают доступность узлов ИТКС. Графиками, представленные на (рис.2, б) и (рис.2, г), иллюстрируется динамика изменения количества узлов ИТКС во фронте действия помехи. Например (см. график на рис.2, б), в точке «Д» количество узлов ИТКС во фронте действия помехи равно 35 единицам на момент времени $t_1 \approx 90$ сек: то есть на девяностой секунде (с начала наблюдения) одновременно на 35-ти узлах ИТКС действуют помехи, уменьшающие значение $К^Д_i$ на величину Δd.

А за время t^k_j количество p_j «недоступных» узлов ИТКС достигнет значения p^k_j (точка «E_1» на (рис.2, а) и точка «E_2» на (рис.2, в)). Графики, представленные на (рис.3), демонстрируют динамику роста количества «недоступных» в ИТКС узлов связи в двух альтернативных вариантах структуры.

Далее необходимо ранжировать альтернативные варианты подключения абонентов по значению величины p^k_j (критического соотношения «опасных» и «безопасных» узлов). Для этого отмеряют на шкале времени значения t^k_j альтернативных (конкурирующих) структур ИТКС. Так, например, из графиков на (рис.2, *б*) и (рис.2, *г*): $t^k_1 \approx 260$ сек, $t^k_2 = 225$ сек.

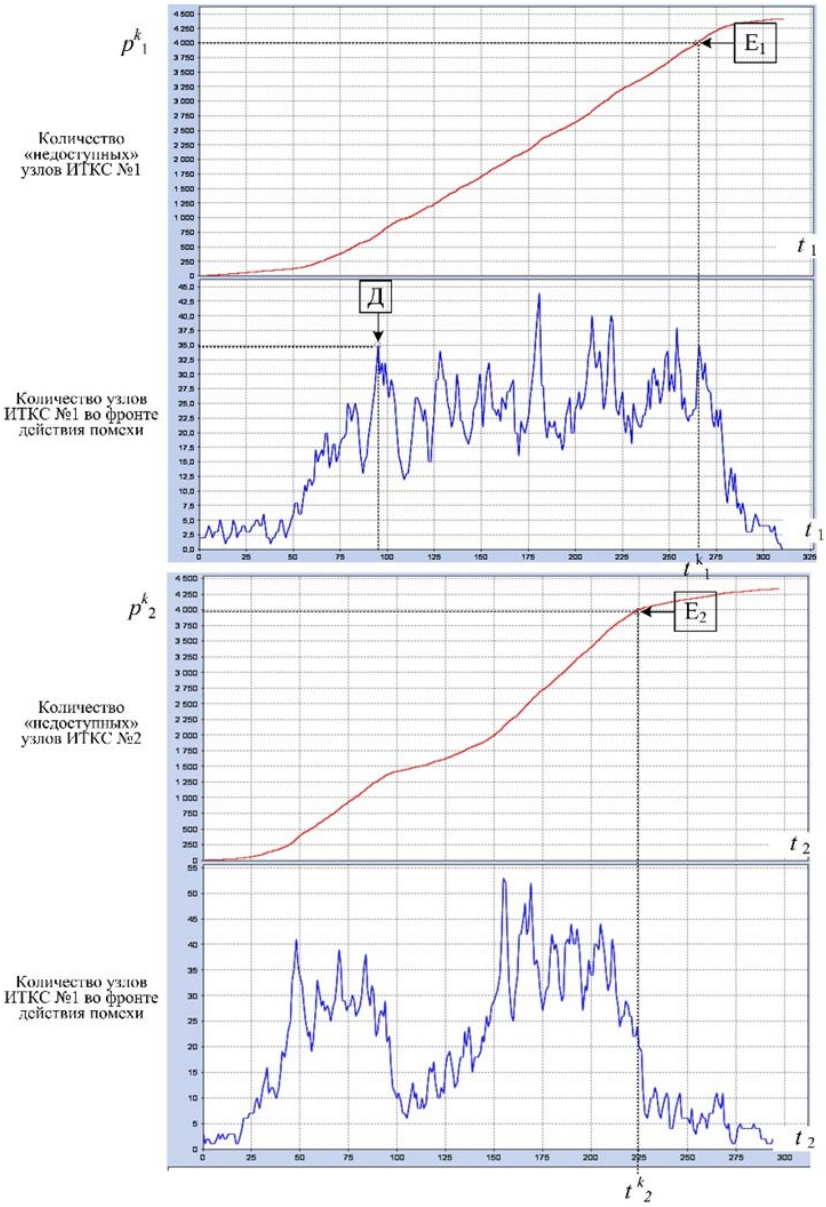

***Рис.2**. Графики, иллюстрирующие динамику роста количества «недоступных» узлов ИТКС в двух конкурирующих вариантах структуры ИТКС*

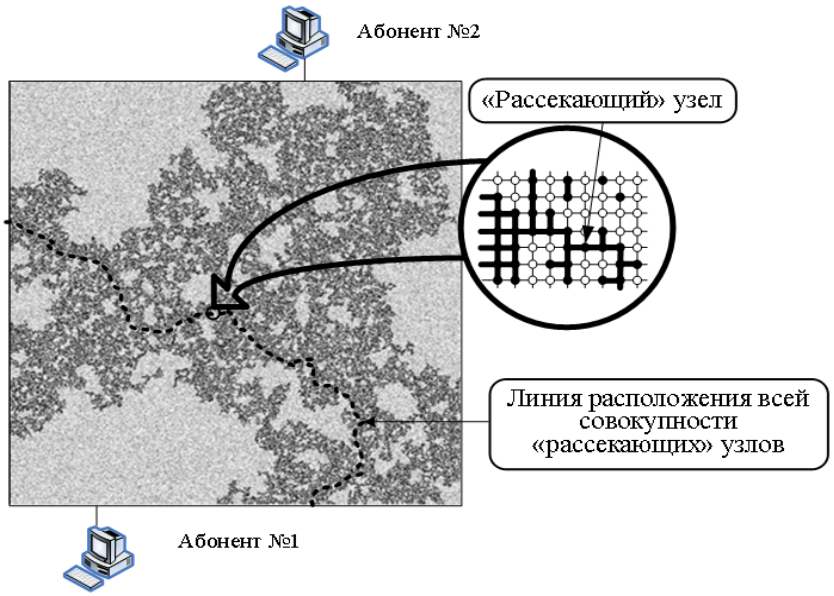

***Рис.3**. Графическая интерпретация «рассекающего» узла в ИТКС, размерностью 1000 на 1000 узлов связи*

Из двух конкурирующих (альтернативных) структур выбирают варианты со значением $t^k_j \geq t^{k\min}_j$ и запоминают их. Пусть $t^{k\min}_j = 250$ сек.

Тогда из графиков на (рис.2, *б*) и (рис.2, *г*) выбирают структуру № 1, т. к. $t^k_1 \approx 260$ сек, что соответствует условию $t^k_j \geq t^{k\min}_j$ (260 сек > 250 сек). Если $t^{k\min}_j < 225$ сек, то для выбора оснований недостаточно и необходим дополнительный критерий.

Совокупность «недоступных» узлов, связанных между собой, образует внутри ИТКС структуру – «кластер», свойства которого описывают, в частности, в [7, стр. 108-150]. Например, формулируют задачу поиска структурно обособленных ветвей кластера, связанных с его остовом через единственный узел. Эту задачу в предметной области сетей и систем связи целесообразно трактовать следующим образом: требуется найти все «недоступные» узлы ИТКС, «замена» любого из которых на «доступные» узлы приводит к разрушению кластера «недоступных» узлов и восстановлению связи между абонентами. Такие узлы именуют «рассекающими». Потенциальные возможности по восстановлению связи между абонентами в ИТКС тем больше, чем больше «рассекающих» узлов.

На (рис.3) в общей структуре ИТКС выделен один из «рассекающих» узлов.

Для поиска «рассекающих» узлов необходимо [14] вычислить показатель связности *N* каждого *i*-го «недоступного» узла ИТКС для каждого *j*-го подключения абонентов и задать минимальное значение показателя связности $N^{\min}$ «недоступных» транзитных узлов ИТКС. Выбрать те «недоступные» узлы ИТКС, показатель связности которых $N = N^{\min}$, и запомнить их. После этого увеличить значение $К^Д_i$ каждого *i*-го «недоступного» транзитного узла ИТКС до выполнения условий $К^Д_i \geq К^{Д\min}$ и проверить наличие связи между абонентами.

Если связь между абонентами не восстановилась, то увеличить значение минимального показателя связности $N^{\min}$ «недоступных» транзитных узлов ИТКС на единицу. Если связь между абонентами восстановилась, то запомнить *i*-й «недоступный» транзитный узел ИТКС как «рассекающий». На (рис.3) показана кривая расположения на кластере совокупности «рассекающих» узлов.

Далее для обоснования выбора структуры из числа альтернатив необходимо ранжировать альтернативные варианты ИТКС по количеству «рассекающих» узлов и выбрать вариант с максимальным значением количества «рассекающих» узлов ИТКС, обеспечивающим наибольшие потенциальные возможности по восстановлению связи между абонентами.

Вероятность $P^{НС}_j$ нарушения между корреспондентами связи для *j*-той структуры формализуют как функциональную зависимость, представленную на (рис. 4) от соотношения p^j «опасных» и «безопасных» узлов. Доля «опасных» узлов, где $p^j < p^j_k$, то есть относительно малая, обеспечивает допустимо малую (и даже пренебрежимо малую) вероятность нарушения связи между абонентами.

Вероятность нарушения связи резко возрастает при увеличении p^j до области критических значений вблизи $p^j_k \approx 0{,}6$, и при $p^j \to 1$ ($p^j > p^j_k$ на (рис.4)) возрастает до единицы. «Крутизна» зависимости связана с размахом структуры ИТКС. В [14] детально изложен алгоритм методики.

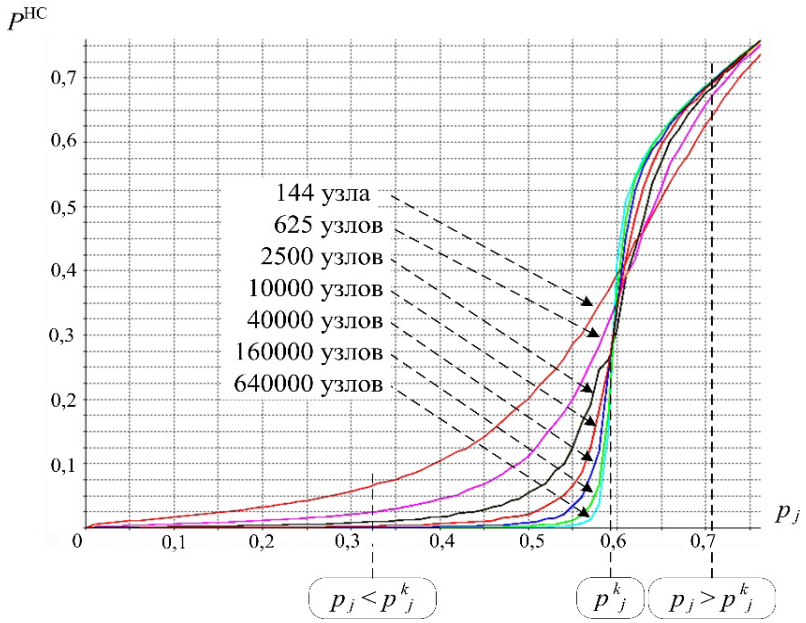

Рис.4. *Зависимость $P^{НС}_j$ от числа узлов, подверженных деструктивным воздействиям*

Сравнительная оценка конечных структур интегрированных ИТКС, решение перколяционной задачи по связям

Для конечных структур значение p^k_j – случайная величина, среднеквадратическое отклонение значений которой увеличивается по степенному закону с уменьшением числа узлов и (или) линий связи. Для конечных структур четко определяемого порога p^k_j не существует, а существует критическая область, занятая интервалом значений $p^{k_D}_j$, полученных в D экспериментах с различными случайными последовательностями [15]. Кроме этого, критическое значение p^k_j для узлов связи во всех практических топологиях ИТКС всегда меньше, чем для линий связи, так как при выходе из строя одного узла связи разрывается не одна линия связи, а все линии связи этого узла. Это означает, что полученная без учета линий связи оценка будет недостоверной.

Перколяционная задача по связям решается аналогично задаче по узлам. Предварительно задают параметры ИТКС и альтернативные варианты подключения абонентов. В качестве параметров задают идентификаторы узлов сети, линии связи между ними; минимальное допустимое значение комплексного показателя безопасности $П^{Лmin}$ для линий связи; общее количество D^{max} случайных испытаний, которое обеспечивает достоверность результатов экспериментов, номер испытания обозначают как $D = 1, 2, \ldots D^{max}$.

Имитационное моделирование деградации ИТКС при решении перколяционной задачи по связям осуществляется также, как и в рассмотренной выше задаче по узлам.

Выделяют массивы памяти для хранения идентификаторов абонентов и альтернативных маршрутов пакетов сообщений, двумерный массив памяти (табл.1) для хранения значений критического соотношения «опасных» и «безопасных» линий связи $p^{k_D}_j$ каждого из D случайных испытаний по каждому j-му варианту подключения абонентов, где $j = 1, 2, \ldots$. Формируют топологическую схему ИТКС, из которой выделяют альтернативные маршруты пакетов сообщений для каждой пары альтернативных вариантов подключений к ИТКС абонентов. Запоминают альтернативные маршруты пакетов сообщений для каждого j-го варианта подключения абонентов. Значение текущего количества случайных испытаний $D^{ТЕК}$ задают равным нулю.

Для учета перспективного снижения значений комплексных показателей безопасности линий связи, вызванного воздействием на линии связи ИТКС случайных и преднамеренных помех, необходимо увеличить долю «опасных» линий на величину Δp и найти $p^{k_D}_j$ – критическое соотношение «опасных» и «безопасных» линий связи для каждого j-го варианта подключения абонентов, при котором исключается информационный обмен между абонентами.

Для этого выбирают случайным образом из каждого ранее запомненного варианта подключения абонентов p^D_j -ю часть линий связи из общего их количества и запоминают их как «опасные», из смежных «опасных» линий связи формируют связанные цепочки и запоминают их, затем последовательно увеличивают долю

«опасных» линий связи на величину Δp и повторяют формирование связанной цепочки до выполнения условий $p_j^D = p_j^{k_D}$, запоминают критическое соотношение «опасных» и «безопасных» линий связи $p_j^{k_D}$ в двумерном массиве памяти (табл.1). Величину Δp задают исходя из требуемой точности результатов расчетов в интервале Δd = 0,01 ÷ 0,1. Результат вычисления $p_j^{k_D}$ заносят в таблицу двухмерного массива памяти для хранения значений критического соотношения «опасных» и «безопасных» линий связи (табл.1).

После этого увеличивают значение счетчика количества случайных испытаний $D^{\text{ТЕК}}$ на единицу, чем фиксируют номер случайного испытания.

Каждое случайное испытание $D^{\text{ТЕК}}$, осуществляемое в процессе экспериментов с помощью численного моделирования методом статистических испытаний Монте – Карло приводит к формированию различных структур из связанных между собой «опасных» линий связи и получению случайных значений $p_j^{k_D}$, которые запоминают в (табл.1), пока выполняется условие $D^{\text{ТЕК}} < D^{\max}$, ограничивающее общее количество случайных испытаний. Малая доля «опасных» линий связи $p_j^D = p_j^{k_D}$ обеспечивает пренебрежимо малую вероятность нарушения связи между абонентами ИТКС.

Общее количество $D^{\max}$ случайных испытаний, обеспечивающее достоверность результатов экспериментов, вычисляют по формуле $D^{\max} = Z_{\alpha/2}^2 / 4d^2$, где $Z_{\alpha/2}$ – стандартная нормальная статистика для искомой вероятности, d – приемлемая ошибка.

Альтернативный порядок вычисления количества $D^{\max}$ случайных испытаний при практической реализации имитационной модели $D^{\max}$ осуществляют следующим образом. Для каждого варианта подключения абонентов к ИТКС j сначала вычисляют очередное значение последовательности $p_j^{k_D}$, где $D = D^{\text{ТЕК}}$ а затем вычисляют среднее арифметическое $\overline{p_j^{k_D}}$ по всей совокупности вычисленных значений $p_j^{k_D}$, то есть итерационно. Полученная последовательность $\overline{p_j^{k_D}}$ стремится к точному решению при увеличении количества опытов $D^{\text{ТЕК}}$. Тогда критерием останова итерационного процесса будет $\left|\overline{p_j^{k_{D^{TEK}}}} - \overline{p_j^{k_{D^{TEK-1}}}}\right| \le \varepsilon$, где ε – приемлемая ошибка. Значение приемлемой ошибки задают декларативно, исходя из требуемой точности вычислений. Диапазон значений ε зависит от степени различия сравниваемых структур ИТКС и из опыта вычислений находится в интервале $0{,}01 \le \varepsilon \le 0{,}1$. После завершения итерационного процесса $D^{\max}$ будет равно $D^{\text{ТЕК}}$.

При выполнении условия $D^{\text{ТЕК}} \ge D^{\max}$ вычисляют значение показателя центра распределения выборки $\overline{p_j^{k_D}}$ по всей совокупности $D^{\max}$ случайных испытаний для каждого j-го варианта подключения абонентов как математическое ожидание, или среднее арифметическое, или среднее геометрическое, или среднее гармоническое, или среднее степенное, или среднее взвешенное, или медиану, или моду значений $p_j^{k_D}$ по всей совокупности из D случайных испытаний по каждому j-му варианту подключения абонентов. Результаты расчета показателей центра распределения выборки $\overline{p_j^{k_D}}$ по всей совокупности $D^{\max}$ случайных испытаний для двух альтернативных структур ИТКС и $D^{\max}$ = 6 представлены в (табл.1). При этом в строке 1 (табл.1) записаны результаты расчетов для регулярной структуры ИТКС со связностью каждого узла связи, равной четырем. В строке 2 (табл.1) запомнены результаты расчетов для регулярной структуры ИТКС со связностью каждого узла связи, равной трем.

Среднее арифметическое вычисляют по формуле:

$$\overline{p_j^{k_{D^{\max}}}} = \frac{1}{D^{\max}} \sum_{D=1}^{D^{\max}} p_j^{k_D}. \qquad (1)$$

Таблица 1.

Двумерный массив памяти значений критических соотношения

D / j	1	2	3	4	5	$D^{\max}$=6	$\overline{p_j^{k_{D^{\max}}}}$	$G(p_j^{k_{D^{\max}}})$	$A_{-1}(p_j^{k_{D^{\max}}})$	$Me(p_j^{k_{D^{\max}}})$
1	0,726	0,548	0,262	0,738	0,250	0,417	0,490	0,447	0,406	0,482
2	0,565	0,318	0,271	0,129	0,341	0,071	0,282	0,231	0,179	0,294
⋮										

Например, для строки 1 (табл.1):

$$\overline{p_1^{k_6}} = \frac{1}{6}\sum_{D=1}^{6} p_1^{k_D} = \cdot$$

$$= \frac{(0{,}726 + 0{,}548 + 0{,}262 + 0{,}738 + 0{,}250 + 0{,}417)}{6} =$$

$$= 0{,}490 \ . \qquad (2)$$

Значения других показателей центра распределения выборки вычисляют аналогично по следующим формулам.

Среднее геометрическое вычисляют по формуле:

$$G(p_j^{k_{D^{\max}}}) = \sqrt[D^{\max}]{\sum_{D=1}^{D^{\max}} p_j^{k_D}} \ . \qquad (3)$$

Среднее гармоническое вычисляют по формуле:

$$A_{-1}(p_j^{k_{D^{\max}}}) = \frac{D^{\max}}{\sum_{D=1}^{D^{\max}} \frac{1}{p_j^{k_D}}} \cdot \qquad (4)$$

Среднее степенное вычисляют по формуле:

$$A_d(p_j^{k_{D^{\max}}}) = \sqrt[d]{\frac{\sum_{D=1}^{D^{\max}} p_j^{k_D}}{D^{\max}}} \ . \qquad (5)$$

Среднее степенное зависит от параметра d. При $d = 1$ среднее степенное равно среднему арифметическому, а при $d = -1$ среднему гармоническому.

Для расчета медианы необходимо ранжировать (сортировать по убыванию) вычисленные значения $p_j^{k_D}$. Если $D^{\max}$ – нечетное число, то медиана будет соответствовать центральному значению полученной сортированной последовательности. Если $D^{\max}$ – четное число, то медиана будет равна среднему арифметическому двух центральных значений полученной сортированной последовательности.

Понятия «альтернативные варианты подключения абонентов ИТКС» и «альтернативные структуры ИТКС» являются синонимами – равнозначными с точки зрения применения изложенного порядка сравнения альтернатив. Если структура ИТКС нерегулярная, то при различных вариантах подключения к ней абонентов между этими абонентами образуются различные структуры ИТКС, как альтернативные пути передачи пакетов сообщений.

После этого ранжируют альтернативные варианты подключения абонентов к ИТКС по значению величины показателя центра распределения выборки, и выбирают из их вариант с максимальной величиной значения показателя центра распределения выборки $\overline{p_j^{k_D}} \to \max$. Для примеров расчетов, представленных в таблице (см. табл.1), максимальную величину значения показателя центра распределения выборки имеет вариант, записанный в строке 1.

После осуществления сравнительной оценки по всем приведенным выше показателям к сети связи подключают абонентов и осуществляют между ними информационный обмен. Детальные алгоритмы, описывающие последовательность действий по многоэтапной сравнительной оценке, приведены в [12, 13, 14, 15].

Заключение

При работе ИТКС случайные и преднамеренные помехи неизбежны, что может привести к сбоям в работе ИТКС и, как следствие, системы управления ведомства [16, стр. 187-200]. Применением методики достигается решение задачи сравнительной оценки живучести ИТКС, обеспечивающей повышение достоверности результатов оценки при вариации количества узлов и линий связи в условиях воздействия преднамеренных и случайных программных помех, обеспечение адаптационных возможностей структуры ИТКС к дестабилизирующим факторам внешней среды, а также повышение достоверности результатов оценки структур, размер которых можно принять конечным по количеству элементов – узлов и линий связи, за счет учета критической области, занятой интервалом значений $p_j^{k_D}$ линий связи, полученных в экспериментах с различными случайными последовательностями.

***Рецензент**: Финько Олег Анатольевич, профессор, доктор технических наук, академический советник Российской академии ракетных и артиллерийских наук по отделению технических средств и технологий разведки, навигации, связи и управления, г. Краснодар, Россия, E-mail: ofinko@yandex.ru*

Литература

1. Давыдов А.Е., Максимов Р.В., Савицкий О.К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем // Москва, 2015. – 520 с.
2. Голуб Б.В., Кузнецов Е.М., Максимов Р.В. Методика оценки живучести распределенных информационных систем // Вестник Самарского университета. Естественнонаучная серия. 2014. № 7 (118). С. 221-232.
3. Daqing Li, Qiong Zhang, Enrico Zio, Shlomo Havlin, Rui Kang. Network reliability analysis based on percolation theory // Reliability Engineering and System Safety 142 (2015). P. 556-562.

4. Daqing Li, Bowen Fu, Yunpeng Wang, Guangquan Lu, Yehiel Berezin, H. Eugene Stanley, Shlomo Havlin. Percolation transition in dynamical traffic network with evolving critical bottlenecks // Proc Natl Acad Sci U S A. 2015 Jan 20; 112(3). P. 669-672.
5. Hyunseok Oh, Seunghyuk Choi, Keunsu Kim, Byeng D. Youn, Michael Pecht. An empirical model to describe performance degradation for warranty abuse detection in portable electronics // Reliability Engineering and System Safety 142 (2015). P. 92-99.
6. Максимов Р.В., Савинов Е.А. Оценка живучести распределенных интегрированных информационных систем // В сборнике: Информационные технологии и нанотехнологии (ИТНТ-2016) материалы Международной конференции и молодёжной школы. Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет); Институт систем обработки изображений РАН. 2016. С. 431-438.
7. Федер Е. Фракталы. – М.: Мир, 1991 – 254 с.
8. Эфрос, А.Л. Физика и геометрия беспорядка // Библ. «Квант», выпуск 19. – М.: Наука, 1982 – 264 с.
9. Grimmett, G. Percolation / G. Grimmett. Cambridge: Springer, 1999. 444 p.
10. Максимов Р.В., Выговский Л.С. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 1. № 72. С. 181-187.
11. Максимов Р.В., Выговский Л.С. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. Т. 3. № 60. С. 166-173.
12. Способ сравнительной оценки структур информационно-вычислительной сети: пат. 2408928 Рос. Федерация: МПК G 06 F 21/20 / Берест П.А., Богачев К.Г., Выговский Л.С., Зорин К.М., Игнатенко А.В., Кожевников Д.А., Краснов В.А., Кузнецов В.Е., Максимов Р.В.; заявитель и патентообладатель Военная академия связи имени С.М. Буденного. № 2009129726/08; заявл. 03.08.2009; опубл. 10.01.11, Бюл. №1. 16 с.: ил.
13. Способ сравнительной оценки структур сетей связи : пат. 2450338 Рос. Федерация: МПК G 06 F 15/00 / Игнатенко А.В., Ковалевский С.Г., Максимов Р.В., Озеров О.В., Тевс О.П., Шляхтенко Д.Б.; заявитель и патентообладатель Военная академия связи имени С.М. Буденного. № 2011119469/08; заявл. 13.05.2011; опубл. 10.05.12, Бюл. № 13. 16 с.: ил.
14. Способ сравнительной оценки структур сетей связи: пат. 2460123 Рос. Федерация: МПК G 06 F 13/00 / Апарин Н.Н., Астахов А.И., Жираковский А.А., Игнатенко А.В., Костарев А.Л., Максимов Р.В., Нехаев М.А.; заявитель и патентообладатель Военная академия связи имени С.М. Буденного. № 2011133438/08; заявл. 09.08.2011; опубл. 27.08.12, Бюл. № 24. 19 с.: ил.
15. Способ сравнительной оценки структур сети связи: пат. 2626099 Рос. Федерация: МПК G 06 F 15/00 / Искольный Б.Б., Лазарев А.А., Лыков Н.Ю., Максимов Р.В., Хорев Г.А., Шарифуллин С.Р.; заявитель и патентообладатель Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. № 2016145568; заявл. 21.11.2016; опубл. 21.07.2017, Бюл. № 21. 19 с.: ил.
16. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С. Маркова. – М.: ДМК Пресс, 2017. – 224 с.: ил.

EVALUATION OF THE SURVIVABILITY OF INTEGRATED INFORMATION-TELECOMMUNICATION NETWORKS

Iskolnyy B.B.[4], Maximov R.V.[5], Sharifullin S.R.[6]

The technique is applicable in case of comparative assessment of the distributed information and telecommunication networks regarding their ability to provide information exchange between correspondents in the conditions of accidentals and premeditated (the computer attacks, use of not declared software opportunities) program noises (destructive program influences). Impact on a network of the random and premeditated noises causing chains of failures is described in model of degradation of a network based on theories of percolation. Increase in reliability of estimation of structures of the distributed integrated information and telecommunication networks in case of a variation of quantity of nodes and communication lines of a network is result of use of a technique. The technique considers safety of communication lines which unlike nodes cannot be isolated from influences of an external environment.

Keywords: *information security, survivability, the integrated information and telecommunication networks, deliberate interference, routing, adaptation.*

4 Iskolnyy Boris Borisovich, Krasnodar General S. Shtemenko Military Institute, Krasnodar, isk-boris@mail.ru

5 Maximov Roman Victorovich, Dr.Sc., Professor, Krasnodar General S. Shtemenko Military Institute, Krasnodar, rvmaxim@yandex.ru

6 Sharifullin Sergey Ravilevich, Ph.D., Associate Professor, Krasnodar General S. Shtemenko Military Institute, Krasnodar, SharifullinSR@mail.ru

Reference

1. Davydov A.E., Maksimov R.V., Savickij O.K. Zashchita i bezopasnost' vedomstvennyh integrirovannyh infokommunikacionnyh sistem // Moskva, 2015. – 520 s.
2. Golub B.V., Kuznecov E.M., Maksimov R.V. Metodika ocenki zhivuchesti raspredelennyh informacionnyh sistem // Vestnik Samarskogo universiteta. Estestvennonauchnaya seriya. 2014. № 7 (118). S. 221-232.
3. Daqing Li, Qiong Zhang, Enrico Zio, Shlomo Havlin, Rui Kang. Network reliability analysis based on percolation theory // Reliability Engineering and System Safety 142 (2015). P. 556-562.
4. Daqing Li, Bowen Fu, Yunpeng Wang, Guangquan Lu, Yehiel Berezin, H. Eugene Stanley, Shlomo Havlin. Percolation transition in dynamical traffic network with evolving critical bottlenecks // Proc Natl Acad Sci U S A. 2015 Jan 20; 112(3). P. 669-672.
5. Hyunseok Oh, Seunghyuk Choi, Keunsu Kim, Byeng D. Youn, Michael Pecht. An empirical model to describe performance degradation for warranty abuse detection in portable electronics // Reliability Engineering and System Safety 142 (2015). P. 92-99.
6. Maksimov R.V., Savinov E.A. Ocenka zhivuchesti raspredelennyh integrirovannyh informacionnyh sistem // V sbornike: Informacionnye tekhnologii i nanotekhnologii (ITNT-2016) materialy Mezhdunarodnoj konferencii i molodyozhnoj shkoly. Samarskij gosudarstvennyj aehrokosmicheskij universitet imeni akademika S.P. Korolyova (nacional'nyj issledovatel'skij universitet); Institut sistem obrabotki izobrazhenij RAN. 2016. S. 431-438.
7. Feder E. Fraktaly. – M.: Mir, 1991 – 254 s.
8. EHfros, A.L. Fizika i geometriya besporyadka // Bibl. «Kvant», vypusk 19. – M.: Nauka, 1982 – 264 s.
9. Grimmett, G. Percolation / G. Grimmett. Cambridge: Springer, 1999. 444 p.
10. Maksimov R.V., Vygovskij L.S. Model' prednamerennyh destruktivnyh vozdejstvij na informacionnuyu infrastrukturu integrirovannyh sistem svyazi // Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikacii. Upravlenie. 2009. T. 1. № 72. S. 181-187.
11. Maksimov R.V., Vygovskij L.S. Model' prednamerennyh destruktivnyh vozdejstvij na informacionnuyu infrastrukturu integrirovannyh sistem svyazi // Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikacii. Upravlenie. 2008. T. 3. № 60. S. 166-173.
12. Sposob sravnitel'noj ocenki struktur informacionno-vychislitel'noj seti: pat. 2408928 Ros. Federaciya: MPK G 06 F 21/20 / Berest P.A., Bogachev K.G., Vygovskij L.S., Zorin K.M., Ignatenko A.V., Kozhevnikov D.A., Krasnov V.A., Kuznecov V.E., Maksimov R.V.; zayavitel' i patentoobladatel' Voennaya akademiya svyazi imeni S.M. Budennogo. № 2009129726/08; zayavl. 03.08.2009; opubl. 10.01.11, Byul. №1. 16 s.: il.
13. Sposob sravnitel'noj ocenki struktur setej svyazi : pat. 2450338 Ros. Federaciya: MPK G 06 F 15/00 / Ignatenko A.V., Kovalevskij S.G., Maksimov R.V., Ozerov O.V., Tevs O.P., SHlyahtenko D.B.; zayavitel' i patentoobladatel' Voennaya akademiya svyazi imeni S.M. Budennogo. № 2011119469/08; zayavl. 13.05.2011; opubl. 10.05.12, Byul. № 13. 16 s.: il.
14. Sposob sravnitel'noj ocenki struktur setej svyazi: pat. 2460123 Ros. Federaciya: MPK G 06 F 13/00 / Aparin N.N., Astahov A.I., ZHirakovskij A.A., Ignatenko A.V., Kostarev A.L., Maksimov R.V., Nekhaev M.A.; zayavitel' i patentoobladatel' Voennaya akademiya svyazi imeni S.M. Budennogo. № 2011133438/08; zayavl. 09.08.2011; opubl. 27.08.12, Byul. № 24. 19 s.: il.
15. Sposob sravnitel'noj ocenki struktur seti svyazi: pat. 2626099 Ros. Federaciya: MPK G 06 F 15/00 / Iskolnyy B.B., Lazarev A.A., Lykov N.YU., Maksimov R.V., Horev G.A., SHarifullin S.R.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche imeni generala armii S.M. SHtemenko. № 2016145568; zayavl. 21.11.2016; opubl. 21.07.2017, Byul. № 21. 19 s.: il.
16. Barabanov A.V., Dorofeev A.V., Markov A.S., Cirlov V.L. Sem' bezopasnyh informacionnyh tekhnologij / pod red. A.S. Markova. – M.: DMK Press, 2017. – 224 s.: il.