УДК 681.324; 519.15

ИССЛЕДОВАНИЕ ИМИТАЦИОННОЙ МОДЕЛИ ЖИВУЧЕСТИ ИНТЕГРАЛЬНОЙ ИНФОРМАЦИОННОЙ СЕТИ

В. П. Блукке, аспирант Института вычислительной математики и математической геофизики (ИВМ и МГ) СО РАН; vvv_bl@ngs.ru
В. К. Попков, профессор ИВМ и МГ СО РАН д. ф.-м. н.; popkov@sscc.ru

Ключевые слова: *гиперсеть, нестационарная гиперсеть, информационные сети, живучесть, разрушающие воздействия, устойчивость.*

Структура сети и классификация основных элементов. В качестве объекта исследования рассматривается интегральная информационная сеть (ИИС), построенная на основе современных информационно-коммуникационных технологий [1,2]. Для моделирования основные элементы сети были условно классифицированы и сведены в схему, приведенную на рис. 1.

Разрушающие воздействия (РВ) и их классификация. Общая классификация основных типов РВ и их поражающих факторов приведена на рис. 2. Все множество потенциальных угроз разделяется на два класса по природе их возникновения: естественные (объективные) и искусственные (субъективные) [3].

Естественные угрозы — это угрозы, вызванные воздействиями на ИИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы — это угрозы, обусловленные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании ИИС и ее элементов, а также ошибками в программном обеспечении, в действиях персонала и т. п.;
- преднамеренные угрозы.

Для примеров в расчетах используется класс преднамеренных РВ искусственного происхождения. Классификация РВ приведена на рис. 2.

Оценка влияния РВ на основные элементы сети. Под *живучестью* понимается устойчивость системы связи к повреждению элементов стихийными факторами и преднамеренными РВ.

Устойчивость — свойство системы связи, заключающееся в ее способности осуществлять своевременную передачу информации в необходимом объеме и с качеством не хуже заданного при определенных условиях функционирования [4].

Наиболее эффективными показателями живучести являются характеристики сетей, связанные с потоками в сетях:

- математическое ожидание максимального *s-t* потока;
- коэффициент обеспеченности пропускной способности — отношение математического ожидания максималь-

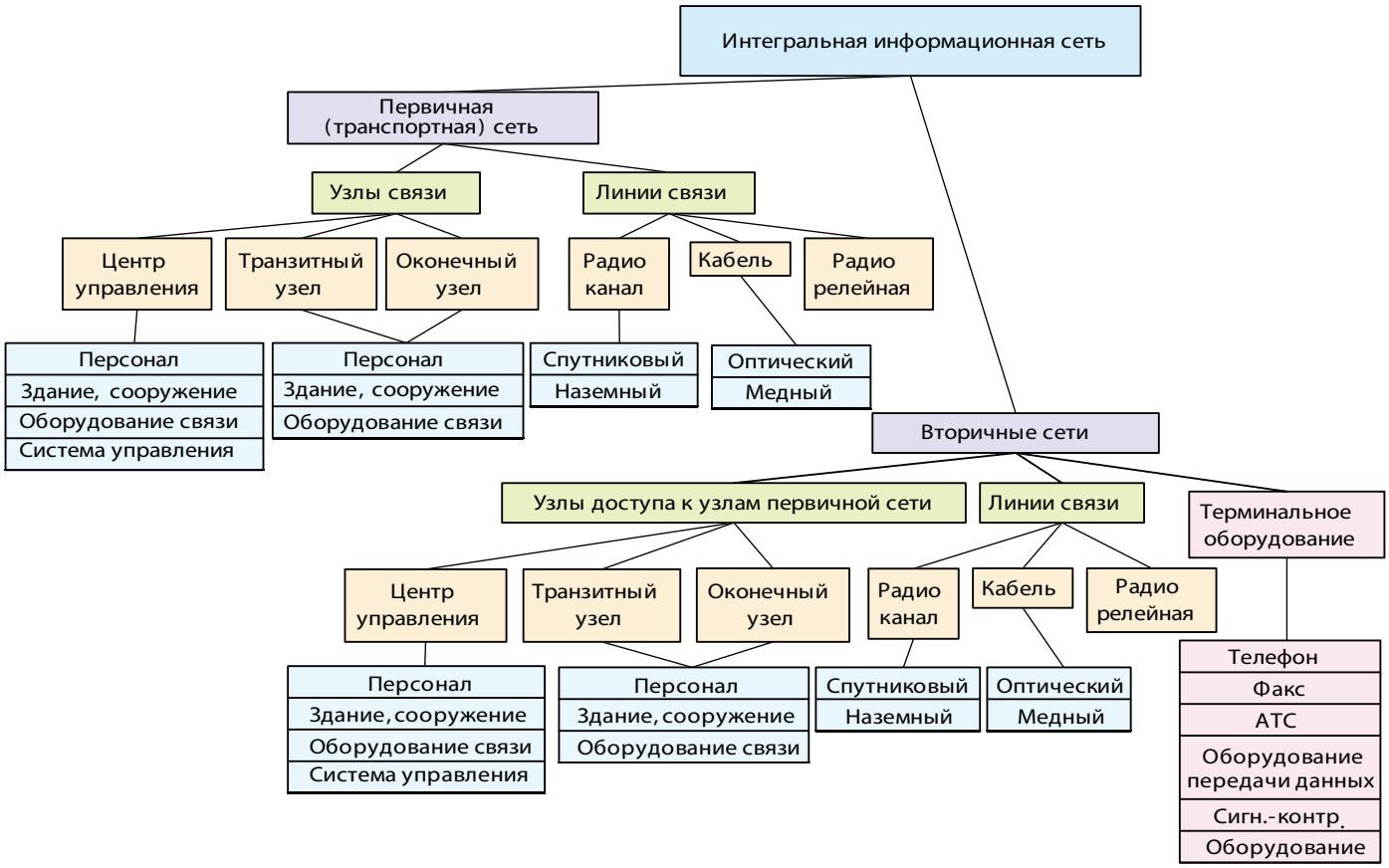

Рис. 1

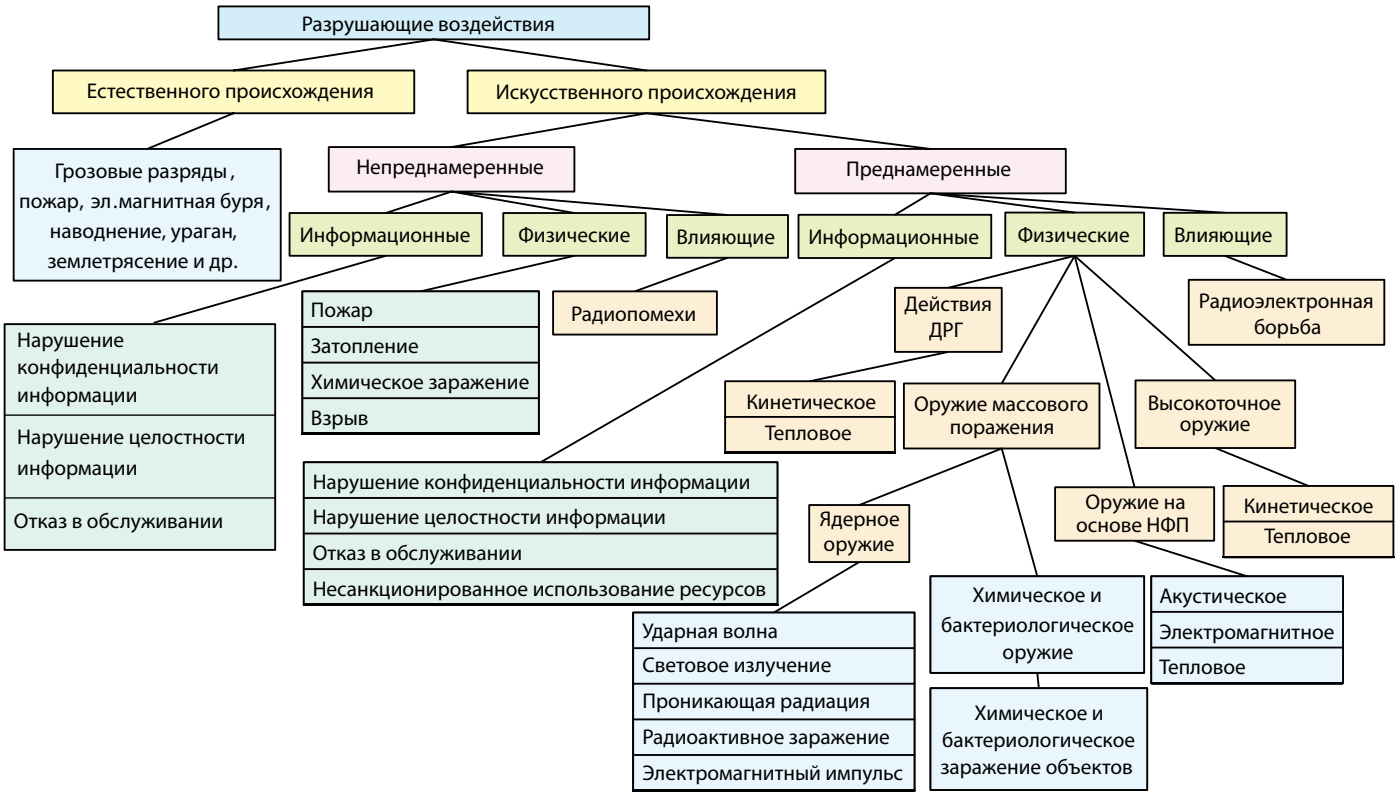

Рис. 2

Таблица 1

Вид РВ	Процесс	Основные элементы сети							
		персонал		здание		оборудование		система управления	
		ΔS, %	T, с	ΔS, %	T, с	ΔS, %	T, с	ΔS, %	T, с
РФВво	разрушение	80—100	$1{,}0 \cdot 10^0$	80—100	$1{,}0 \cdot 10^0$	80—100	$1{,}0 \cdot 10^0$	80—100	$1{,}0 \cdot 10^0$
	восстановление	80—100	$2{,}6 \cdot 10^6$	80—100	$2{,}6 \cdot 10^6$	80—100	$1{,}21 \cdot 10^6$	80—100	$1{,}21 \cdot 10^6$
РФВдг	разрушение	50—80	$1{,}2 \cdot 10^3$	50—80	$7{,}2 \cdot 10^3$	50—80	$3{,}6 \cdot 10^3$	50—80	$1{,}2 \cdot 10^3$
	восстановление	80—100	$8{,}64 \cdot 10^4$	80—100	$2{,}42 \cdot 10^6$	80—100	$8{,}64 \cdot 10^4$	80—100	$5{,}40 \cdot 10^4$
РИВнц	разрушение	—	—	—	—	80—100	$3{,}60 \cdot 10^3$	80—100	
	восстановление	—	—	—	—	80—100	$2{,}16 \cdot 10^4$	80—100	$1{,}80 \cdot 10^4$
РИВоо	разрушение	—	—	—	—	—	—	80—100	$7{,}2 \cdot 10^3$
	восстановление	—	—	—	—	—	—	80—100	$4{,}68 \cdot 10^4$

Здесь ΔS — уменьшение (увеличение) потока, в %, за время $T_{разр}$, ($T_{восст}$).

ного *s-t* потока к максимальному *s-t* потоку в не атакованной сети;

- вероятность того, что текущий максимальный *s-t* поток не меньше заданной величины [5,6].

Расчет максимального потока в сети производится с помощью методов статистического (имитационного) моделирования и программной математической модели структурно-надежных сетей связи на основе графов и гиперсетей. Модель разработана в Лаборатории математического моделирования информационных сетей ИВМ и МГ СО РАН. В программной модели для расчета максимального *s-t* потока между заданной парой узлов сети при заданном РВ разных типов для любого элемента сети используется метод Форда-Фалкерсона.

На основе сокращенной классификации основных элементов ИИС (см. рис. 1) и классификации РВ (рис. 2) для некоторых видов преднамеренных РВ искусственного происхождения и некоторых типов основных элементов ИИС составлена табл. 1, в которой РФВ — разрушающее физическое воздействие с помощью высокоточного оружия, РФВдг — с помощью диверсионной группы, РИВнц — разрушающее информационное воздействие типа «несанкционированное использование ресурсов», РИВоо — типа «отказ в обслуживании». Табл. 1 устанавливает степень потери и восстановления ресурса каждого элемента сети в зависимости от вида РВ и его поражающего фактора, выраженная в процентах с учетом времени разрушения и восстановления элемента.

Таблица 2

№ примера	Тип атаки	Элемент сети	Время, ч				$\Delta P_{отн}$, ,%, от величины		
			ΔT_0	ΔT_1	ΔT_2	ΔT_3	ΔP_1	ΔP_2	ΔP_3
1	РФВво	$X_п$	1	0	3	27	20	20	100
		$X_{ус}$		0	10	20	20	20	100
		$X_{тс}$		0	4	10	20	20	100
		$X_{су}$		0	4	5	10	20	100
2	РФВдг	$X_п$	3	1	3	26	20	50	100
		$X_{ус}$		6	10	20	20	50	100
		$X_{тс}$		3	4	10	20	50	100
		$X_{су}$		4	4	10	10	20	100
3	РИВнц	$X_п$	5	—	—	—	—	—	—
		$X_{ус}$		—	—	—	—	—	—
		$X_{тс}$		3	4	10	20	50	100
		$X_{су}$		2	4	10	10	20	100
4	РИВоо	$X_п$	10	—	—	—	—	—	—
		$X_{ус}$		—	—	—	—	—	—
		$X_{тс}$		—	—	—	—	—	—
		$X_{су}$		2	5	5	10	10	100

Для оценки и сравнительного анализа изменения потока предлагается сравнивать значения относительного потока $P_{отн}$, а также среднюю скорость снижения потока $\upsilon_{\downarrow p}$ и среднюю скорость возрастания потока $\upsilon_{\uparrow p}$ при воздействии различных типов РВ.

Относительный поток $P_{отн}$ показывает отношение номинальной пропускной способности к снижению пропускной способности сети при заданном сценарии разрушения и восстановления.

Относительный поток $P_{отн}$ определяется из выраженй:

$$P_{отн} = \frac{P_n + P_{n+1}}{nP_0}; \quad P_{отн} = \frac{\sum P_n}{nP_0},$$

где P_0 — поток без влияния РВ; P_n — поток при начальном РВ; P_{n+1} — поток после начала РВ.

Средняя скорость снижения $\upsilon_{\downarrow p}$ и скорость возрастания потока $\upsilon_{\uparrow p}$ определяется как:

$$\upsilon_{\downarrow P} = \frac{P_0 - P_{n+1}}{\Delta T_2}; \quad \upsilon_{\uparrow P} = \frac{P_0 - P_{n+1}}{\Delta T_4},$$

где ΔT_1 — время доставки (внедрения) РВ; ΔT_2 — время действия РВ; ΔT_3 — время до начала восстановления элемента сети; ΔT_4 — время восстановления элемента сети.

На основании сравнения величин $P_{отн}$ и $\upsilon_{\downarrow p}$, $\upsilon_{\uparrow p}$ можно сделать выводы о необходимых мерах по повышению живучести для конкретной сетевой структуры.

Таблица 3

№ расчета	Тип РВ	$P_{отн}$	$P_{отн}$, %, от P_0	$\Delta P_{отн}$, %, от P_0	$\upsilon_{\downarrow p}$	$\upsilon_{\uparrow p}$
1	РФВво	0,737	73,7	-26,3	43,7	5,5
2	РФВдг	0,746	74,6	-25,4	11,25	3,21
3	РИВнц	0,861	86,1	-13,9	22,5	3,21
4	РИВоо	0,872	87,2	-12,8	22,5	9,0

Результаты, полученные при проведении имитационного моделирования. *Пример 1. Разные типы атак при неизменяемой конфигурации сети.* Взят граф сети связи, состоящий из пяти узлов и восьми ветвей, вес ребер графа приводится на рис. 3. Пример включает четыре расчета. На узле 5 проводятся преднамеренные РВ искусственного происхождения четырех типов: РФВво, ОФВдг, РИВнц, РИВоо

Каждому типу РВ соответствуют индивидуальные временные параметры ΔT_1—ΔT_4, имеющие свои значения для основных элементов узла (табл. 2): $X_п$ — обслуживающий персонал; $X_{ус}$ — узел связи (здание, сооружение); $X_{тс}$ — техника связи; $X_{су}$ — система управления.

Максимальный *s-t* поток в примере рассчитывается между узлами 1 и 3. Расчетные значения $P_{отн}$ и $\upsilon_{\downarrow p}$, $\upsilon_{\uparrow p}$ приведены в табл. 3.

Сравнение значений $P_{отн}$, $\upsilon_{\downarrow p}$, $\upsilon_{\uparrow p}$ показывает, что устойчивость сети данной конфигурации к атакам типа РИВнц и РИВоо наибольшая, а к атакам РФВво и РФВдг, произведенным на один и тот же узел сети, — наименьшая. Следовательно, для данной сетевой структуры необходи-

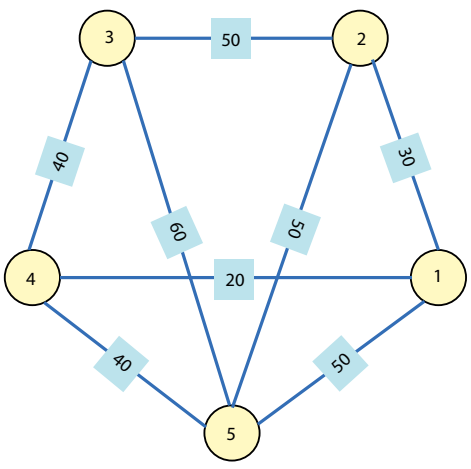

Рис. 3

Таблица 4

№ примера	Узел №	Элемент сети	Время, ч				$\Delta T_{отн}$, %, от величины		
			ΔT_0	ΔT_1	ΔT_2	ΔT_3	ΔT_1	ΔT_2	ΔT_3
1	5	$X_п$	3	1	3	26	20	50	100
		$X_{ус}$		6	10	20	20	50	100
		$X_{тс}$		3	4	10	20	50	100
		$X_{су}$		4	4	10	10	20	100
2	2	$X_п$	3	1	3	26	20	50	100
		$X_{ус}$		6	10	20	20	50	100
		$X_{тс}$		3	4	10	20	50	100
		$X_{су}$		4	4	10	10	20	100
3	4	$X_п$	3	1	3	26	20	50	100
		$X_{ус}$		6	10	20	20	50	100
		$X_{тс}$		3	4	10	20	50	100
		$X_{су}$		4	4	10	10	20	100

Таблица 5

№ расчета	Тип РВ	$P_{отн}$	$P_{отн}$, %, от P_0	$\Delta P_{отн}$, %, от P_0	$\upsilon_{\downarrow p}$	$\upsilon_{\uparrow p}$
1	5	0,746	74,6	-25,4	11,25	3,21
2	2	0,847	84,7	-15,3	6,75	1,93
3	4	0,898	89,8	-10,2	4,5	1,28

мо большее внимание уделить усилению защиты от атак РФВво и РФВдг.

Пример 2. Атаки одного типа на разные узлы сети. Взят граф сети связи аналогичный примеру 1. Пример включает три расчета. На узлы 5, 2 и 4 оказывается преднамеренное РВ искусственного происхождения типа РФВдг.

Временные параметры ΔT_1—ΔT_4 одинаковые, а следовательно, и устойчивость подэлементов, составляющих узел, одинакова (табл. 4).

Максимальный *s-t* поток в примере рассчитывают между узлами 1 и 3. Расчетные значения $P_{отн}$ и $\upsilon_{\downarrow p}$, $\upsilon_{\uparrow p}$ приведены в табл. 5.

Сравнение значений $P_{отн}$, $\upsilon_{\downarrow p}$, $\upsilon_{\uparrow p}$ показывает, что устойчивость сети такой конфигурации при проведении атаки типа РФВдг на узел 5 наименьшая, а на узел 4 — наибольшая. Следовательно, узел 5 нуждается в наибольшей защите от атак данного типа.

Пример 3. Атаки одного типа на один узел. Устойчивость подэлементов различная. Взят граф сети связи, аналогичный примеру 1. Пример включает три расчета. На узел 5 оказывается преднамеренное РВ искусственного происхождения типа РФВдг. Временные параметры ΔT_1—ΔT_4 различны, а следовательно, и устойчивость подэлементов, составляющих узел, разная (табл. 6).

Максимальный *s-t* поток в примере рассчитывается между узлами 1 и 3. Расчетные значения $P_{отн}$ и $\upsilon_{\downarrow p}$, $\upsilon_{\uparrow p}$ приведены в табл. 7.

Сравнение значений $P_{отн}$, $\upsilon_{\downarrow p}$, $\upsilon_{\uparrow p}$ показывает, что устойчивость сети при увеличении устойчивости отдельных элементов узла при проведении атаки типа РФВдг повышается на 1,5 % во втором опыте и на 3,1 % — в третьем. Таким образом, в данном случае можно сделать вывод о не суще-

Таблица 6

№ примера	Элемент сети	Время, ч				$\Delta P_{отн}$, %, от величины		
		ΔT_0	ΔT_1	ΔT_2	ΔT_3	ΔP_1	ΔP_2	ΔP_3
1	$X_п$	3	1	5	19	20	50	100
	$X_{ус}$		6	5	12	20	50	100
	$X_{тс}$		3	4	10	20	50	100
	$X_{су}$		4	6	10	10	20	100
2	$X_п$	3	3	3	19	20	50	100
	$X_{ус}$		8	3	12	20	50	100
	$X_{тс}$		5	2	10	20	50	100
	$X_{су}$		6	4	10	10	20	100
3	$X_п$	3	5	1	19	20	50	100
	$X_{ус}$		10	1	12	20	50	100
	$X_{тс}$		7	0	10	20	50	100
	$X_{су}$		8	2	10	10	20	100

Таблица 7

№ расчета	Тип РВ	$P_{отн}$	$P_{отн}$, %, от P_0	$\Delta P_{отн}$, %, от P_0	$\upsilon_{\downarrow p}$
Норм. работа	1,000	100,0	0,0	0,0	0,0
1	0,793	79,3	-20,7	13,3	2,86
2	0,808	80,8	-19,2	7,5	3,21
3	0,824	82,4	-17,6	5,63	3,75

ственном повышении устойчивости, а следовательно, и живучести в этом случае.

Заключение. Разные РВ имеют различные свойства, влияющие на характер и степень разрушения элементов сетей. Все элементы могут иметь два или более состояния — полной работоспособности или неработоспособности, а также промежуточные состояния — частичной работоспособности в зависимости от степени повреждения, степени защищенности и сложности самого элемента. Степень повреждения должна определятся из типа РВ и свойств элемента, позволяющих это воздействие выдержать. Из этих факторов можно определить степень работоспособности элемента и его пригодность для исполнения основных функций.

При оценке сети с точки зрения ее живучести необходимо учитывать все основные параметры сетей, их свойства и отношения, оказывающие значительное влияние на синтез оптимальной структуры сети связи. Для наиболее эффективной оценки необходимо учитывать взаимодействие первичной и вторичной сети, т. е. в качестве математической модели рассматривать нестационарные гиперсети [6].

ЛИТЕРАТУРА

1. **Давыдов Г. Б., Рогинский В. Н., Толчан А. Я.** Сети электросвязи. — М.: Связь.. 1977. — 360 с.
2. **Шмалько А. В.** Цифровые сети связи: основы планирования и построения. — М.: Эко-Трендз, 2001.
3. **Дудник Б. Я., Овчаренко В. Ф., Орлов В. К.** и др. Надежность и живучесть системы связи. — М.: Радио и связь, 1984.
4. **Попков В. К.** Математические модели живучести сетей связи. — Новосибирск: ВЦ СО РАН, 1990.
5. **Блукке В. П., Попков В. К.** Классификация информационных атак в распределенных вычислительных системах/Тр. ИВМ и МГ СО РАН. Сер. Информатика. — Новосибирск, 2002. — Вып. 4. С. 11—24.
6. **Блукке В. П., Ершов К. А., Попков В. К.** Об одной концептуальной модели живучести глобальных информационных сетей/Материалы IX-й междунар. конф. «Проблемы функционирования информационных сетей». — Новосибирск, 31 июля-3 августа 2006. — С. 43—47.

Получено 27.10.10

ИНФОРМАЦИЯ

РСС: СОТРУДНИЧЕСТВО В СФЕРЕ ИКТ

28 сентября 2010 г. в Кишиневе (Республика Молдова) состоялось **16-е заседание Координационного совета государств — участников СНГ по информатизации при Региональном содружестве в области связи**. В заседании приняли участие делегации национальных органов по информатизации Республики Армения, Республики Казахстан, Кыргызской Республики, Республики Молдова, Российской Федерации, Республики Таджикистан, Республики Узбекистан, Украины, а также присутствовали представители Азербайджанской Республики, Республики Болгария, Исполкома СНГ и Исполкома РСС. Вел заседание председатель Координационного совета, министр связи и массовых коммуникаций Российской Федерации **И. О. Щёголев**.

На заседании Координационного совета была заслушана информация о выполнении Стратегии сотрудничества государств — участников СНГ в сфере информатизации (Стратегия) и Плана действий по ее реализации до 2010 г. (План действий). Учитывая новые приоритеты построения информационного общества, изменения в уровне развития ИКТ, было принято решение организовать НИР о внесении изменений и дополнений в Стратегию и План действий на период до 2015 г. Данные документы и рассматривались на заседании Координационного совета. Его участники высказали ряд замечаний и предложений, потребовавших уточнения следующих вопросов:

- хода выполнения Плана действий на период до 2010 г. и национальных программ информатизации, проектов построения информационного общества и развития ИКТ в государствах–участниках СНГ;
- предложений по реализации приоритетных направлений дальнейшего сотрудничества в области ИКТ и построения информационного общества для формирования проекта Плана действий на период до 2015 г.

Совет поручил рабочим органам РСС рассмотреть на своих заседаниях проект изменений и дополнений в Стратегию и проект Плана действий на период до 2015 г. и представить свои предложения и замечания на очередном заседании.

Координационный совет обсудил работу, проводимую в государствах Содружества по реализации и внедрению национальных программ, проектов и новых технологий для развития ИКТ, направленных на построение информационного общества.

Важное место в этой деятельности занимают мероприятия по обеспечению информационной безопасности инфраструктуры электронного правительства. Комиссии по информационной безопасности было поручено использовать опыт Республики Беларусь, Республики Казахстан и Российской Федерации по взаимодействию в вопросах применения информационных технологий при обмене электронными документами во внешней и взаимной торговле. Анализ этой деятельности необходим для разработки Конвенции о порядке признания юридической значимости электронных документов в международном информационном обмене между государствами-участниками СНГ. Не менее важно и обоснование необходимости решения уполномоченными органами и организациями стран СНГ проблем, которые возникают при осуществлении трансграничного информационного обмена и связаны с контролем над регулированием импорта/экспорта ИКТ-продуктов, содержащих криптографические функции.

Решению данного вопроса могла бы способствовать НИОКР «О создании пилотного проекта системы защищенного трансграничного юридически значимого информационного обмена в рамках СНГ», возможность проведения которой в 2011—2013 гг. было поручено рассмотреть Комиссии РСС по экономике связи.

Осознавая необходимость Единого центра по обеспечению безопасности в киберпространстве государств-участников СНГ, Координационный совет поручил Комиссии по информационной безопасности на свое очередное заседание представить перечень мероприятий по его созданию. Предполагается, что разрабатываемые Комиссией по информационной безопасности документы будут включены в раздел «Информационная безопасность» проекта изменений и дополнений в Стратегию сотрудничества государств-участников СНГ в сфере информатизации и проекта Плана действий на период до 2015 г.

Положительную оценку Координационного совета получил опыт Российской Федерации по подготовке и реализации проекта создания кириллического домена .РФ. Результаты внедрения кириллического домена .РФ поручено проанализировать Комиссии РСС по информатизации.

Сотрудничество в сфере ИКТ и выработка совместных действий по построению информационного общества являются необходимым условием успешного развития всех стран Содружества.