



Всероссийская конференция
«Использование возможностей Интернета
в кризисных ситуациях: организационные
и технологические решения»
(«ИНФОФОРУМ-Антикризис»)



«ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТ-РЕШЕНИЙ В КРИЗИСНЫХ СИТУАЦИЯХ: ЗАРУБЕЖНЫЙ ОПЫТ»

Анатолий Иванович СМИРНОВ

д-р ист.наук, профессор,
Руководитель Кризисного центра МИД России,
Чрезвычайный и Полномочный Посланник

тел.(7-495)-244-20-64 aismirnov@mids.ru

Критерии международного права по кризису: диспут (через инцидент) трансформируется в кризис. Военный конфликт - острая фаза кризиса. Есть до 60 критериев кризиса.

Мировой финансовый кризис побудил вернуться к рассекреченным прогнозам ЦРУ «**Контур** мирового будущего: доклад по проекту – 2020» - 4 версии:

1. **«Давосский мир»:** во главе экономик мира встают Китай и Индия и это придает менее западный облик глобализации.

2. **Rex Americana:** США □ сохраняют свою доминирующую роль и формируют новый миропорядок.

3. **New Caliphate** ислам бросает вызов западным нормам и становится фундаментом новой системы.

4. **«Кольцо страха»** □ - угроза распространения ОМП приводит к превентивным интервенциям, что способно вернуть цивилизацию к оруэлловскому миру.²

Оппоненты ЦРУ в книге "**Россия-2020: будущее страны в условиях глобальных перемен**", исследуют три сценария:

1. «Конец истории» - глобализация справилась с вызовами. Россия интегрирована в неё как периферия, а её элита – в мировую элиту на вторых ролях. Сетевые структуры подчинены глобальной информационной олигархии, контролирующей мировое правительство.

2. «Великие потрясения» - глобализация рухнула, новая Великой депрессии, в мире - волна революций и этноконфликтов. Российская элита смещена, что даёт для новой элиты вариант **«догоняющего развития»**.

3. «Третья волна во втором эшелоне» - в России создается социально-креативный уклад, полномочное самоуправление, поддержка гражданского общества и корневых информструктур Интернета. Используется **«неосоветское возрождение снизу»**, а также опыт стран **«первого эшелона»** в преодолении **«третьей волны»**.

Итак, и версии ЦРУ, и наши сценарии при всем их отличии, совпадают в одном – важности ИНТЕРНЕТА.

По данным ЦРУ, число стран, разрабатывающих информационное оружие (через Интернет) превышает 120 (при 30, разрабатывающих ОМУ) и они получают возможность вести информационные войны.

Основными задачами в них будут:

- дезорганизация функционирования критически важных военных, промышленных, административных объектов и систем противника;
- информационно-психологическое воздействие на военно-политическое руководство, войска и население;
- в США создана система ведения информационных войн (Information operations) технической и психологической направленности.



Ряд экспертов предрекает усиление противодействия западной экспансии евроазиатского идеологического контрнаступления. В этом плане показательна точка зрения ректора Лондонской Дипакадемии.

Bits & Bytes, Not Bullets

Bits & bytes, not bullets, are the weapons of the new millennium.

Or, most dramatically, a combination of bits & bytes, bullets, bombs and biotechnology.



По мнению ректора:

Who Controls the Cyberstate?

**According to all appearances
there seems to be one answer...**



**Microsoft, Intel & other US
companies!!!**

Vulnerable Systems

Information Systems

Transportation

Emergency Services

Government Services

Banking and Finance

Water Supply Systems

Electrical Power Systems

Gas & Oil Production, Storage, and Transportation

Отставание международного права от ИКТ

Угрозы МИБ приобретают особую остроту в связи со значительным отставанием международного права от стремительно развивающихся ИКТ (исчезают понятия «граница», «территория»).

В этом случае выявление «виновного» может замениться на его «назначение», как это уже было в новейшей истории (Так, США неоднократно «назначали» Китай).

Россия традиционно придерживается принципа сложения, а не конкуренции усилий для формирования архитектуры международной безопасности. При этом его вектор распадается на следующие составляющие:

- противодействие кибертерроризму и киберпреступности, в т.ч. борьба с преступным и террористическим использованием Интернета;
- защита критической информационной инфраструктуры общества и государства;
- защита информационно-психологической сферы общества от негативного контента;
- обеспечение безопасности трансграничного обмена информацией с ограниченным доступом;
- демонополизация управления Интернетом.

За российский документ в декабре 2006 г. в ООН высказались 176 государств. Против были только США. В число соавторов проекта вошли наши партнеры по СНГ, по ОДКБ и ШОС, ряд других государств.

Важную роль в этом сыграли: глобальная контртеррористическая стратегия ООН (сентябрь 2006 г.), Конвенция Совета Европы о предупреждении терроризма (2005 г. вступает в силу с 1 июня 2007 г.) и другие, в которых особое внимание уделяется борьбе с кибертерроризмом.

Резолюция 61/54 подтверждает решение ГА ООН о создании в 2009 году Группы правительственных экспертов по МИБ. Позвольте выразить надежду, что коллеги по СНГ в различных форматах продолжат взаимодействие в столь чувствительной сфере во благо обеспечения мира.

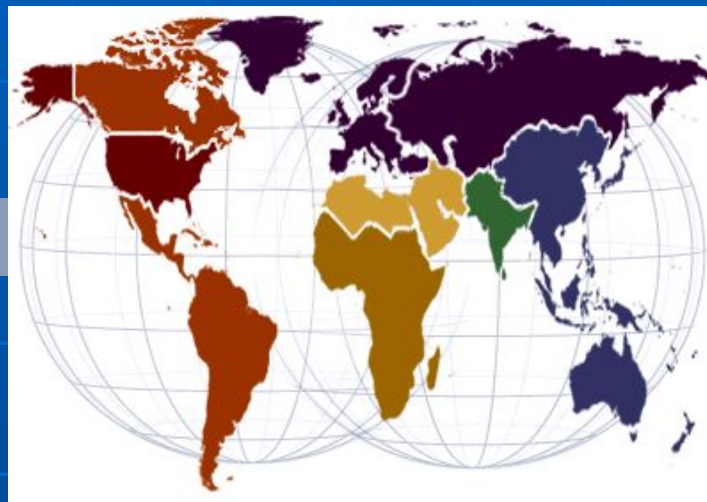
Киберпреступность представляет собой самую серьезную общественную опасность и может угрожать безопасности государств и мирового сообщества в целом. Каждый год фиксируются сотни тысяч попыток несанкционированного вмешательства в государственные, военные, банковские, корпоративные компьютерные системы, компьютеры отдельных пользователей.

Хакинг, крэкинг, фрикинг, фишинг и иные преступления через Интернет становятся все более изощренными по техническим, экономическим, а также и политическим последствиям (участившиеся проникновения в сети госучреждений, в т.ч. оборонных).

Глобальная информационная система Госдепа США и 260 заграничных учреждений (из доклада Конгрессу США)

(1 –я очередь - \$ 2 млрд.)

OPENNET PLUS: BALANCING INFORMATION SHARING REQUIREMENTS AND SECURITY NEEDS



Information Sharing

- § Ready Access To Global Information*
- § Collaboration With Other Agencies And Countries*
- § World-Wide Information Dissemination*

Security Issues

- § Cyber-Attacks*
- § Email-Borne Virus*
- § Internet Technology Presents New Risks*
- § Protection Of Sensitive Information Enhanced*

Objectives

- § Minimize Costs and Complexity– Maximize Information Access*

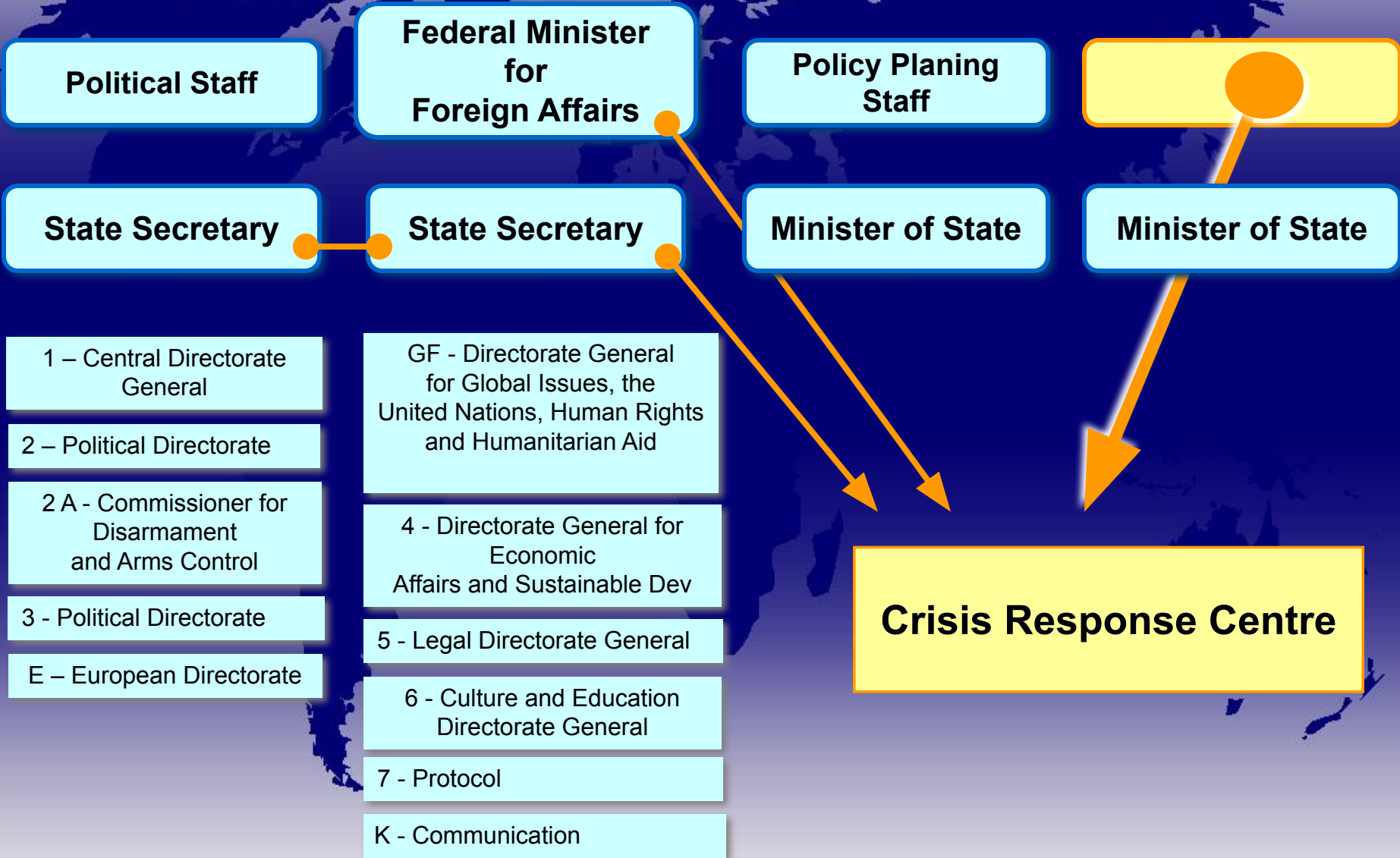


The Crisis Response Center





The Crisis Response Centre within the Foreign Office





ЗАДАЧИ

Центра кризисного реагирования

- ✓ **Круглосуточный мониторинг сообщений посольств и СМИ (Ситуационный центр)**
- ✓ **Обеспечение докладов по предкризисным ситуациям и вариантам реагирования на них**
- ✓ **Координация всех предостережений**
- ✓ **Обеспечение информацией туроператоров и агентств**
- ✓ **Раннее предупреждение о чрезвычайной ситуации и инициативы по превентивным мерам**
- ✓ **Связь с другими госструктурами и частным сектором**
- ✓ **Созыв целевых кризисных групп**
- ✓ **Оказание помощи пострадавшим (спецсвязь с посольствами, кон консультирование турагентств, визовая поддержка, связь по телефону или электронной почте)**
- ✓ **Обеспечение картографическими и фотоматериалами со спутников**



Структура и численность Центра кризисного реагирования (всего 31 чел.)

Дежурные Ситцентра
(8 чел.)

Кризисное
реагирование (10 чел.)

Оказание помощи
гражданам (5 чел.)

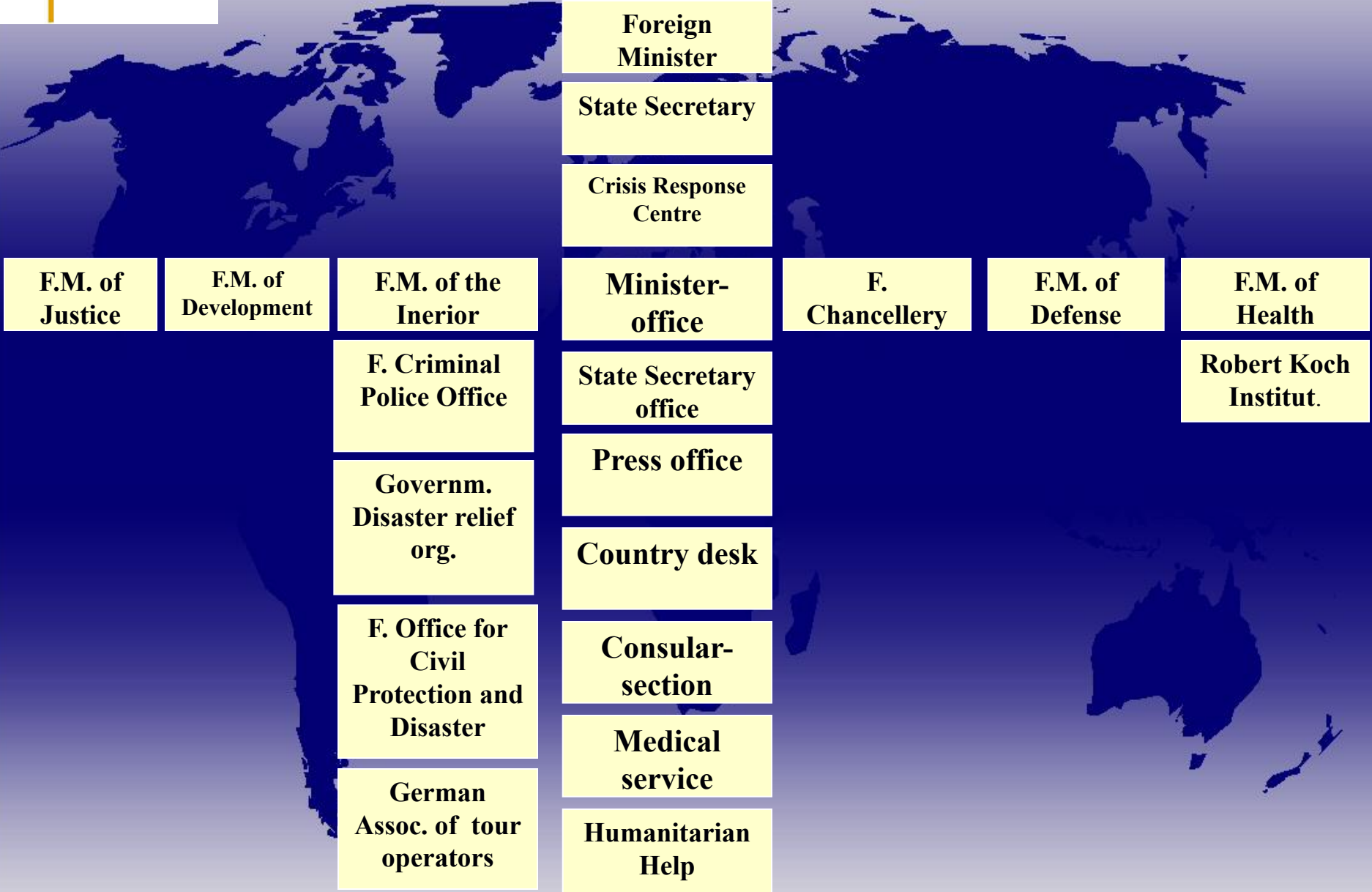
Офицеры связи
из разведки (2 чел.)

Офицер
Минобороны (1 чел.)

Офицеры федеральной
криминальной полиции (2 чел.)

Карты, ГИС (3 чел.)

Structure of Crisis Task Force Tsunami





Structure of Crisis Task Force

other national agencies:

Federal Ministry of the Interior
Federal Criminal Police Office
Federal Police

Federal Chancellery
Federal Intelligence Service

Federal Ministry
of Defence

Federal Ministry for
Economic Cooperation
and Development

Further
institutions

→ Non-governmental organizations

international players:

→ Situation and Crisis Centres of partner states

→ Situation Centre of the EU



Training

- Prerequisite for staff: consular experience, experience in crisis situation at previous post, hardship post
- 4 weeks training on the job for duty officers
- training courses for various staff members (e.g. crisis response officers)
- training courses for various groups of volunteers (220 FO staff volunteered for crisis response teams, 200 for hotline purposes)
- crisis management training is offered at various career levels by Crisis Response Centre
- training is also part of Diplomatic School syllabus

С учетом регламента я завершаю выступление
и хотел бы дать ссылку на электронную версию своей книги:

www.polpred.com



Александр Иванович Смирнов — доктор исторических наук, руководитель Учебно-консультационного Центра по информатике, главный советник МИД России, Чрезвычайный и Полномочный Посол в Российской Федерации 2-го. Владеет немецким, английским, норвежским и финским языками.

Выпускник Ленинградского института иностранных языков дорожного транспорта и Ленинградской высшей партийной школы. Работал в телекоммуникационной сфере, в международных отделах Ленинградской области и ЦК КПСС. После окончания Дипломатической академии занимал руководящие должности в центральном аппарате МИД России и за рубежом, в том числе был Генеральным консулом России в Северной Норвегии (1992–1997). Прошел обучение информатике в Центре передовых технологий в Корнелле, в Российской академии госслужбы при Президенте России. Удостоен сертификата эксперта по «Электронному правительству» (E-Gov) Мэрии Нью-Йорка.

А.И. Смирнов — автор свыше 90 монографий и статей по международному сотрудничеству, языкам и на иностранных языках, а также по информационной глобализации. Регулярно представлял Россию на крупных международных конференциях и в экспертных советах, в т. ч. в СНГ, активно участвует по данным проблемам в отечественных научных форумах, в т. ч. под эгидой Совета Безопасности Российской Федерации. Является со-редактором русского издания «Новый курс» ИВЕСКО и научным консультантом русского издания ИВЕСКО «История человечества». Член команды Российской академии естественных наук, член Академии проблем Безопасности, обороны и правопорядка, профессор Дипломатической академии МИД России и Петербургского государственного университета им. Ш. Шумейкина. Читал лекции во многих зарубежных университетах.

ИНФОРМАЦИОННАЯ ГЛОБАЛИЗАЦИЯ И РОССИЯ:
ВЫЗОВЫ И ВОЗМОЖНОСТИ

А.И.СМИРНОВ

А.И.СМИРНОВ

ИНФОРМАЦИОННАЯ ГЛОБАЛИЗАЦИЯ И РОССИЯ:
ВЫЗОВЫ И ВОЗМОЖНОСТИ



СПАСИБО ЗА ВНИМАНИЕ!