svjazi_takticheskogo_zvena_upravlenija_sukhoputnykh_vojsk_ssha_2012/11–1–0–2120.
22. **Романюк В.А**. Мобильные радиосети — перспективы беспроводных технологий // Сети и телекоммуникации. — 2001. — № 12. — С. 62–68.
23. **Кучерявый Е.А**. Управление трафиком и качество обслуживания в сети Интернет. — СПб.: Наука и техника, 2004. — 336 с.
24. **Вегенша Ш.** Качество обслуживания в сетях IP: Пер. с англ. — М.: Вильямс, 2003. — 386 с.
25. **Куроуз Дж., Росс К.** Компьютерные сети: Пер. с англ., 2-е изд. — СПб.: Питер, 2004. — 765 с.
26. **Столлингс В.** Современные компьютерные сети. 2-е изд. — СПб.: Питер, 2003. — 783 с.
27. **Таненбаум Э.** Компьютерные сети: Пер. с англ. — СПб.: Питер, 2002. — 848 с.
28. **Бабков В., Мартиросова М.** Протоколы маршрутизации в самоорганизующихся пакетных радиосетях // Мобильные телекоммуникации. — 2009. — № 10. — С. 32–37.
29. **Карманов М.Л**. Протокол маршрутизации для ad hoc сетей // Вестник ЮУрГУ. — 2009. — № 26 (10). — С. 47–51.
30. **Метелев А.П., Чистяков А.В., Жолобов А.Н**. Протоколы маршрутизации в беспроводных самоорганизующихся сетях // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2013. — № 3 (1). — С. 75–78.
31. **Осипов Е.А**. Проблема реализации надежной передачи данных в самоорганизующихся и сенсорных сетях // Электросвязь. — 2006. — № 6. — С. 29–33.
32. **Perkins C.E., Bhagwat P.** Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers // Sigcomm, 1994. — P. 234–244.
33. **Perkins C.E., Belding-Royer E., Das S.** Ad Hoc On-Demand Distance Vector (AODV) Routing / RFC3561 // Онлайновый источник: www.ietf.org/rfc/rfc3561.txt.

Получено после доработки 25.12.14

УДК 621.391

ОРГАНИЗАЦИЯ ОПЕРАТИВНОГО УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ ИНТЕНСИВНЫХ ВОЗДЕЙСТВИЙ

К.Е. Легков, заместитель начальника кафедры АСУ Военно-космической академии им. А.Ф. Можайского, к.т.н.; constl@mail.ru
А.Н. Буренин, доцент кафедры АСУ ВКА им. А.Ф. Можайского, к.т.н.; konferencia_asu_vka@mail.ru

Сегодня средства информационного воздействия различных злоумышленников и нарушителей на телекоммуникационные сети и системы управления (СУ) достигли такого уровня, что могут нарушить нормальную работу инфокоммуникационной сети специального назначения (ИКС СН), воздействуя не только на нее, но и на СУ. Поэтому к организации управления ИКС СН предъявляются особые требования, включающие не только традиционные способы обеспечения информационной безопасности СУ, но и способы выработки управляющих воздействий. При этом обеспечение нормальной работы современных ИКС СН в условиях интенсивных воздействий (в том числе компьютерных атак) предполагает, что в самой СУ необходимо использовать специальные методы управления, позволяющие рационально организовывать работу ИКС СН. В соответствии с особенностями построения и условиями функционирования ИКС СН предлагаются различные варианты организации управления, обеспечивающие их нормальную работу при интенсивных воздействиях на сеть.

Ключевые слова: *инфокоммуникационная сеть, оперативное управление, интенсивные воздействия, управление, услуги, эффективность.*

Введение. В настоящее время в рамках различных ведомственных систем специального назначения (СН) создаются подсистемы, предназначенные для своевременного удовлетворения потребностей пользователей в санкционированных информационных и телекоммуникационных услугах. Эти сети, получившие название инфокоммуникационных сетей специального назначения (ИКС СН), развертываются на базе современных технических, технологических и организационных решений с широким использованием телекоммуникационных и информационных технологий. При этом ИКС СН задается совокупностью уровней (рис. 1), каждый из которых предоставляет определенный класс услуг (услуги инфраструктурного, промежуточного и базового уровней).

В качестве модели ИКС СН может быть использовано множество уровневых сетей услуг $G = \{G_i\}$ соответственно для инфраструктурного $i = 1$, промежуточного $i = 2$ и базового $i = 3$ уровней, каждый элемент которого G_i может быть описан неориентированным регулярным графом без петель $G_i(B_i, L_i)$, $i = 1,2,3$ с множеством вершин (узлов услуг) $B_i = \{B_{ij}\}$, $j = 1,...N_i$ и множеством ветвей (линий связи) $L_i = \{l_{ikj}\}$, соединяющих вершины.

Многочисленные разработанные в разные годы способы управления современными информационными и телекоммуникационными сетями, применение которых ограничено в сетях, основанных на принципах сетей следующего поколения (NGN) [1–5], не могут быть использованы в ИКС СН, так как организация управляемых процессов в них [6–8] должна быть распределенной по уровням архитектуры (см. рис. 1). Кроме того, подавляющее большинство известных способов управления сетями, во-первых, ориентировано на телекоммуникационные сети и может иметь только фрагментарное применение для ИКС СН, а во-вторых — используется тогда, когда системе управления доступна полная информация о сети и протекающих в ней процессах [1–5].

Поэтому при организации управления необходимо опираться на способы управления, реализация которых в СУ позволит обеспечить устойчивое и эффективное функционирование ИКС СН в сложных условиях.

Восстановление функционирования и организация управления ИКС СН. Архитектура современных ИКС СН

Рис. 1. **Архитектура современных ИКС СН**

содержит три основных уровня: инфраструктурный, промежуточный и базовый, на каждом из которых [6, 8] управление осуществляется по пяти основным задачам: управление производительностью уровня, безопасностью, структурой и адресацией, ресурсами уровня и сбойными ситуациями.

Обычно каждый уровень архитектуры ИКС СН представляют сетевыми моделями: совокупностью сетей прикладных услуг соответственно инфраструктурного, промежуточного уровней, а также телекоммуникационных сетей — транспортной сети, сетей доступа и сетей традиционной связи (ТЛФ, телеграфных, факсимильных и т.д.) [7, 8].

Вместе с тем в современных условиях имеющиеся и перспективные средства информационного воздействия на ИКС СН и особенно на их СУ достигли такого уровня, что стало возможно частично или полностью дезорганизовать их работу, воздействуя только на СУ. Поэтому для обеспечения работы современной ИКС СН с показателями качества не ниже требуемого уровня в условиях интенсивных воздействий, способных вывести из строя элементы или всю ИКС СН, целесообразно в саму систему управления заложить методы управления, позволяющие организовать работу сетей ИКС СН в сложных условиях.

Существенные изменения в функционировании ИКС СН могут быть вызваны как естественным выходом из строя различного оборудования, так и внешними причинами, связанными с чрезвычайными ситуациями и воздействием атак. Выходы из строя оборудования ИКС СН во многом прогнозируемы и могут быть учтены при ее проектировании и создании — в то время как чрезвычайные ситуации (ЧС) во многом являются неожиданными и непредсказуемыми. Анализ произошедших ЧС показывает, что средства связи ИКС СН повреждаются в зависимости от тяжести и пространства реализации ЧС. На практике средства связи ИКС СН повреждаются либо при объектовой ЧС, когда аварии происходят непосредственно на объектах связи, либо при региональной или глобальной ЧС, из-за воздействия внешних природных сил. Во время объектовых и местных ЧС, как правило, повреждаются местные узловые центры, проводные и воздушные линии связи.

Ввиду того что средства связи ИКС СН могут быть разрушены как непосредственно, так и в результате косвенного, вторичного воздействия, а также от природных явлений, необходимо четкое представление о характере возможных деструктивных изменений, чтобы максимально предусмотреть минимизацию или полное предупреждение потерь в услугах связи в условиях возникновения ЧС в месте расположения элементов ИКС СН.

Террористические акты следует рассматривать как один из возможных видов ЧС, имеющих по своим последствиям потери, соизмеримые с потерями, возникающими при других видах ЧС, включая землетрясения. Подчас не менее негативные последствия имеют массированные информационные воздействия.

Из-за непредсказуемости и многообразия возможных террористических актов и информационных воздействий предусмотреть защиту от них техническими способами практически невозможно, в то же время необходимы быстрое реагирование для устранения возможных повреждений и организация управления, минимизирующего последствия. При этом возникает задача принятия мер противодействия и защиты, которая математически сводится к отысканию максимума между затратами на разрушение и защиту (включая особые режимы управления) ИКС СН:

$$\Delta\theta_S = \max\{C(A_s) - d(A_s)\}, \quad A_s \in S_S, \qquad (1)$$

где $C(A_s)$ — затраты на разрушение элементов A_s ИКС СН; $d(A_s)$ — «доход», «выгода» от разрушения или ущерба ИКС СН, полученная разрушителем (нарушителем, противником).

В реальных условиях функционирования ИКС СН должны быть решены n подобных задач для объектов воздействий и наиболее вероятного разрушения.

Поскольку любая защита ИКС СН не исключает разрушения системы, это рано или поздно произойдет, и в этом случае должна быть решена задача восстановления ИКС СН и организации «чрезвычайного» управления. В задаче восстановления ИКС СН следует определить восстановительные средства, необходимые для обеспечения заданного уровня услуг связи потребителей в условиях деструктивных нарушений, стоимость которых должна быть минимальной при различных вариантах восстановления:

$$\Delta\phi_S = \min \sum_{k=1}^{n_k} \sum_{l=1}^{n_l} C_{lk}, \qquad (2)$$

где C_{lk} — стоимость l-го восстановительного средства на k-м элементе ИКС СН.

Эффективность функционирования ИКС СН определяется критериями надежности ее работы и обеспечения требуемого качества обслуживания пользователей из состава органов и пунктов управления (ПУ).

С точки зрения системы управления ИКС СН представляют собой сложное сочетание линий, каналов и трактов передачи информации, коммутационного и серверного оборудования, к эксплуатации которых предъявляются достаточно жесткие требования, обусловливающие нормальные режимы работы потребителей информационных и телекоммуникационных услуг. Естественно, что наиболее повреждаемыми элементами ИКС СН при чрезвычайных ситуациях являются линии связи, каналы и тракты передачи информации, а при информационных воздействиях — оборудование узлов (коммутационное, сервер-

ное). Поэтому первостепенное значение имеют действия оперативного персонала ПУ и служб эксплуатации ИКС СН по предотвращению повреждений и реализации информационных воздействий, восстановлению оборудования после аварий и разрушений, а также по созданию удовлетворительных условий работы оборудования узлов, восстановлению линий связи, каналов и трактов передачи информации.

При использовании автоматизированной системы управления (АСУ) ИКС СН с функциями эксплуатации и восстановления появляется возможность принятия более эффективных решений для ликвидации аварийных режимов и последствий информационных воздействий. Следовательно, необходима разработка соответствующего математического и программного обеспечения для анализа происходящих процессов при повреждении линий, каналов, трактов или оборудования узлов, изменения их работы под влиянием информационных воздействий (в том числе при блокировании их работы), а также для выдачи соответствующих рекомендаций по предотвращению ситуаций, способствующих развитию или усугублению деструктивных изменений в ИКС СН.

Естественно, что для обеспечения требуемого уровня надежности функционирования ИКС СН применяются все необходимые меры и средства повышения надежности программно-аппаратных средств узлов, линейного и каналообразующего оборудования.

При ликвидации последствий информационных воздействий, когда происходят сбои и отказы в работе или возникают чрезвычайные ситуации, можно выделить три основные группы системотехнических решений по обеспечению надежности функционирования и восстановления ИКС СН:

1. Решения, связанные с многоплановым резервированием программных средств (резервные копии операционных систем, другого программного продукта), с созданием и хранением резервных средств коммуникаций, резервных серверов, резервных источников питания, которые в случае необходимости могут быть подключены вместо вышедшего (выведенного) из строя оборудования.

2. Решения, связанные с созданием функционально избыточных структур ИКС СН (резерв производительности серверов, коммутаторов и маршрутизаторов, мультиплексоров, резерв пропускной способности каналов и трактов) и с функциональными возможностями их использования при необходимости организации физических или логических подключений пользователей органов управления и ПУ к функционально дублирующим средствам, канальному ресурсу, используемым в процессе функционирования ИКС СН.

3. Решения по организации качественного управления ИКС СН, обеспечивающего устойчивое функционирование системы в условиях выведения из строя комплексов и средств, а также активных информационных воздействий на средства ИКС СН.

Первые две группы системотехнических решений достаточно изучены, широко применяются на практике и теоретически проработаны.

Третья группа представляет наиболее трудно реализуемую составляющую всех системотехнических решений, так как предполагает выработку достаточно сложных процедур управления, основанных на данных оперативного мониторинга состояния ИКС СН с обоснованным выбором процедур сбора, обработки и оценки параметров. Общая схема организации управления в условиях интенсивных воздействий и ликвидации последствий компьютерных атак (КА), при сбоях и отказах в работе оборудования и при функционировании в чрезвычайных ситуациях приведена на рис. 2.

В этом случае целесообразно применять различные способы управления ИКС СН, основанные на разработанных стратегиях, учитывающих специальное назначение ИКС СН и обеспечивающих повышенные требования по устойчивости и безопасности самих процедур управления. При этом очевидно, что в ЧС, в условиях массированного применения КА, при значительной структурной деградации самой ИКС СН потребуется принятие срочных управляющих воздействий, позволяющих ИКС СН оставаться в работоспособном состоянии.

Поэтому в контурах СУ ИКС СН целесообразно заложить процедуры чрезвычайного управления для решения всех задач как по восстановлению структуры ИКС СН и ликвидации последствий КА, так и по восстановлению максимально возможного уровня работоспособности оборудования, компонентов и всей инфокоммуникационной сети в целом. Процедуры чрезвычайного управления должны обеспечить непрерывность функционирования ИКС СН в переходный период и приемлемый уровень качества предоставляемых услуг пользователям органов управления.

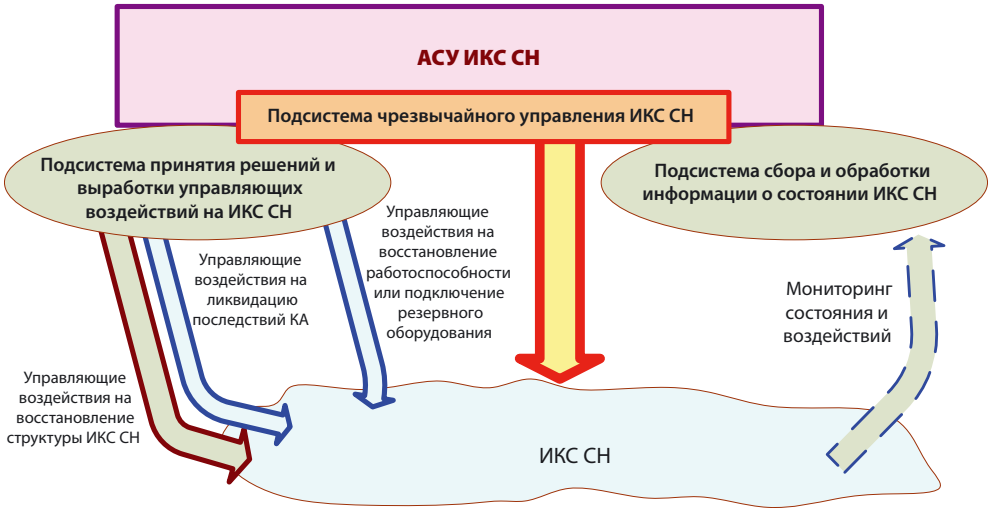


Рис. 2. **Организация управления в условиях интенсивных воздействий на ИКС СН**

Как основа процедур чрезвычайного управления могут быть предложены понятия обобщенного состояния ИКС СН, для которого характерна унификация состояний работоспособности и неработоспособности фрагментов, комплексов средств или отдельного оборудования независимо от того, чем вызвано это состояние (деструктивными изменениями или КА). При этом каждое возможное состояние ИКС СН $S_S(t)$ определяется кортежем (тройкой) состояний каждого уровня $S_S(t) = \{S_S(1, t), S_S(2, t), S_S(3, t)\}$ соответственно для инфраструктурного $S_S(1, t)$, промежуточного $S_S(2, t)$ и базового $S_S(3, t)$ уровней.

Способы управления в условиях интенсивных воздействий. В условиях интенсивных воздействий противника, нарушителей или злоумышленников на средства ИКС СН, приводящих к существенным деструктивным изменениям в системе, или при ЧС возможности получения достоверных оценок состояния $S_S^o(t) = \{S_S^o(1,t), S_S^o(2,t), S_S^o(3,t)\}$ обычными средствами мониторинга в составе СУ существенно снижаются или даже отсутствуют. В этом случае для организации чрезвычайного управления ИКС СН могут быть применены способы, основанные на построении эквивалентного «рельефа» (прямое применение способа рельефов) в модели каждой уровневой сети [5, 9], если деструктивные изменения не столь велики, или способы на основе поисковых процедур [9, 10], если деструктивные изменения значительны и полностью нарушено функционирование управляющей сети СУ [7].

Оценка обеспечения качества обслуживания пользователей ИКС СН при организации управления на основе способа рельефов в условиях чрезвычайных ситуаций и интенсивных информационных воздействий в зависимости от значительности деструктивных изменений приведена на рис. 3.

Ясно, что в случае значительных деструктивных изменений в ИКС СН способы прямого управления [5, 9] не только не обеспечивают требуемое качество функционирования, но даже не гарантируют работоспособность ИКС СН. В этом случае возможно применение различных поисковых способов [9, 10]. Однако характерные для них низкая информативность, существенная загрузка сетей ИКС СН управляющей информацией, положительно коррелированной с пользовательской нагрузкой, приводят к низкой эффективности такого управления. Поэтому предлагается новый вариант поискового способа управления (рис. 4), основанный на использовании интеллектуальных поисковых зондов: способ интеллектуального зондового управления (СИЗУ).

Предлагаемый СИЗУ можно отнести к классу групповых детерминированных способов управления, которые целесообразно применять в условиях интенсивных воздействий при существенных деструктивных изменениях в ИКС СН. Способ состоит в том, что периодически через определенное время $\Delta t_П$ с каждого i-го узла ($У_i$) ИКС СН по соответствующей уровневой сети передаются две «волны» интеллектуальных зондов (ИЗ): поисковая $П_{LE}(t) = П_E(t)$ и ответная $O_{LE}(t) = O_E(t)$.

Поисковая волна ИЗ, которая при поступлении заявки на чрезвычайное управление посылается с $У_i$, транслируется всеми узлами уровневой сети и служит для обнаружения входящего узла $У_j$ (узла назначения), который и обеспечит обслуживание требования.

При этом предполагается одинаковая задержка ИЗ в каждом $У$, а ИЗ поисковой волны при обеспечении виртуальных соединений от $У_A$ к $У_E$ ($П_L$) распространяются по сети поэтапно (см. рис. 4, *а*). При этом обозначение $П_E(t_0)$ будет означать начальный момент (пуск) поисковой волны ИЗ $П_E$, а $П_E(t_i)$ — i-й момент прохождения сигналов волны $П_E$.

В памяти сервера или АРМ ДЛ фиксируется только тот ИЗ волны $П_E$, который пришел раньше других. При одновременном поступлении ИЗ $П_E$ с двух и более направлений фиксируется один из них либо процедурой случайного выбора, либо на основе конкретной локальной информации.

Ответная волна $ИЗ_2$ посылается входящим узлом $У_j$ уровневой сети после получения поискового ИЗ и также транслируется всеми узлами. При этом ИЗ заполняется $УК_j$ справочной информацией о своем состоянии и уровне воздействий (если такие данные имеются). Ответная волна $ИЗ_2$ не только служит для маркировки и оценки характери-

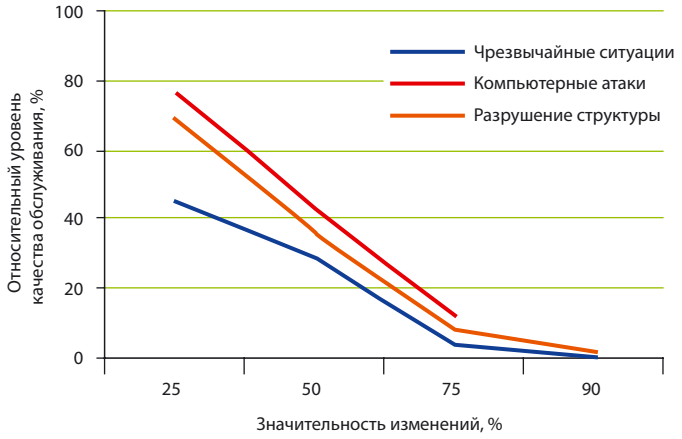


Рис. 3. **Качественные показатели ИКС СН при чрезвычайном управлении на основе способа рельефов**

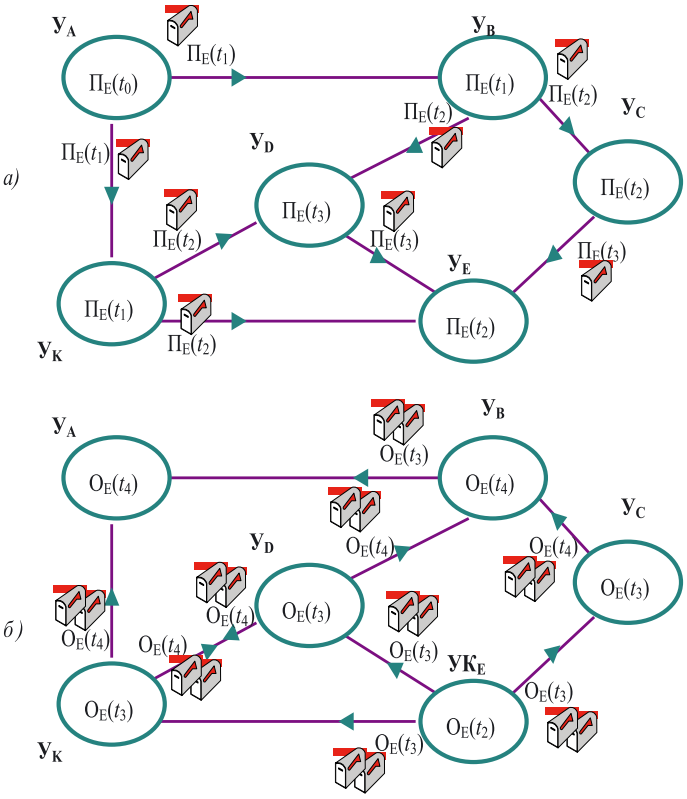
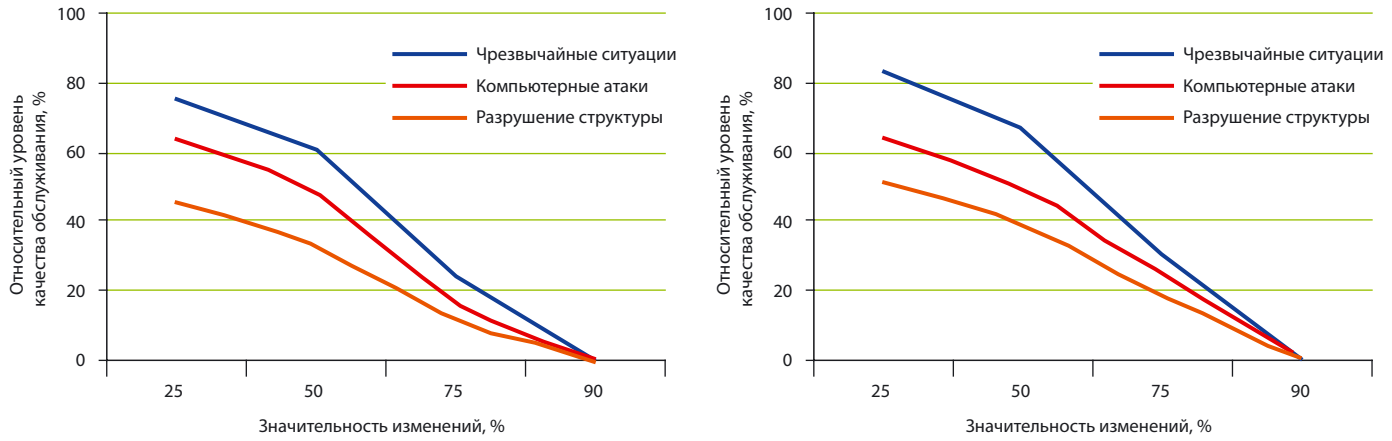


Рис. 4. **Способ интеллектуального зондового управления ИКС СН: *а* — процесс прохождения ИЗ волны $П_E$; *б* — процесс прохождения $ИЗ_2$ ответной волны $O_E(t)$**



а) *б)*

Рис. 5. **Качественные показатели ИКС СН при чрезвычайном управлении на основе СИЗУ:**
а — $\Delta t_{\Pi} = t_f$; *б* — $\Delta t_{\Pi} = 2\Delta t_f$

стик виртуального пути между исходящими и входящими *У*, но и выполняет функции по прекращению трансляции поисковых ИЗ, а также по сбору требуемой информации с транзитных *У* (минимально — фиксация номеров транзитных узлов).

Процесс прохождения $ИЗ_2$ ответной волны ($O_E(t)$) аналогичен процессу прохождения ИЗ волны $П_E$ (см. рис. 4, *б*), при этом начальный момент (пуск) ответной волны $O_E(t)$ совпадает с моментом поступления в $У_E$ первого ИЗ волны $П_E$ плюс время на «загрузку» информации в ИЗ (момент $t_2 + t_{z_i}$), т.е. плюс время преобразования ИЗ в $ИЗ_2$.

Кроме большей информативности, СИЗУ отличается от поисково-волнового способа управления тем, что здесь отсутствует фаза формирования зондов заключительной волны после получения ответных зондов.

Таким образом, первый $ИЗ_2$, пришедший на узел инициатор рассылки, показывает возможность, оптимальный путь и оценку полноты получения требуемых услуг соответствующего уровня ИКС СН (путь первого выбора), второй — путь второго выбора и т.д.

Для выбора пути на узле уровневой сети для каждого требования на обслуживание должна храниться следующая информация: номер и состояние входящего *У* (обеспечивающего обслуживание и предоставление услуги), вид зонда (поисковый ИЗ, ответный $ИЗ_2$), номер и другие характеристики исходящего *У*, т.е. узла, откуда поступила волна $П_E$.

В целом, оценивая качественные показатели функционирования ИКС СН в условиях интенсивных воздействий при управлении на основе применения СИЗУ (рис. 5), можно утверждать, что они существенно выше, чем при управлении на основе рельефных методов.

Периодичность посылки ИЗ определенным образом влияет на эффективность чрезвычайного управления ИКС СН (см. рис. 5). Вместе с тем слишком частая посылка ИЗ значительно загружает ресурсы уровневых сетей ИКС СН, которые в условиях интенсивных воздействий и так снижены. Формальных способов разрешения данного противоречия, очевидно, не существует, поэтому компромиссное значение Δt_{Π} выбирается на основе анализа результатов моделирования и корректируется в процессе эксплуатации ИКС СН в различных чрезвычайных условиях.

Заключение. Таким образом, для устойчивого и достаточно эффективного функционирования ИКС СН в условиях интенсивных воздействий на нее и СУ требуется организовать в СУ специальный контур чрезвычайного управления ИКС СН. В рамках данного контура чрезвычайного управления, в зависимости от выраженности структурных и функциональных деградаций ИКС СН, необходимо применять либо способ рельефов с периодической посылкой «минимальных векторов», либо способ интеллектуального зондового управления соответственно для умеренных и значительных деструктивных изменений в ИКС СН. При этом следует правильно выбрать периодичность посылки интеллектуальных зондов.

ЛИТЕРАТУРА

1. **Олифер В.Г., Олифер Н.А**. Компьютерные сети: принципы, технологии, протоколы. — СПб.: Питер, 2000. — 668 с.
2. **Лазарев В.Г., Фоломеев А.К**. Методы динамического управления потоками информации на сетях АТМ // Электросвязь. — 2004. — № 12. — С. 24–28.
3. **Ершов В.А., Ершова Э.Б**. Динамическая маршрутизация в широкополосной мультисервисной АТМ-сети //Электросвязь. — 2004. — № 2. — С. 16–18.
4. **Дымарский Я.С., Крутякова Н.П., Яновский Г.Г**. Управление сетями связи: принципы, протоколы, прикладные задачи. — М.: Связь и бизнес, 2003. — 384 с.
5. **Буренин А.Н**. Об управлении маршрутизацией на основе модифицированных адаптивных методов // Техника средств связи. — 1991. — № 7. — С. 51–59.
6. **Буренин А.Н., Легков К.Е**. Уровни управления инфокоммуникационными сетями в условиях сетецентрических конфликтов. // Тр. XIII Рос. науч.-техн. конф. «Новые информационные технологии в системах связи и управления», Калуга, 4 июня 2014 г. — Калуга: Ноосфера, 2014. — С. 54–56.
7. **Легков К.Е., Буренин А.Н**. Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // Наукоемкие технологии в космических исследованиях Земли. — 2012. — № 1. — С. 14–16.
8. **Легков К.Е.** К вопросу организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. — 2014. — № 5. — С. 34–40.
9. **Лазарев В.Г., Саввин Н.Г**. Сети связи, управление, коммутация. — М.: Связь, 1973. — 264 с.
10. **Лазарев В.Г**. Электронная коммутация и управление в узлах связи. — М.: Связь, 1974. — 271 с.

Получено после доработки 30.04.15