УДК 004.056.57, 519.16

МЕТОДИКА ОЦЕНКИ ЖИВУЧЕСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

© 2014 Б.В. Голуб, Е.М. Кузнецов, Р.В. Максимов[1]

Методика относится к области информационной безопасности информационных сетей и может быть использована при сравнительной оценке информационных сетей на предмет их устойчивости к отказам, вызванным воздействиями случайных и преднамеренных помех. Техническим результатом является повышение достоверности результатов сравнительной оценки структур информационных сетей. Для достижения технического результата учитывают динамику воздействия на узлы сети случайных и преднамеренных помех, а также возможности по восстановлению связи между транзитными узлами. Для этого вычисляют значения показателей доступности узлов информационных сетей, время достижения критического соотношения "опасных" и "безопасных" узлов для каждого варианта подключения абонентов, а также связность смежных "опасных" узлов, образующих цепочки, исключающие обмен между абонентами.

Ключевые слова: информационная безопасность, структура информационной сети, живучесть, преднамеренные помехи.

Область применения методики. Методика относится к области информационной безопасности интегрированных информационных систем и может быть использована при сравнительной оценке структур информационных систем, конкурирующих на предмет их реализации в условиях воздействия случайных (явления техногенного характера, такие как сбои, отказы и аварии систем обеспечения узла сети) и преднамеренных (умышленное использование дефектов программного обеспечения) программных помех (деструктивных воздействий).

Такие воздействия — это возмущения, снижающие качество информационных систем: реальную скорость передачи данных (фрагментация пакетов сообщений) и доступность узлов (средств) связи (отказ в обслуживании) посредством создания дополнительной (нештатной) нагрузки на процессы и устройства, их реализующие.

Живучесть — это способность информационных систем выполнить свои основные функции, несмотря на действие возмущений.

Информационный обмен между абонентами защищенных сегментов информационных систем (ИС) осуществляют маршрутизацией пакетов сообщений через последовательность транзитных узлов сетей связи общего пользования (ССОП). Совокупность альтернативных маршрутов пакетов сообщений между корреспондирующими абонентами составляет структуру ИС.

[1]Голуб Борис Владимирович (71us@mail.ru), Кузнецов Егор Михайлович (Tid63@yandex.ru), Максимов Роман Викторович (rvmaxim@yandex.ru), кафедра безопасности информационных систем Самарского государственного университета, 443011, Российская Федерация, г. Самара, ул. Акад. Павлова, 1.

Использование для информационного обмена интегрированных систем приводит к необходимости давать интегрированную оценку, то есть оценивать качество подсистем, не принадлежащих оценщику. Кроме того, что объекты оценки принадлежат третьим лицам, состоящие из них сети связи являются, безусловно, большими и динамичными. Можно говорить даже не о структуре ИС, а о процессе ее структурирования. Несмотря на то что элементы ИС (узлы и каналы связи) являются высоконадежными элементами при условии их функционирования в штатном режиме, информация о составе – элементы и связи между ними — постоянно меняется.

Недостатками известных методик являются:

отсутствие адаптации к изменениям структуры ССОП в части неполного учета качества сетевых ресурсов для выбора пути прохождения потоков сообщений;

отсутствие адаптации к изменениям структуры ССОП в части децентрализованной корректировки маршрутов, что приводит к охвату корректировкой не всей интегрированной ИС, а лишь отдельных ее участков;

относительно низкая достоверность результатов сравнительной оценки структур интегрированных ИС при увеличении количества узлов связи.

Низкая достоверность результатов сравнительной оценки и узость области применения известных методик обусловлены:

большими временными и ресурсными затратами, необходимыми для получения исходных данных по большому количеству узлов интегрированной ИС;

увеличением комбинаторной сложности решения задачи поиска безопасного маршрута при большом количестве узлов интегрированной ИС;

снижением чувствительности показателя безопасности маршрута, вызванное тем, что при увеличении количества узлов интегрированной ИС будет расти число маршрутов с близким значением показателя безопасности маршрута;

отсутствием процедур адаптации маршрута к изменениям структуры интегрированной ИС и изменению значений показателей безопасности узлов связи под воздействием помех.

Назначение методики. Целью методики является решение задачи сравнительной оценки живучести распределенных интегрированных ИС, обеспечивающей повышение достоверности результатов оценки при увеличении количества узлов связи и в условиях воздействия на узлы связи случайных и преднамеренных программных помех, а также обеспечение адаптации структуры интегрированной ИС к воздействиям дестабилизирующих факторов внешней среды.

Повышение достоверности результатов сравнительной оценки структур интегрированных ИС осуществляется путем учета перспективного снижения значений показателей защищенности узлов связи, вызванного воздействием случайных и преднамеренных программных помех.

Адаптация структуры интегрированной ИС к воздействиям дестабилизирующих факторов внешней среды осуществляется путем выбора наилучшей структуры ИС из числа допустимых альтернатив, а также восстановлением связи между транзитными узлами ИС. При этом поиск альтернатив может осуществляться путем мониторинга сети связи общего пользования специализированным ПО (утилиты *tracert*, *ping* и *pathping*).

Физическая (содержательная) постановка задачи. Информационный обмен между абонентами ИС осуществляют маршрутизацией пакетов сообщений через последовательность транзитных узлов сети.

Определение маршрута — сложная задача, особенно когда между каждой парой абонентов существует множество альтернативных маршрутов. При этом выбор маршрута осуществляют в узлах сети (маршрутизаторах) операторов связи. В качестве критериев выбора маршрутов выступают, например, номинальная пропускная способность; загруженность каналов связи; задержки, вносимые каналами; количество промежуточных транзитных узлов сети; надежность каналов и транзитных узлов сети.

Для обеспечения информационной безопасности интегрированных ИС необходимо осуществлять сравнительную оценку альтернативных структур интегрированных ИС на предмет их способности обеспечить информационный обмен между абонентами в условиях воздействия случайных и преднамеренных программных помех, снижающих качество интегрированной ИС и создающих дополнительную (нештатную) нагрузку на процессы информационного обмена и устройства, их реализующие.

Таким образом, возникает ряд противоречий:

между потребностью обеспечивать повышение достоверности результатов оценки и увеличением ресурсоемкости задачи оценивания в условиях увеличения количества узлов и связей интегрированной ИС, подверженных влиянию помех;

между потребностью оценивать адаптационные возможности интегрированной ИС и необходимостью учитывать для этого перспективное снижение значений показателей защищенности узлов связи.

На устранение указанных противоречий и направлена методика.

Показатели и критерии. Пусть интегральным показателем живучести интегрированных ИС является вероятность P нарушения связи между корреспондирующими абонентами, а показателем живучести узла ИС — коэффициент доступности $K_{\text{Д}}$, характеризующие его возможности по обеспечению абонентов услугами с требуемым качеством. Порядок вычисления значений показателей, частные критерии и их вклад в итоговую оценку изложены по тексту.

Теоретической основой методики являются теории систем управления, вероятности, математической статистики, перколяции. Теория перколяции (от англ. *percolation* — протекание) — одна из ветвей развития теории графов. Воздействие на ИС случайных и преднамеренных программных помех, вызывающих цепочки отказов, аналогично представленному в работах [1–4] процессу перколяции и дает возможность описать в простой форме глобально процессы деградации ИС наподобие эпидемии.

Исходные данные. В качестве основных исходных данных в методике выступают план связи (схема связи $\|a_{ij}\|$ органов управления и время $T_{\text{ИС}}^{\text{Общ}}$ органов управления и время $P_{HC}^{\text{Доп}}$ и минимальное допустимое значение коэффициента доступности $K_{\text{Д}min}$ узла ССОП, идентификаторы узлов ССОП и наличие линий связи между ними. Для достижения цели методики осуществляют следующую последовательность действий. Задают исходные данные:

план связи (схема связи $\| a_{ij} \|$ органов управления и время $T_{\text{ИС}}^{\text{Общ}}$ существования распределенной интегрированной ИС);

требования к показателям качества ИС $P_{\text{НС}}^{\text{Доп}}$ и $K_{\text{Д}min}$;

идентификаторы узлов сети связи общего пользования и наличие линий связи между ними.

Перечисленные исходные данные определяют структуру и параметры распределенной интегрированной ИС. При этом план связи и требования к показателям

качества ИС задает система вышестоящего уровня иерархии – система управления.

Структуру ССОП в том случае, если ее невозможно получить как исходные данные от оператора связи, выявляют путем мониторинга ССОП специализированным ПО (например, утилитами *tracert* (*traceroute* в ОС типа *Unix*), *ping* и *pathping*, встроенными в ОС *Windows*). Количество "точек", из которых ведется мониторинг, и их взаимное расположение определяют достоверность (полноту) результатов мониторинга. Достоверность в данном случае определяется изоморфизмом модели и истинной структуры ССОП. Пункты мониторинга целесообразно иметь в каждом защищенном сегменте ИС, подключаемом к сети связи общего пользования. В результате такое многоагентное ПО позволит решать задачи подсистемы мониторинга структуры и параметров ИС и определять альтернативные варианты структур ИС для подключения органов управления. Пример результата визуализации структур конкурирующих ИС представлен на рис. 1 [5; 6].

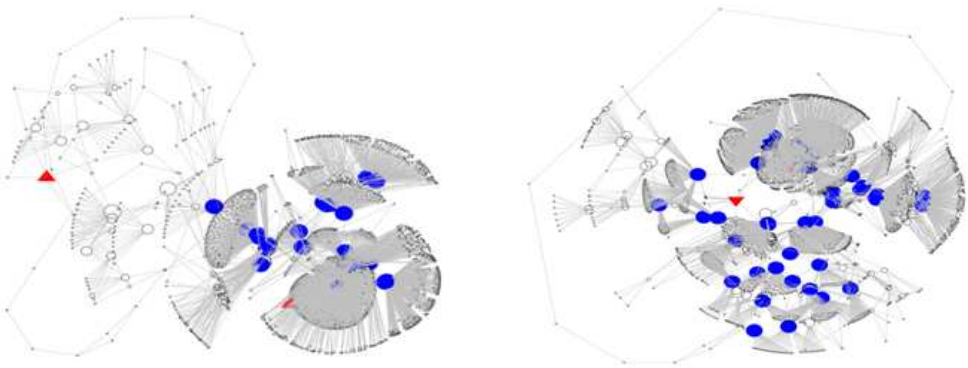

Рис. 1. Пример визуализации структур конкурирующих ИС

Под показателем доступности узла ИС понимается, например, коэффициент его доступности (исправного действия), который вычисляют по формуле $K_{\text{Д}} = ((T - T_{\text{П}}) \ / \ T)$ ffl 100%, где $T_{\text{П}}$ — длительность промежутка времени, когда абонентам ИС недоступны от узла услуги с требуемым качеством (время простоя); T — общее время работы узла ИС. Воздействие на узел ИС случайных и преднамеренных помех создает дополнительную (нештатную) нагрузку на процессы связи и устройства, их реализующие. В результате $T_{\text{П}}$ длительность промежутка времени, когда абонентам недоступны от узла ИС услуги с требуемым качеством (время простоя), увеличивается, а показатель доступности узла ИС уменьшается. Экспериментальные исследования и опыт эксплуатации ИС показали, что значение $\text{П}_{\text{Д}}$ должно задаваться в интервале $0{,}6 < \text{П}_{\text{Д}} < 1$.

Далее вычисляют комплексный показатель безопасности П_K для каждого узла ИС. Под комплексным показателем i-го, где $i = 1, 2, 3, \ldots$ узла ИС П_{K_i} понимается нормированное численное значение свертки параметров безопасности, характеризующее способность узла ИС противостоять угрозам безопасности. Расчет П_{K_i} вычисляют путем суммирования, или перемножения, или как среднее арифметическое значение его параметров безопасности. Кроме этого в предварительно заданные исходные данные в качестве параметров ИС дополнительно задают минимальное допустимое значение комплексного показателя безопасности $\text{П}_{K\,min}$ для узлов ИС и альтернативные варианты подключения абонентов к ИС.

Значение Π_{Kmin} задают директивно с учетом реализованных функций безопасности как минимальный уровень доверия к производителю оборудования (регламентируется нормативными документами). Экспериментальные исследования и опыт эксплуатации ИС показали, что значение Π_{min} должно задаваться в интервале $0{,}5 < \Pi_K < 1$.

Далее сравнивают значение ранее вычисленного комплексного показателя безопасности Π_{K_i} i-го узла ИС с предварительно заданным минимальным допустимым значением Π_{Kmin}.

При $\Pi_{K_i} < \Pi_{Kmin}$ запоминают i-й узел как "опасный", а при $\Pi_{K_i} \geqslant \Pi_{Kmin}$ запоминают узел как "безопасный". При большом количестве узлов связи в структуре ИС, как правило, существуют альтернативные варианты маршрутизации пакетов сообщений. Надежность и живучесть систем связи обеспечивают как резервированием каналов связи, так и известными адаптивными способами маршрутизации, реализуемыми в оборудовании операторов связи.

Пусть, для примера, вариант структуры ИС представляет собой регулярную структуру, в узлах которой размещены узлы связи (см. рис. 2), а p^j-я часть узлов из общего их количества является "опасными" (узлы черного цвета), исключающими возможность прохождения пакетов сообщений между абонентами № 1 и № 2. Из смежных "опасных" узлов формируют связанные цепочки и запоминают их (узлы и связи между ними черного цвета). Из приведенного примера, где $p^j = 0{,}3$, видно, что при представленной на рис. 2, *а* и рис. 2, *б* p^j-й части "опасных" узлов из общего их количества существует большое количество альтернативных вариантов маршрутизации пакетов сообщений между абонентами ИС (узлы белого цвета и связи между ними на рис. 2, *б*), три из которых показаны на рисунке стрелками.

Для того чтобы учесть перспективное снижение значений комплексных показателей безопасности узлов связи, вызванное воздействием на каналы связи и узлы ИС случайных и преднамеренных помех, необходимо увеличить долю "опасных" узлов на величину Δp. Величину Δp задают исходя из требуемой точности результатов расчетов в интервале $\Delta p = 0{,}01..0{,}2$. При представленной на рис. 2, *в* p^j-й части "опасных" узлов, где $p^j = 0{,}5$, из общего их количества существует только 4 альтернативных варианта маршрутизации пакетов сообщений между абонентами СС (узлы и связи между ними белого цвета на рис. 2, *г*), показанные на рисунке стрелками.

Для того чтобы вычислить критическое соотношение "опасных" и "безопасных" узлов p_k^j для каждого j-го варианта подключения абонентов, необходимо последовательно увеличивать долю "опасных" узлов на величину Δp (где, например, $\Delta p = 0{,}01$) до выполнения условий $p^j = p_k^j$, при котором смежные "опасные" узлы образуют цепочки, исключающие обмен между абонентами.

Схемы, представленные на рис. 3, иллюстрируют образование структур из связанных между собой "опасных" узлов на примере структуры ИС, реализованной как регулярная структура, размерностью $L = 1\,000\,000$ узлов связи (1 000 на 1 000 узлов связи) и связностью каждого узла, равной четырем. При этом на рис. 3 выполнены условия $p_i = p_k^j = 0{,}593$ (рис. 3, *а*) и $p^j > p_k^j = 0{,}594$ (рис. 3, *б*). После вычисления критического соотношения p_k^j для каждой альтернативной структуры ИС и ранжирования альтернативных вариантов подключения абонентов к ИС в соответствии со значениями p_k^j дополнительно выбирают из них варианты с допустимым значением p_k^j ($p_k^j \geqslant p_{\text{Доп}}$) и запоминают их [7; 8].

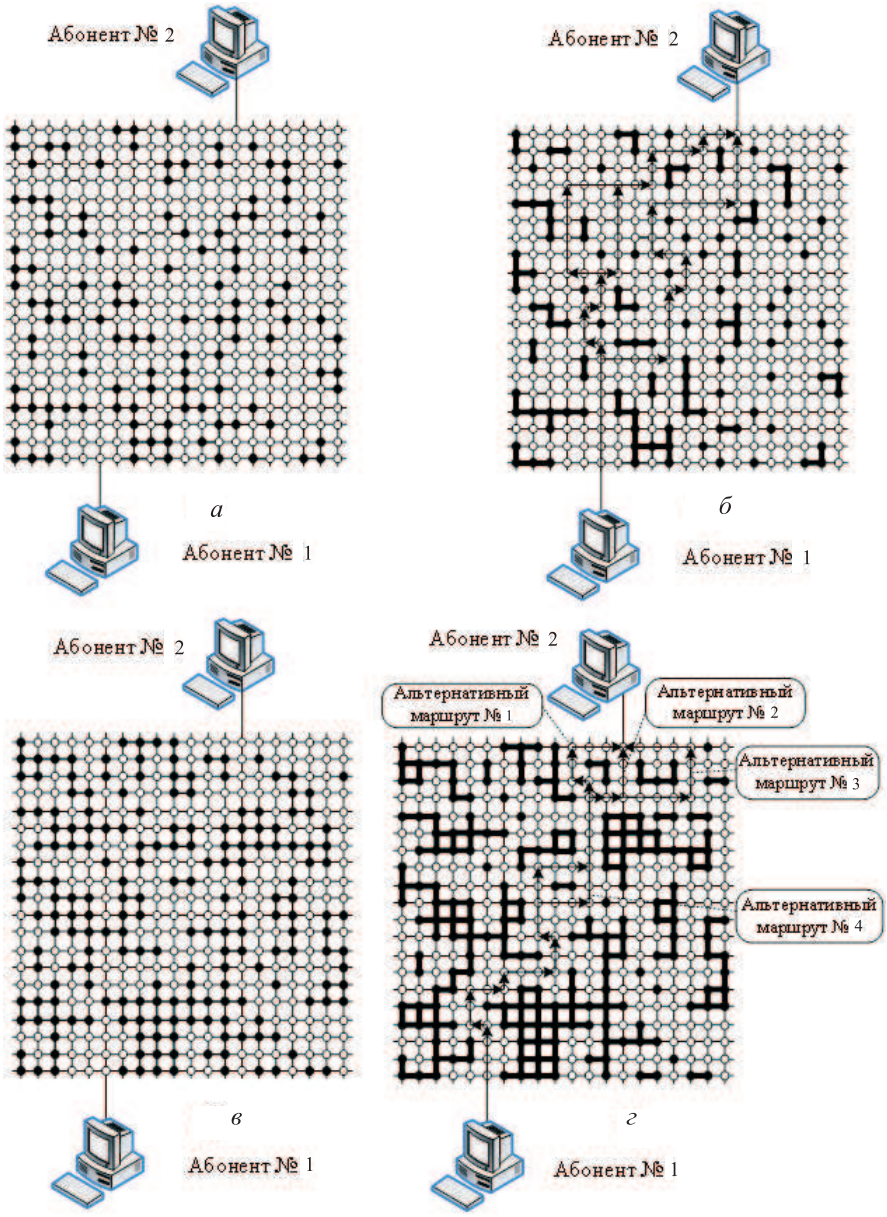

Рис. 2. Вариант регулярной структуры ИС с различным количеством "опасных" узлов

Далее вычисляют показатель доступности $К_Д$ для каждого "опасного" узла ИС и сравнивают значение показателя доступности $K_{Дi}$ i-го узла ИС с предварительно заданным минимальным допустимым значением $K_{Дimin}$. При $K_{Дi} \geqslant K_{Дimin}$ запоминают i-й узел как "доступный", в противном случае при $К_{Дi} < К_{Дimin}$ запоминают узел как "недоступный". Затем последовательно уменьшают значение показателя доступности узла ИС $К_{Дi}$ на величину Δd до выполнения условий

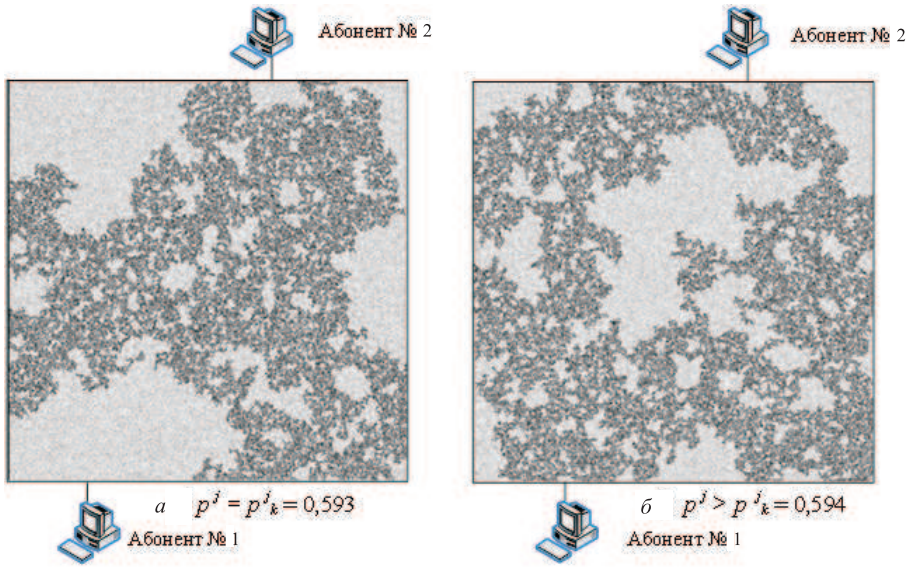

Рис. 3. Иллюстрация альтернативных структур размерностью L = 1 000 000 узлов связи (1 000 на 1 000 узлов связи)

$К_{Дi} < К_{Дimin}$. Величину Δd задают исходя из требуемой точности результатов расчетов в интервале $\Delta d = 0,01 \div 0,1$. Далее вычисляют длительность промежутка времени $T_{Дi}$, в течение которого выполнялось условие $К_{Дi} \geqslant К_{Дimin}$.

Помехи, инжектированные в одной или нескольких точках ИС, снижают доступность узлов ИС. Графики, представленные на рис. 4, *б* и рис. 4, *г*, иллюстрируют изменение количества узлов ИС во фронте действия помехи. Например, в точке "Д" на графике рис. 4, *б* количество узлов ИС во фронте действия помехи равно 35 на момент времени $t^1 \approx 90$ с. Это означает, что на девяностой секунде с начала наблюдения одновременно на 35-ти узлах ИС действуют помехи, уменьшая значение показателей доступности $К_{Дi}$ на величину Δd. А за время $t^j{}_k$ количество p^j "недоступных" узлов ИС достигнет значения p^j_k (точки "$Е^1$" и "$Е^2$" на рис. 4,*а* и рис. 4,*в*). Графики, представленные на рис. 6, иллюстрируют динамику увеличения количества "недоступных" узлов ИС в двух альтернативных вариантах структуры ИС.

Далее альтернативные варианты подключения абонентов ИС ранжируют по значению величины t^j_k. Для этого на шкале времени отмеряют значения t^j_k альтернативных (конкурирующих) структур ИС. Так, например, из графиков на рис. 4, *б* и рис. 4, *г*: $t^1_k \approx 260$ с, $t^2_k = 225$ с.

Из двух альтернативных структур выбирают варианты со значением $t^j{}_k \geqslant t^j{}_{k\,min}$ и запоминают их. Пусть $t^j{}_{k\,min} = 250$ с. Тогда из графиков на рис. 4, *б* и рис. 4, *г* выбирают структуру № 1, т. к. $t^1_k \approx 260$ с, что соответствует условию $t^j{}_k \geqslant t^j{}_{k\,min}$ (260 с > 250 с). Если $t^j{}_{k\,min} <$225 с, то оснований для выбора недостаточно. Необходим дополнительный критерий.

Совокупность связанных между собой "недоступных" узлов образует внутри ИС структуру ("кластер"), свойства которой описывают, например, в [1, с. 108–150]. В частности, выделяют задачу поиска обособленных ветвей,

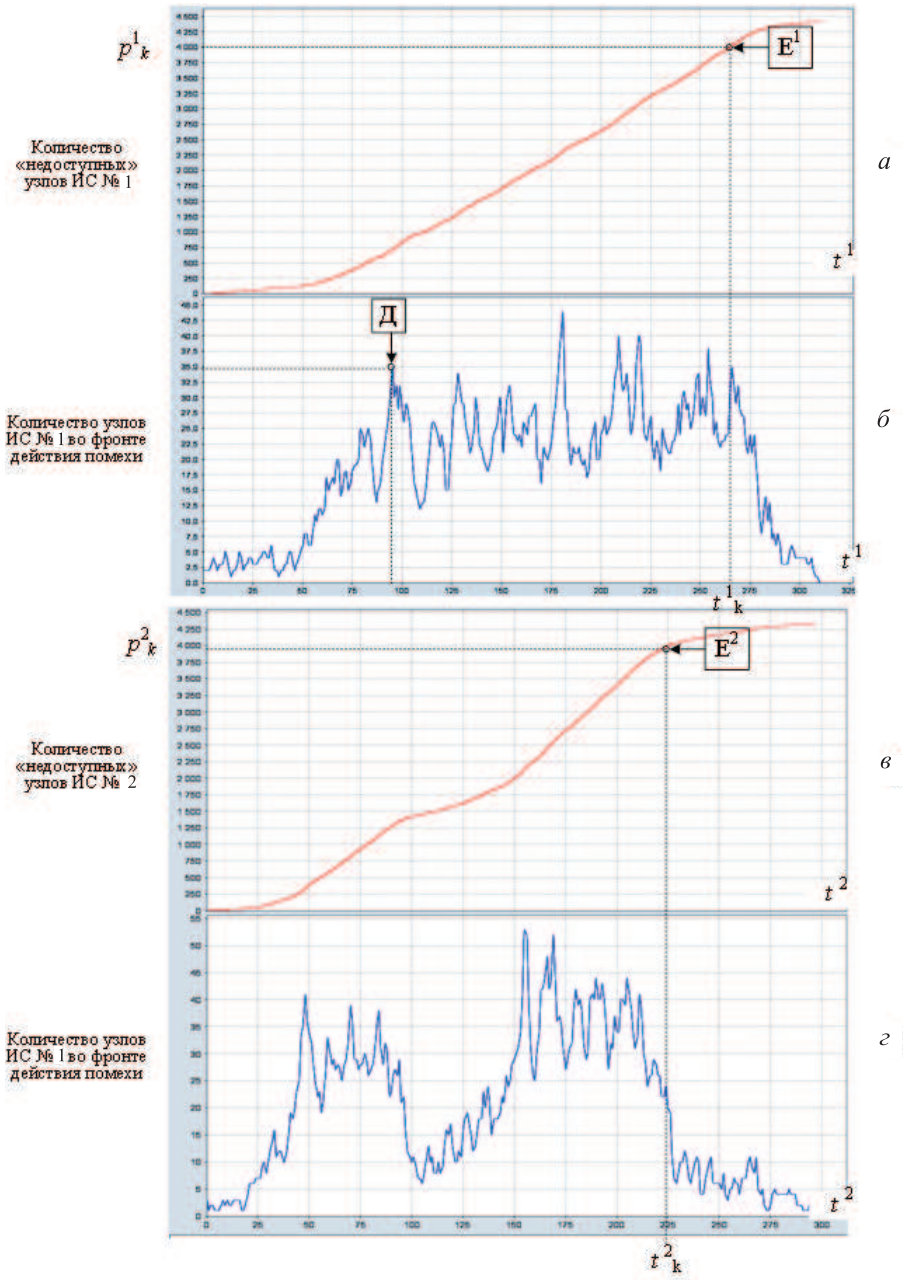

Рис. 4. Графики, иллюстрирующие динамику увеличения количества "недоступных" узлов ИС в двух альтернативных вариантах структуры ИС

связанных с остовом кластера через единственный узел. Эта задача в предметной области сетей и систем связи трактуется следующим образом.

Необходимо найти те "недоступные" узлы ИС, "замена" любого из которых на "доступные" узлы приводит к тому, что кластер, состоящий из "недоступных" узлов ИС связи, разрушается — связь между абонентами восстанавливается.

Здесь и далее такие узлы ИС именуются ”рассекающими”. Чем больше ”рассекающих” узлов в ИС, тем больше потенциальные возможности по восстановлению связи между абонентами.

На рис. 5 в общей структуре ИС выделен один из ”рассекающих” узлов.

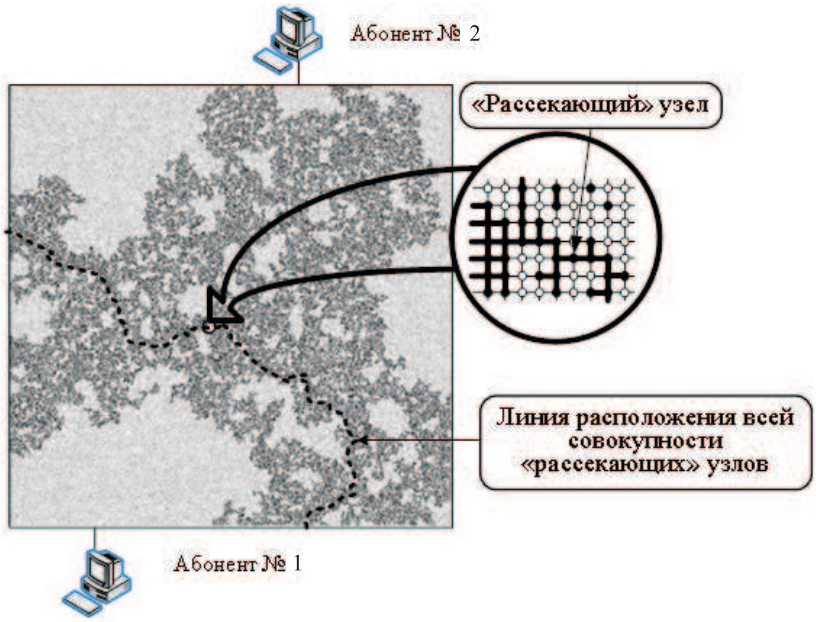

Рис. 5. Иллюстрация ”рассекающего” узла на структуре ИС, размерностью L = 1 000 000 узлов связи (1 000 на 1 000 узлов связи)

Для поиска ”рассекающих” узлов [9] вычисляют показатель связности N каждого i-го ”недоступного” транзитного узла ИС для каждого j-го варианта подключения абонентов и задают минимальное значение показателя связности N_{min} ”недоступных” транзитных узлов ИС. Выбирают те ”недоступные” транзитные узлы ИС, показатель связности которых $N = N_{min}$, и запоминают их. После этого увеличивают значение показателя доступности каждого i-го ”недоступного” транзитного узла ИС $K_{Дi}$ до выполнения условий $K_{Дi} \geqslant \mathrm{K}_{Дimin}$ и проверяют наличие связи между абонентами.

В случае отсутствия связи между абонентами увеличивают значение минимального показателя связности N_{min} ”недоступных” транзитных узлов ИС на единицу. В противном случае запоминают i-й ”недоступный” транзитный узел ИС как ”рассекающий”. На рис. 5 показана линия расположения всей совокупности ”рассекающих” узлов. Далее ранжируют альтернативные варианты подключения абонентов к ИС по количеству ”рассекающих” узлов ИС и выбирают вариант подключения абонентов к ИС с максимальным значением количества ”рассекающих” узлов ИС.

Вероятность P^j_{HC} нарушения связи между корреспондентами j-той структуры находят как функциональную зависимость (см. рис. 6) от соотношения p^j ”опасных” и ”безопасных” узлов. Малая доля ”опасных” узлов ($p^j < p^j_k$) обеспечивает пренебрежимо малую вероятность нарушения связи между абонентами ИС, тогда как при увеличении p^j вероятность нарушения связи резко возрастает вблизи

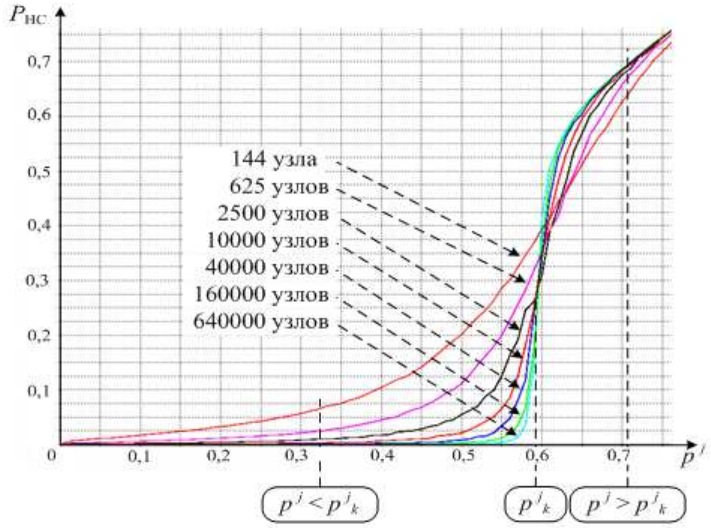

Рис. 6. Зависимость P^j_{HC} от числа узлов, подверженных деструктивным воздействиям

$p^j_k \approx 0{,}6$ и при $p^j \to 1$ ($p^j > p^j_k$ см. рис. 6) возрастает до единицы. "Крутизна" зависимости увеличивается с увеличением структуры ИС.

Таким образом, применением методики достигается решение задачи сравнительной оценки живучести распределенных интегрированных ИС, обеспечивающей повышение достоверности результатов оценки при увеличении количества узлов связи и в условиях воздействия на узлы связи случайных и преднамеренных программных помех, а также обеспечение адаптации структуры интегрированной ИС к воздействиям дестабилизирующих факторов внешней среды.

Научная новизна методики заключается в применении математического аппарата теории перколяции [10] в предметной области обеспечения информационной безопасности интегрированных информационных систем.

Практическая значимость заключается в обосновании выбора структуры ИС из числа конкурирующих альтернатив, осуществлении возможности адаптации структуры ИС к воздействиям дестабилизирующих факторов внешней среды.

Литература

[1] Федер Е. Фракталы. М.: Мир, 1991. 254 с.

[2] Эфрос А.Л. Физика и геометрия беспорядка // Библ. "Квант". Вып. 19. М.: Наука, 1982. 264 с.

[3] Grimmett G. Percolation. Cambridge: Springer, 1999. 444 p.

[4] Шкловский Б.И., Эфрос А.А. Электронные свойства легированных полупроводников. М.: Наука, 1979. 416 с.

[5] Выговский Л.С. Модель и метод оценки интегрированных объектов информатизации в условиях воздействия преднамеренных и непреднамеренных помех // Известия Санкт-Петербургского государственного электротехнического университета "ЛЭТИ". 2010. № 7. С. 26–30.

[6] Выговский Л.С. Метод, методика и способы обеспечения надежности интегрированных компьютерных сетей: дис. ... канд. техн. наук. СПб., 2011. 163 с.

[7] Способ сравнительной оценки структур информационно-вычислительной сети: пат. 2408928 Рос. Федерация: МПК G 06 F 21/20 / П.А. Берест, К.Г. Богачев, Л.С. Выговский [и др.]; заявитель и патентообладатель Военная академия связи имени С.М. Буденного. № 2009129726/08; Заявл. 03.08.09; Опубл. 10.01.11. Бюл. № 1. 16 с.

[8] Способ сравнительной оценки структур сетей связи: пат. 2450338 Рос. Федерация: МПК G 06 F 15/00 / А.В. Игнатенко, С.Г. Ковалевский, Р.В. Максимов [и др.]; заявитель и патентообладатель Военная академия связи имени С.М. Буденного. № 2011119469/08; Заявл. 13.05.11; Опубл. 10.05.12. Бюл. № 13. 16 с.

[9] Способ сравнительной оценки структур сетей связи: пат. 2460123 Рос. Федерация: МПК G 06 F 13/00 / Н.Н. Апарин, А.И. Астахов, А.А. Жираковский [и др.]; заявитель и патентообладатель Военная академия связи имени С.М. Буденного. № 2011133438/08; Заявл. 09.08.11; Опубл. 27.08.12. Бюл. № 24. 19 с.

[10] Massachusetts Institute of Technology // Percolation Theory. URL: http://www.mit.edu/ levitov/8.334/notes/ percol_notes.pdf (date of reference: 04.03.2003).

References

[1] Feder E. Fractals.: Mir, 1991, 254 p. (in Russian)

[2] Efros A.L. Physics and Geometry of Disorder. Bibl. "Kvant", issue 19. M., Nauka, 1982, 264 p. (in Russian)

[3] Grimmett G. Percolation. Cambridge: Springer, 1999. 444 p.

[4] Shklovskiy B.I., Efros A.A. Electronic properties of doped semiconductors. M., Nauka, 1979, 416 p. (in Russian)

[5] Vygovskiy L.S. Model and method for assessment of integrated computer network under the impact of intentional and unintentional interferences. *Izvestiia Sankt-Peterburgskogo gosudarstvennogo elektrotekhnicheskogo universiteta "LETI"* [Proceedings of Saint Petersburg State Electrotechnical University "LETI"], 2010, no. 7, pp. 26–30. (in Russian)

[6] Vygovskiy L.S. *Metod, metodika i sposoby obespecheniia nadezhnosti integrirovannykh komp'iuternykh setei: dis. ... kand. tekhn. nauk.* [Method, technique and means for ensuring of reliability of integrated computer networks: Candidate of Engineering Sciences thesis. SPb., 2011, 163 p. (in Russian)

[7] *Sposob sravnitel'noi otsenki struktur informatsionno-vychislitel'noi seti* [Method of comparative assessment of structures of information and computer networks: patent 2408928 Russian Federation: MPK G 06 F 21/20. P.A. Berest, K.G. Bogachev, L.S. Vygovskiy [et al.]; patent applicant and patent holder S.M. Budjonny Military Academy of the Signal Corps. No. 2009129726/08; applied 03.08.09; published 10.01.11, Bulletin no.1, 16 p. (in Russian)

[8] *Sposob sravnitel'noi otsenki struktur setei sviazi* [Method of comparative evaluation of communication network structures]: patent 2450338 Russian Federation: IPC G 06 F 15/00. A.V. Ignatenko, S.G. Kovalevskiy, R.V. Maksimov [et al.]; patent applicant and patent holder S.M. Budjonny Military Academy of the Signal Corps. No. 2011119469/08; applied 13.05.11; published 10.05.12, Bulletin no.1, 16 p. (in Russian)

[9] *Sposob sravnitel'noi otsenki struktur setei sviazi* [Method of comparative evaluation of communication network structures]: patent 2460123 Russian Federation: IPC G 06 F 13/00. N.N. Aparin, A.I. Astakhov, A.A. Zhirakovskiy [et al.]; patent applicant and patent holder S.M. Budjonny Military Academy of the Signal Corps. No. 2011133438/08; applied 09.08.11; published 27.08.12, Bulletin no.24, 19 p. (in Russian)

[10] Massachusetts Institute of Technology // Percolation Theory. Available at: http://www.mit.edu/ levitov/8.334/notes/ percol_notes.pdf (accessed: 04.03.2003).

Поступила в редакцию 21/ *V* /2014;
в окончательном варианте — 21/ *V* /2014.

METHOD FOR ESTIMATION OF VITALITY OF ALLOCATED INFORMATION SYSTEMS

© 2014 B.V. Golub, E.M. Kuznetsov, R.V. Maximov[2]

The method refers to the information security domain of information networks and can be used at a comparative estimation of information networks structures in order to determine their stability to the failures, caused by the impact of random or deliberate interferences. The destination is to improve results reliability of comparative estimation of information networks structures. To achieve technical result the dynamics of impact of random or deliberate interferences on information network nodes and also possibilities on communication recovery between transit nodes of information network are consider. For this purpose values of indexes of availability of information network nodes, time of achievement of critical ratio of "dangerous"and "safe"nodes for each variant of connection of subscribers, and also connectivity of adjacent "dangerous"nodes forming chains, eliminating exchange between subscribers are calculated.

Key words: information security, information network structure, stability, deliberate interferences.

Paper received 21/ *V* /2014.
Paper accepted 21/ *V* /2014.

[2]Golub Boris Vladimirovich (71us@mail.ru), Kuznetsov Egor Mikhailovich (Tid63@yandex.ru), Maksimov Roman Viktorovich (rvmaxim@yandex.ru), the Dept. of Security of Information Systems, Samara State University, Samara, 443011, Russian Federation.