УДК 004.7

Н.А. Князева, И.В. Грищенко, С.В. Шестопалов
Научно-учебный институт холода, криотехнологий и экоэнергетики ОНАПТ,
ул. Дворянская, 1/3, г. Одесса, 65026, Украина

МЕТОД ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ НА ОСНОВЕ ПЕРЕРАСПРЕДЕЛЕНИЯ РЕСУРСОВ СЕТИ

В статье приведены показатели и параметры, характеризующие живучесть сети. Представлен метод обеспечения живучести телекоммуникационной сети ТКС на основе перераспределения ресурсов сети для обслуживания потоков требований при возникновении неблагоприятных воздействий позволяет:
- выполнить оценку работоспособности сети на основе предложенного показателя;
- выявить «узкие места» сети для возможности их резервирования.
Предложенный метод может быть использован на этапе проектирования ТКС для оценки работоспособности сети при изменении ее топологии.
Ключевые слова: *Телекоммуникационная сеть – Живучесть – Показатели – Критерии – Резервирование – Узел – Пропускная способность – Суммарная емкость*

Н.О. Князєва, І.В. Грищенко, С.В. Шестопалов
Науково-навчальний інститут холоду, кріотехнологій та екоенергетики ОНАХТ,
вул. Дворянська, 1/3, м. Одеса, 65026, Україна

МЕТОД ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ ПЕРЕРОЗПОДІЛУ РЕСУРСІВ МЕРЕЖІ

У статті наведені показники і параметри, що характеризують живучість мережі. Представлено метод забезпечення живучості телекомунікаційної мережі ТКС на основі перерозподілу ресурсів мережі для обслуговування потоків вимог при виникненні несприятливих впливів дозволяє:
- виконати оцінку працездатності мережі на основі запропонованого показника;
- виявити «вузькі місця» мережі для можливості їх резервування.
Запропонований метод може бути використаний на етапі проектування ТКС для оцінки працездатності мережі при зміні її топології.
Ключові слова: *Телекомунікаційна мережа – Живучість – Показники – Критерії – Резервування – Вузол – Пропускна здатність – Сумарна ємність*

I ВВЕДЕНИЕ

При проектировании телекоммуникационной сети (ТКС) возникает необходимость обеспечения живучести как сети в целом, так и отдельных участков и узлов.

Живучесть характеризует устойчивость сети связи против действия причин, лежащих вне сети и приводящих к разрушениям или значительным повреждениям некоторых её частей. Живучесть – свойство сети сохранять способность выполнять требуемые функции в условиях, создаваемых воздействием внешних дестабилизирующих факторов [1].

На сегодняшний день существует множество способов обеспечения живучести сетей (систем) различного назначения. В работе А.Г. Додонова и Д.В. Флейтмана [2] делается попытка формализовать в наиболее общем виде задачу обеспечения живучести информационной системы, сделав ее доступной для построения алгоритмов решения этой проблемы на основе решения задач сбора, обработки, хранения и представления информации специалистам для принятия решений по обеспечению деятельности работы системы. Создание такой системы сводится к построению комплекса технических средств топологии сети и распределения ресурсов по узлам сети.

В работе Додонова А.Г. и Ландэ Д.В. [3] для обеспечения функционирования системы предложено применение стратегии обеспечения живучести. В процессе формирования такой стратегии для каждого состояния необходимо дополнительно выработать решения, относящиеся к функциям системы: суживать или нет множество функций, которые вместе составляют цель функционирования, как это сделать, упрощать или нет алгоритм реализации функций, при которых необходимо противодействовать угрозам нарушения работоспособности.

В работе Стекольникова Ю.И. [4] предложена структурная S-система, которая является

наиболее распространенным типом систем, где присутствует четко выраженная структура, которая дает возможность увязывать показатель живучести со стойкостью каждого из элементов. В основе такого подхода лежит возможность перечислять все состояния способности системы (матрицы состояния способности, число элементов обеспечивающих состояние способности). Таким образом, постановкой задачи обеспечения живучести является обнаружение и локализация неблагоприятной ситуации, требующей оперативного принятия решения, чтобы предупредить распространение последствий нештатной ситуации в сети; обеспечение функционирования сети в критическом режиме; продолжение функционирования без потерь информации путем перераспределения потоков среди уцелевших элементов сети в условиях непредвиденного уменьшения технических ресурсов, вследствие которого полноценное выполнение всех функций сети невозможно.

Важным вопросом для достижения высокой степени живучести системы является выбор показателей и критериев живучести.

Основными показателями живучести являются [4]:

- показатель вероятности сохранения системой состояния восстановления в течение заданного времени;
- показатель неуязвимости;
- условный закон непоражения, характеризующий «динамику» сохранения системой состояния работоспособности при количестве воздействий на систему, равном некоторому *I*;
- условный закон неуязвимости структуры, характеризующий «динамику» сохранения системой состояния работоспособности при последовательном удалении ее элементов;
- число воздействий, при котором система теряет состояние способности;
- среднее число изъятых из структуры элементов, при котором она теряет состояние работоспособности.

Основными критериями живучести являются:

- критерий соответствия сети заданным показателям качества и оценки степени ее функционирования;
- критерий оценки эффективности реконфигурации и оптимального перераспределения ресурсов, а также динамики восстановления функциональных возможностей после сбоев;
- критерий, характеризующий изменение производительности и скорости передачи информации в сети при выполнении различных действий в условиях деградации сетевых ресурсов;
- критерий живучести сети, характеризующий процесс удаления всех ребер, инцидентных некоторой вершине, изолируя ее и прерывая все пути к другим вершинам.

Можно отметить, что рассматриваемые показатели и критерии обеспечения и повышения живучести систем можно отнести и к ТКС, т.к. проблема обеспечения живучести ТКС также связана с достоверностью и точностью передаваемой информации, большим количеством возможных реконфигураций сети, а также способностью продолжения функционирования при получении повреждений.

Обеспечение требуемого уровня живучести является одной из важных и актуальных задач проектирования сети. При решении задач проектирования сетей, авторы [2–4] различают функциональную, структурную и структурно-функциональную живучесть. Каждая из них оценивается по определенному критерию. По критериям пригодности, сравнительной оценки и оптимальности оценивается структурно-функциональная живучесть. Решение задач повышения функциональной живучести – с использованием критерия максимизации потоков или критерия количественной оценки компенсированных функциональных отказов; повышение структурной живучести обеспечивается использованием критерия связности. Так как ТКС относятся к структурным системам, вопросы обеспечения структурной живучести приобретают особое значение. Важным вопросом при этом является выбор критерия живучести. Выбор критерия живучести определяется исключительно типом решаемой задачи.

Наиболее эффективным критерием для достижения высокого уровня живучести является способность перераспределять потоки информации и продолжать выполнять предписанные сети функции после того, как отдельные элементы вышли из строя, нарушая структуру сети.

Оценивая существующие методы обеспечения и повышения живучести, можно сказать, что они базируются на четырех основных принципах [5] – распознавания, противодействия, восстановления, адаптации – и включают методы обеспечения безопасности, надежности и отказоустойчивости [6, 7].

Принцип распознавания заключается в способности системы обнаруживать атаки, успешные вторжения, повышение риска выхода из строя важных компонентов системы, риска потери или искажения информации. Этот принцип основывается на методах:

– диагностики – внесения в систему аппаратно-программных средств, позволяющих отслеживать нежелательные отклонения в работе системы и ее отдельных компонентов;

– оповещения – внесения в систему аппаратно-программных средств, позволяющих уведомлять пользователей и системных администраторов о нежелательных отклонениях в работе системы и ее отдельных компонентов;

– регистрации событий – сбора и хранения информации о действиях различных пользователей и компонентов системы;

– анализа шаблонов поведения пользователей – сравнения последовательности действий пользователей и компонентов системы с извест-

ными шаблонами атак и некорректного использования.

Результаты использования этого принципа служат базой для применения активного противодействия (при обнаружении успешных атак или появлении новых рисков) и адаптации.

Принцип восстановления заключается в способности системы восстанавливать функциональность и работоспособность компонентов после отражения атаки. Этот принцип реализуется методами:

– поддержки баз данных изменений – сбором сведений обо всех изменениях и дополнениях информации, хранимой в системе, в таком объеме, который предполагает возможность отказа от каждого конкретного изменения и определения источника каждого конкретного изменения;

– организацией безопасного хранения информации – использованием при хранении информации надежных и отказоустойчивых технологий, которые обеспечивали бы сохранность и доступность информации с заданными показателями качества;

– поддержки транзакционности процессов – организацией работы процессов изменения информации в системе таким образом, чтобы в любой момент времени можно было гарантировать целостность данных, хранимых в системе.

Основная цель этого принципа заключается в построении формализованной автоматизированной процедуры возвращения системы в штатные условия функционирования.

Принцип адаптации заключается в способности системы «обучаться», т.е. развиваться на основании информации об успешных атаках, возникновении нештатных ситуаций, изменении условий функционирования системы. Целью принципа адаптации является, во-первых, создание надежной защиты от отраженных и неизвестных ранее атак, во-вторых, приспособление к новым изменившимся условиям функционирования системы и обеспечение выполнения всех функций системы в таких условиях функционирования.

Принцип противодействия частично позаимствован из сферы безопасности информационных систем и реализуется ее классическими методами:

– идентификацией – доказательством того, что пользователь системы действительно является тем, за кого себя выдает. Для идентификации могут применяться такие средства как «имя пользователя» и «пароль», карты доступа (smart cards), отпечатки пальцев и т.п.;

– авторизацией – набором прав того или иного пользователя на выполнение затребованных им операций;

– ограничением привилегий пользователей – разделением пользователей системы на группы, каждая из которых определяет свой набор прав доступа, например, право на чтение информации, право на запись информации, право на доступ к определенным частям баз данных и т.п.;

– установкой межсетевых экранов – физическим отделением системы от внешней среды;

– внесением избыточности в систему – установкой резервного аппаратного и программного обеспечения, а также архивов информации.

Кроме того, к этому же принципу можно отнести и такие методы:

– реконфигурация – обеспечение функционирования системы при выходе из строя ее ресурсов за счет изменения путей передачи и обработки информации;

– реорганизация – обеспечение функционирования системы при выходе из строя ее ресурсов за счет переопределения функций вышедших из строя компонентов системы между работоспособными компонентами;

– реконструкция – обеспечение функционирования системы при выходе из строя ее ресурсов за счет компенсации потерянной функциональности частично вышедших из строя функционально работоспособных компонентов;

– диверсификация – непрерывное планомерное изменение конфигурации системы, направленное на усложнение организации атак на систему.

Целью принципа противодействия является поддержание условий функционирования.

Анализируя существующие методы повышения живучести, предназначенные для обеспечения реагирования при воздействии внешней среды на сеть, можно сделать вывод, что наиболее важным и «судьбоносным» для сети является метод реконфигурации при уже нанесенном повреждении с последующим перераспределением потоков, т.к. информация (поток информации) должна быть доставлена адресату.

II ОСНОВНАЯ ЧАСТЬ

Целью данной работы является разработка метода обеспечения живучести ТКС на основе перераспределения ресурсов сети при отказе сетевых элементов в результате неблагоприятного воздействия (НВ) на ТКС.

В исходном состоянии, при отсутствии НВ на ТКС, принимается, что сеть является полностью работоспособной. Её состоянию работоспособности S_0 ставится в соответствие количественная оценка работоспособности $\mathrm{OP}_0 = 1$ (или $\mathrm{OP}_0 = 100\%$), соответствующая суммарной пропускной способности C_0 всех маршрутов μ_{st}^{k}, используемых для облуживания поступающих в ТКС требований φ_{st}:

$$C_0 = \sum_{\overline{s=1}}^{n} \sum_{t=1}^{n} \sum_{k=1}^{K_{st}} c_{st}^{k} . \qquad (1)$$

Здесь $s,t = \overline{1,n};\ \ s \neq t;$ n – количество пунктов сети;

$k-k$-й маршрут, используемый для обслуживания требования φ_{st} ;

K_{st} – количество используемых маршрутов для обслуживания требования φ_{st}.

Отметим, что каждое требование φ_{st} принадлежит соответствующему классу обслуживания, определяющего значимость требования φ_{st}, его приоритет.

В случае возникновения некоторого i-го неблагоприятного воздействия на ТКС – $НВ_i$, в результате которого сеть переходит в состояние S_i, метод позволяет выполнить перераспределение ресурсов сети с учетом класса требований φ_{st} с целью максимизации суммарной пропускной способности сети C_i и определить степень работоспособности сети $ОР_i: 0 \le ОР_i \le 1$, $i=\overline{1,I}$ (или $0 \le ОР_i \le 100\%$).

Здесь i – номер (вид) НВ на ТКС; I – число различных возможных неблагоприятных воздействий на ТКС.

Суть метода состоит в выполнении следующих действий:

1. Задание состояний S_i ТКС ($i=\overline{0,I}$), I – число различных возможных НВ на ТКС. Задание состояний S_i (их нумерация) осуществляется следующим образом.

Пусть в сети имеется m элементов (пунктов и ветвей связи). Обозначим состояние работоспособности j – го элемента z_j. Тогда состояние S_0 полной работоспособности сети может быть представлено в виде логического уравнения работоспособности (2):

$$S_0 = z_1 \wedge z_2 \wedge \ldots \wedge z_j \wedge \ldots \wedge z_m \ . \qquad (2)$$

Состояние S_1 сети, когда элемент 1 вышел из строя, может быть представлено в виде следующего логического уравнения работоспособности (3):

$$S_1 = \overline{z_1} \wedge z_2 \wedge \ldots \wedge z_j \wedge \ldots \wedge z_m . \qquad (3)$$

Состояние S_2 ети, когда элемент 2 вышел из строя, может быть представлено в виде следующего логического уравнения работоспособности (4):

$$S_2 = z_1 \wedge \overline{z_2} \wedge \ldots \wedge z_j \wedge \ldots \wedge z_m . \qquad (4)$$

Состояние $S_{1,2}$, когда элементы 1 и 2 вышли из строя, представляется в виде:

$$S_{1,2} = \overline{z_1} \wedge \overline{z_2} \wedge \ldots \wedge z_j \wedge \ldots \wedge z_m . \qquad (5)$$

Аналогично записям (2) – (5) могут быть получены логические уравнения всех остальных возможных состояний ТКС.

2. Получение количественной оценки $ОР_0$ состояния S_0 полной работоспособности ТКС. Для этого определяется суммарная пропускная способность сети C_0 – сумма пропускных способностей маршрутов, составляющих план распределения потоков требований φ_{st} ($s,t=\overline{1,n}$; n – число пунктов сети), на основе выражения (1). Полученному значению C_0 ставится в соответствие $ОР_0 = 1$ (или $ОР_0 = 100\%$).

3. Задание состояния S_i, в соответствии с i-м видом $НВ_i$.

4. Определение маршрутов μ_{st}^{k} требований φ_{st}, которые в состоянии S_i не могут быть реализованы, т.е. тех, которые включают сетевые элементы z_j, на которые было оказано $НВ_i$. Отметим, что в самом неблагоприятном случае:

$$s,t=\overline{1,n};\ j=\overline{1,m};\ k=\overline{1,K_{st}} .$$

5. Формирование множества требований Φ на обслуживание на основе перераспределения ресурсов сети.

Данное множество включает подмножество $\Phi^{нр}$, которое формируется из тех требований $\varphi_{st}^{нр}$, для реализации которых в исходном плане распределения потоков требований были использованы маршруты μ_{st}^{k}, вышедшие из строя в результате $НВ_i$. Кроме этого, множество Φ дополняется также подмножеством $\Phi^{нпр}$ требований $\varphi_{st}^{нпр}$, классы обслуживания которых менее приоритетны, чем классы обслуживания требований $\varphi_{st}^{нр}$. При этом сетевые ресурсы, которые в исходном плане, т.е. в состоянии S_0, были использованы для обслуживания требований $\varphi_{st}^{нпр}$, считаются свободными. Таким образом, $\Phi = \Phi^{нр} + \Phi^{нпр}$.

Итак, имеется множество требований Φ, состоящее из двух подмножеств требований: $\Phi^{нр}$ и $\Phi^{нпр}$, и множество свободных пропускных способностей ветвей сети представленных в виде матрицы $C=\left\|c_{xy}\right\|$, ($x,y=\overline{1,n}$). Отметим, что в матрице $C=\left\|c_{xy}\right\|$ элемент $c_{xy}=0$ соответствует ветви b_{xy}, которая не может быть использована при распределении потоков требований подмножеств $\Phi^{нр}$ и $\Phi^{нпр}$. Подмножества $\Phi^{нр}$ и $\Phi^{нпр}$ удобно представлять в виде матриц $\Phi^{нр}=\left\|\varphi_{st}^{нр}\right\|$ и $\Phi^{нпр}=\left\|\varphi_{st}^{нпр}\right\|$.

6. Формулирование задачи распределения множеств требований $\Phi^{нр} = \left[\varphi_{st}^{нр}\right]$ и $\Phi^{нпр} = \left[\varphi_{st}^{нпр}\right]$ (задачи перераспределения ресурсов сети) как задачи линейного программирования.

Пусть $M = \{\mu_i\}$ – множество (совокупность) маршрутов, которые могут быть использованы для обслуживания потоков требований между пунктами сети, представленными в матрицах $\Phi^{нр} = \left[\varphi_{st}^{нр}\right]$ и $\Phi^{нпр} = \left[\varphi_{st}^{нпр}\right]$; c_i – емкость маршрута μ_i, f_i – вес (ценность) маршрута μ_i, который определяет относительную целесообразность использования маршрута. Выбор f_i зависит от критерия, по которому осуществляется перераспределение множеств требований. При оптимизации по рангу в качестве весового коэффициента маршрута μ_i целесообразно использовать отношение максимального ранга $r_{\max}$ маршрутов множества M к рангу рассматриваемого i-го маршрута μ_i. Рангом r_i назовем количество ветвей, составляющих маршрут μ_i. Будем обозначать данный коэффициент, учитывающий ранг маршрута μ_i, – f_i^r. Тогда:

$$f_i^r = \frac{r_{\max}}{r_i}. \qquad (6)$$

Кроме того, f_i должен учитывать важность требования $\varphi_{st}^{нр}$ (и/или $\varphi_{st}^{нпр}$), использующего маршрут μ_i, т.е. принадлежность соответствующему классу, а именно – чем выше класс, тем большее значение должно быть присвоено коэффициенту f_i. Поэтому, по аналогии с (6), формируется коэффициент f_i^k, определяемый выражением (7):

$$f_i^k = \frac{k_{\max}}{k_i}, \qquad (7)$$

где $k_{\max}$ – показатель самого низкого класса (приоритета обслуживания требования);

k_i – класс требования, для обслуживания которого используется маршрут μ_i.

Отметим, что значение самого приоритетного класса принимается равным «1». На основе полученных в соответствии с (6) и (7) коэффициентов f_i^r и f_i^k формируется результирующий коэффициент f_i (8):

$$f_i = Kf_i^k * f_i^k. \qquad (8)$$

Здесь K – коэффициент, выбираемый таким образом, чтобы все f_i были целыми числами, что обеспечивает возможность получения целочисленного решения.

Тогда для получения оптимальной организации маршрутов между узлами сети необходимо максимизировать взвешенную целевую функцию – суммарную емкость маршрутов [9]:

$$F = \sum_{\mu_i \in M} f_i c_i \to \max \qquad (9)$$

при следующих ограничениях:

1) емкости маршрутов не могут принимать отрицательных значений, т.е. $c_i \geq 0$ для всех $\mu_i \in M$;

2) суммарная емкость совокупности маршрутов $m_{st}^{нр} = \left\{\mu_i^{нр}(s,t)\right\}$ и $m_{st}^{нпр} = \left\{\mu_i^{нпр}(s,t)\right\}$ между произвольной парой s,t пунктов ТКС должна быть равна (если это возможно) величине поступающих в сеть на обслуживание требований $\varphi_{st}^{нр}$ и $\varphi_{st}^{нпр}$:

$$\sum_{\mu_i^{нр}(s,t) \in m_{st}^{нр}} c_i(s,t) \leq \varphi_{st}^{нр} \qquad (10)$$

где $\mu_i^{нр}(s,t)$ – i-й маршрут множества M, используемый для обслуживания требования $\varphi_{st}^{нр}$;

$m_{st}^{нр}$ – совокупность маршрутов $\mu_i^{нр}(s,t)$, используемых для обслуживания требования $\varphi_{st}^{нр}$.

Аналогично:

$$\sum_{\mu_i^{нпр}(s,t) \in m_{st}^{нпр}} c_i(s,t) \leq \varphi_{st}^{нпр} \qquad (11)$$

где $\mu_i^{нпр}(s,t)$ – i-й маршрут множества M, используемый для обслуживания требования $\varphi_{st}^{нпр}$;

$m_{st}^{нпр}$ – совокупность маршрутов $\mu_i^{нпр}(s,t)$, используемых для обслуживания требования $\varphi_{st}^{нпр}$.

Отметим, что ограничения (10) и (11) формируются для всех требований множеств $\Phi^{нр} = \left[\varphi_{st}^{нр}\right]$ и $\Phi^{нпр} = \left[\varphi_{st}^{нпр}\right]$ ($s,t = \overline{1,n}$);

3) для любой ветви b_{xy} сети суммарная пропускная способность $c_i(s,t)$ всех маршрутов μ_i, проходящих по этой ветви, не может превысить пропускной способности $c(x,y)$ этой ветви:

$$\sum_{\forall \mu_i \ni b_{xy}} c_i(s,t) \leq c(x,y) \qquad (12)$$

($x,y = \overline{1,n}$; $s,t = \overline{1,n}$; n – количество пунктов ТКС).

7. Решение задачи линейного программирования в форме (9) – (12), в результате чего осуществляется оптимальное перераспределение ресурсов сети для обслуживания требований подмножеств $\Phi^{нр}$ и $\Phi^{нпр}$.

8. Определение суммарной пропускной способности сети C_i, соответствующей полученному плану перераспределения потоков требований после НВ$_i$ по аналогии с (1).

9. Получение оценки работоспособности ОР$_i$ ТКС в состоянии S_i (13):

$$\text{ОР}_i = \frac{C_i}{C_0} \qquad (13)$$

или $(\text{ОР}_i = \frac{C_i}{C_0} * 100\%)$,

где C_0 – суммарная пропускная способность ТКС в состоянии S_0, определяемая на основе (1).

10. Определение соответствия состояния работоспособности ОР$_i$ ТКС предельно допустимому значению показателя работоспособности ОР$_{пр}$:

$$\text{ОР}_i \geq \text{ОР}_{пр} \qquad (14)$$

Если условие (14) выполняется, это означает, что ТКС обеспечивает необходимое качество обслуживания поступающих требований.

Иначе – вырабатываются необходимые рекомендации относительно:

– ограничения величины поступающих в ТКС требований на обслуживание;

– введения резервного оборудования;

– изменения требований к качеству обслуживания и т.д.

III ЗАКЛЮЧЕНИЕ

Представленный метод обеспечения живучести телекоммуникационной сети на основе перераспределения ресурсов сети для обслуживания потоков требований при возникновении i-го вида неблагоприятных воздействий позволяет:

– выполнить оценку работоспособности сети на основе предложенного показателя;

– обнаружить «узкие места» сети для возможности их резервирования;

– выработать соответствующие рекомендации для обеспечения работоспособности ТКС.

Предложенный метод может быть использован на этапе проектирования ТКС для оценки работоспособности сети при изменении ее топологии.

ЛИТЕРАТУРА

1. **Нетес В.А.** Надежность сетей связи в период перехода к NGN/ В.А.Нетес// – Вестник связи, №9. – 2007, С. 4-5.

2. **Додонов А.Г.** К вопросу живучести корпоративных информационных систем /А.Г. Додонов, Д.В.Флейтман //, Киев, 2004, 130 с.

3. **Додонов А.Г., Ландэ Д.В.** Живучесть информационных систем. – К.: Наук. думка, 2011. – 246 с.

4. **Стекольников Ю.И.** Живучесть систем/ Ю.И. Стекольников // – СПб. - Политехника, 2002. – 152 с.

5. **Додонов А.Г., Кузнецова М.Г.** Проблемы и тенденции создания живучих вычислительных систем: Метод. Разработки. – К.: Наук.думка, 1981, 178 с.

6. **Linger R.C., Mead N.R., Lipson H.F.** Requirements Definition for Survivable Network Systems [Электронный ресурс]. – Режим доступу: http://www.cert.org/archive/pdf/icre.pdf.

7. **Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead.** Survivability: Protecting Your Critical Systems [Электронный ресурс]. – Режим доступу: http://www.cert.org/archive/html/protect-critical-systems.html

8. **Князєва Н.О.** Теорія проектування комп'ютерних систем і мереж. Ч.2. Методи аналізу і синтезу комп'ютерних систем і мереж, Одеса: СПД, 2012 – 240 с.

N. A. Knyazeva, I.B. Gryshchenko, S.V. Shestopalov

Scientific and training Institute of the cold cryotechnologies and ecoenergetics ONAFT,
1/3 Dvoryanskaya str., Odessa, 65026, Ukraine

METHOD OF TELECOMMUNICATION NETWORK SURVIVABILITY BASED ON THE NETWORK RESOURCES REDISTRIBUTION

The article presents the indicators and parameters characterizing the network survivability.The presented method of ensuring the survivability of the telecommunication network based on the TCS network reallocation of resources to service the flows of requirements in the event of adverse effects allows you to:
- perform network performance evaluation based on the proposed measure;
- to identify "bottlenecks" for the possibility of network backup solution.
The proposed method can be used in the design phase of TCS to evaluate your network when you change the topology.
Keywords: *Telecommunication network – Vitality – Performance-criteria – Redundancy – Host – Bandwidth – Total Capacity*

REFERENCES

1. **Netes V.A.** Nadezhnost setey svyazi v period perekhoda k NGN/ V.A.Netes// – Vestnik svyazi, № 9. – 2007, S. 4-5.
2. **Dodonov A.G.** K voprosu zhivuchesti korporativnykh informatsionnykh sistem /A.G. Dodonov, D.V.Fleytman //, Kiyev, 2004, 130 s.
3. **Dodonov A.G., Lande D.V.** Zhivuchest informatsionnykh sistem. – K.: Nauk. dumka, 2011. – 246 s.
4. **Stekolnikov Yu.I.** Zhivuchest system / Yu.I. Stekolnikov // – SPb. - Politekhnika, 2002. – 152 s.
5. **Dodonov A.G., Kuznetsova M.G.** Problemy i tendentsii sozdaniya zhivuchikh vychislitelnykh sistem: Metod. Razrabotki. – K.: Nauk.dumka, 1981, 178 s.
6. **Linger R.C., Mead N.R., Lipson H.F.** Requirements Definition for Survivable Network Systems [Elektronnyi resurs]. – Rezhim dostupu: http://www.cert.org/archive/pdf/icre.pdf.
7. **Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, Nancy R. Mead**. Survivability: Protecting Your Critical Systems [Elektronnyy resurs]. – Rezhim dostupu: http://www.cert.org/archive/html/protect-critical-systems.html
8. **Knyazєva N.O.** Teoriya proyektuvannya komp'yuternikh sistem i merezh. Ch.2. Metodi analizu i sintezu komp'yuternikh sistem i merezh, Odesa: SPD, 2012 – 240 s.

Отримана в редакції 09.06.2014, прийнята до друку 11.06.2014