НИИГлоБ

Национальный институт исследований глобальной безопасности

VII CISO FORUM 2014

14 апреля 2014 года

ГЕОПОЛИТИЧЕСКИЕ СТРАТАГЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анатолий Иванович СМИРНОВ

Президент НИИГлоБ, Член Экспертного совета Комитета Госдумы РФ по безопасности и противодействию коррупции, советник РКСС, Чрезвычайный и Полномочный Посланник РФ в отставке, д-р ист.наук, профессор, член президиума РАЕН

aismirnov@niiglob.ru

В день дипломатического работника 2010 г
с Министром С.В.Лавровым

ИЗБРАННОЕ ИЗРЕЧЕНИЕ ПО ТЕМЕ

«Смена исторических эпох определяется сменой коммуникационных технологий»

Герберт Маршалл Маклюэн

(канадский социолог)

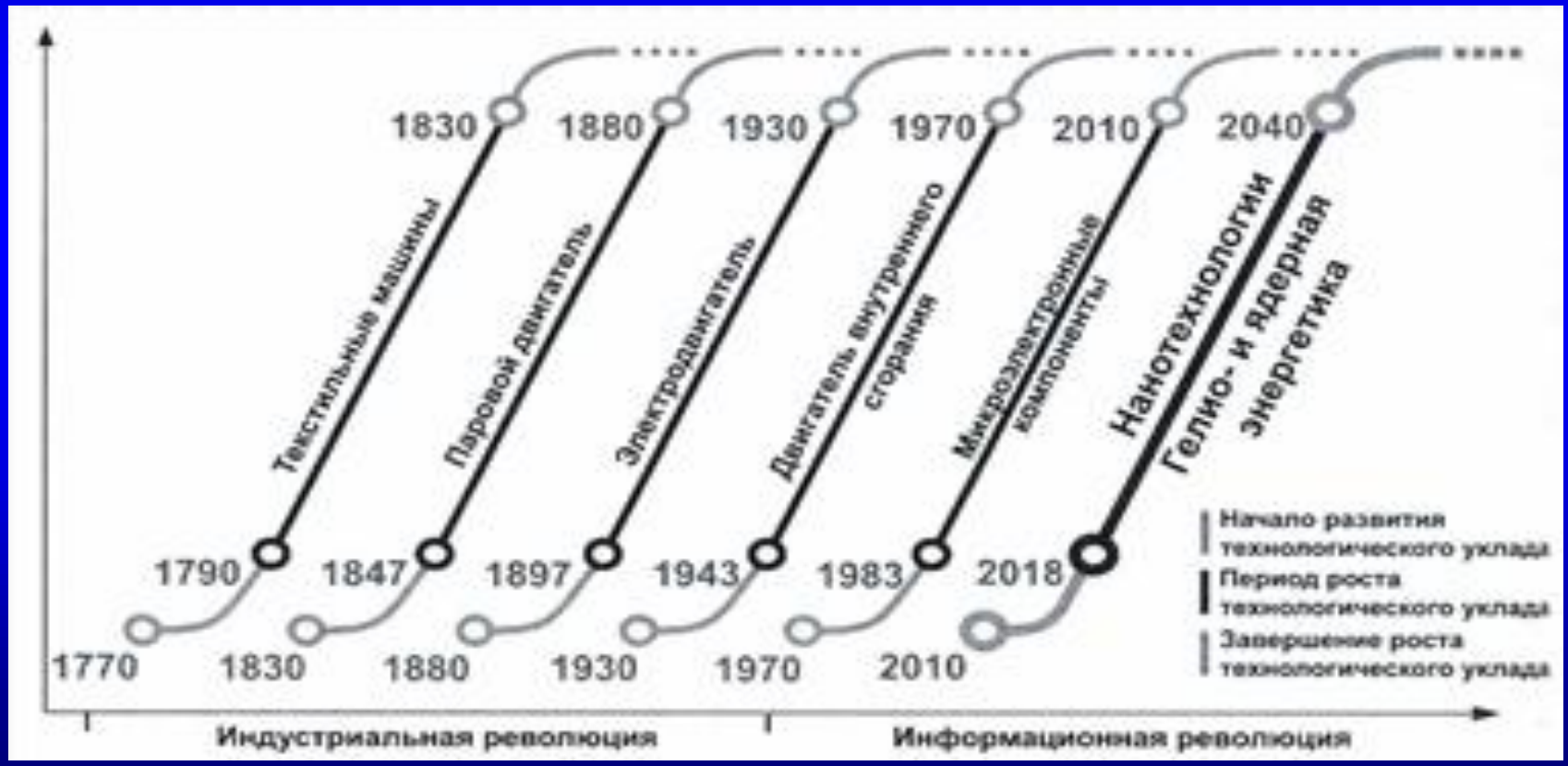
Послание Президента России Федеральному Собранию 12 декабря 2013 г.

«Накал военно-политической, экономической, информационной конкуренции в мире не снижается, а только усиливается. И другие центры влияния внимательно следят за усилением России»

- Начало XXI в. может войти в скрижали человечества как один из самых драматичных (я оптимист – не последних!!!) периодов
- Планета вошла в зону геополитической турбулентности: сполохи войны цивилизаций, международного терроризма, угроза рецессии, рецидивы холодной войны и пиратства, всплеск локальных и региональных конфликтов, техногенные, природогенные, социогенные катастрофы, эпидемии и пандемии, голод. Кризис на Украине – это точка бифуркации в переформатировании всей международно-правовой системы.
- Феномен информационная революция, наряду с несомненным позитивом, на первый план выдвинула и инфогенные угрозы, **т.к.** изменил геополитический код цивилизации и ускорил её переход к шестому технологическому укладу.
- Ведущие страны мира уже реализуют концептуальные и доктринальные стратагемы внедрения НБИК-технологий в геополитической конкуренции. Ибо конвергенция НАНО-БИО-ИКТ и КОГНО наук и технологий способна с превратить страну-лидера во «властелина мира».

Мегатренды: ИКТ – локомотив пятого технологического уклада и основа шестого

«технологический уклад» - комплекс технологий и инноваций, лежащих в основе количественного и качественного скачка в развитии производительных сил общества (акад. С.Глазьев)

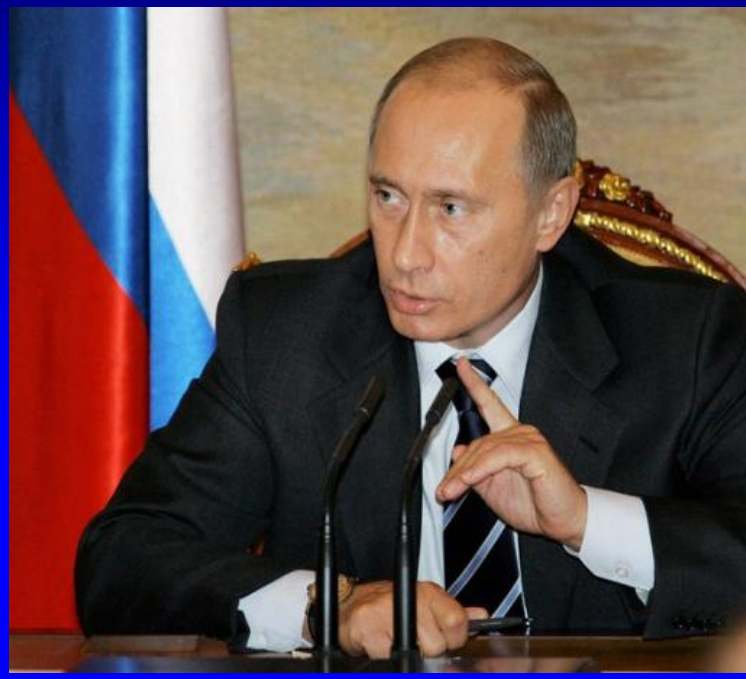


4 -я международная встреча высоких представителей, курирующих вопросы безопасности 2 - 4 июля 2013 года г. Владивосток

- Делегации 60 стран (советы безопасности, аппараты президентов и глав правительств, министерств и ведомств, участвующих в выработке политики в области безопасности своих стран, а также руководство ООН).
- По инициативе КНР продолжено обсуждение вопросов обеспечения МИБ. Участники отметили, что совместная работа постепенно закладывает основы сотрудничества, однако для практического взаимодействия предстоит выработка единых критериев под эгидой ООН.
- По докладу делегации РФ о конвергенции наук и технологий (в т.ч. НБИК-технологии) подчеркнута необходимость формирования нового международного механизма безопасного развития и использования конвергентных технологий как альтернативного ответа на новые вызовы и угрозы глобального характера.

Заседание Совбеза по совершенствованию военной организации РФ на период до 2020 г. (05.07.2013)

«Идёт милитаризация космоса и киберпространства. Широко используются механизмы специальных операций и инструменты так называемой «мягкой силы». Всю совокупность этих факторов мы обязаны учитывать в своей практической работе…



В современных военных конфликтах растёт значение информационных технологий. Так называемые информационные атаки уже применяются для решения задач военно-политического характера. Причём, по оценкам специалистов, их так называемая поражающая сила может быть выше даже, чем от обычных видов оружия.»

Новая редакция Концепции внешней политики РФ (12.02.2013)

(п.20). Впервые введено понятие «мягкая сила» - комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, ИКТ, гуманитарные и другие альтернативные классической дипломатии методы и технологии.

Обращено внимание на риски, связанные с деструктивным и противоправным использованием «мягкой силы» в целях оказания политического давления на государства, вмешательства в их внутренние дела, манипулирования общественным мнением и сознанием.

(п.32 –3,и) Включены меры в интересах обеспечения национальной и МИБ, предотвращения угроз политической, экономической и общественной безопасности РФ, возникающих в информационном пространстве, для борьбы с терроризмом и иными криминальными угрозами в сфере применения ИКТ, противодействовать их использованию в военно-политических целях, противоречащих международному праву, включая действия, направленные на вмешательство во внутренние дела, а также представляющие угрозу международному миру, безопасности и стабильности.

Учитывая особую важность этой проблемы, Россия будет добиваться выработки под эгидой ООН правил поведения по обеспечению МИБ.

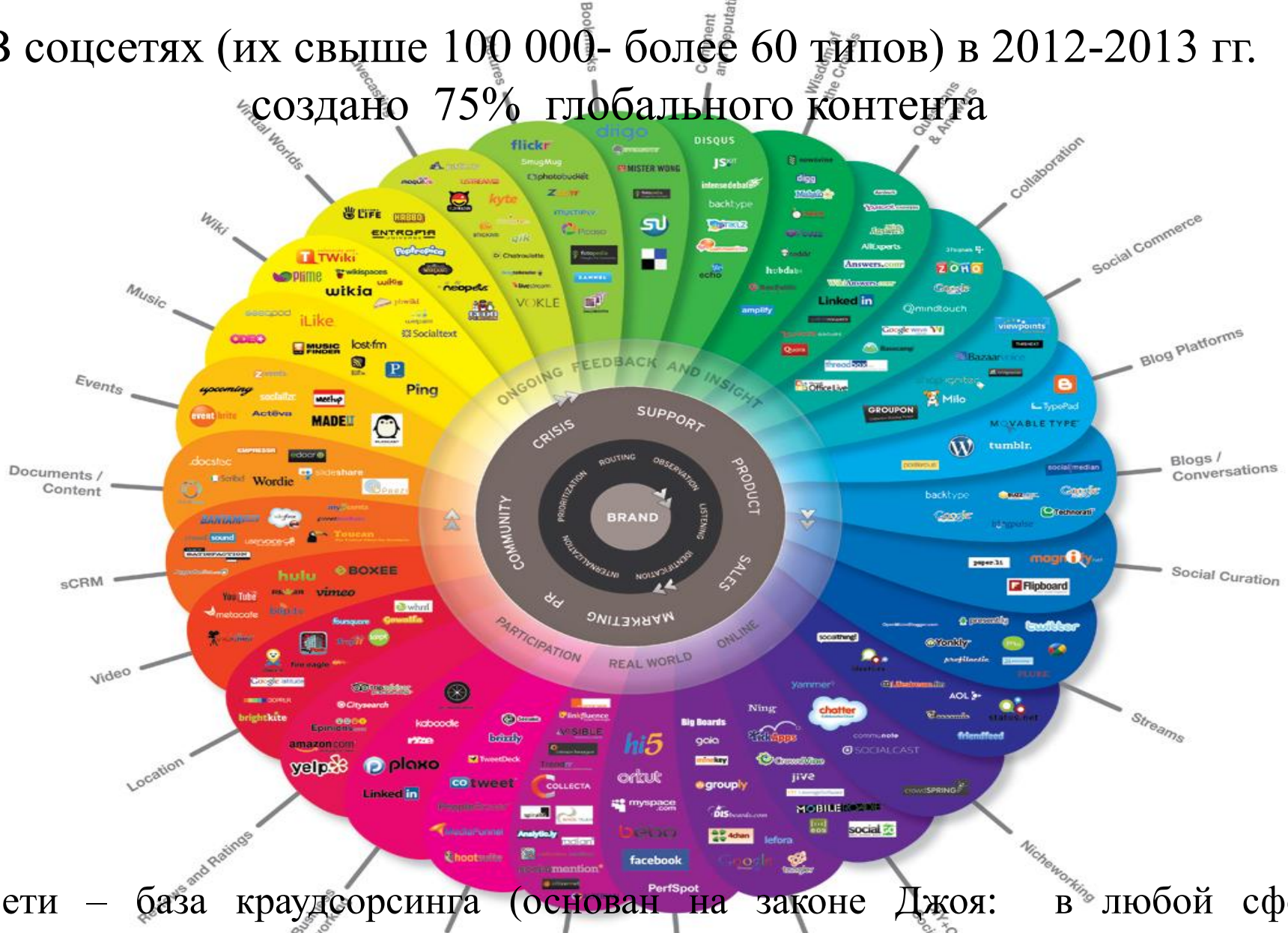
ИКТ в арсенале геополитической конкуренции: «Мягкая сила 2.0»

- В начале 21 века влияние Интернет-среды было существенно ниже влияния СМИ и ТВ - четвертой власти.

  Однако за период с 2010 г., такие события как:
- «арабская весна»,
- летне-осенние беспорядки 2011 г. в Великобритании,
- акция «Захвати Уолл-стрит» в США,
- события по итогам парламентских и президентских выборов в России (2011-2012 г г.)
- В Турции за беспорядки были закрыты ФБ и Твиттер
- Кибервойна в Сирии, на Украине
- «Цифровой фашизм» США (Сноуден: у АНБ «под колпаком» весь мир)

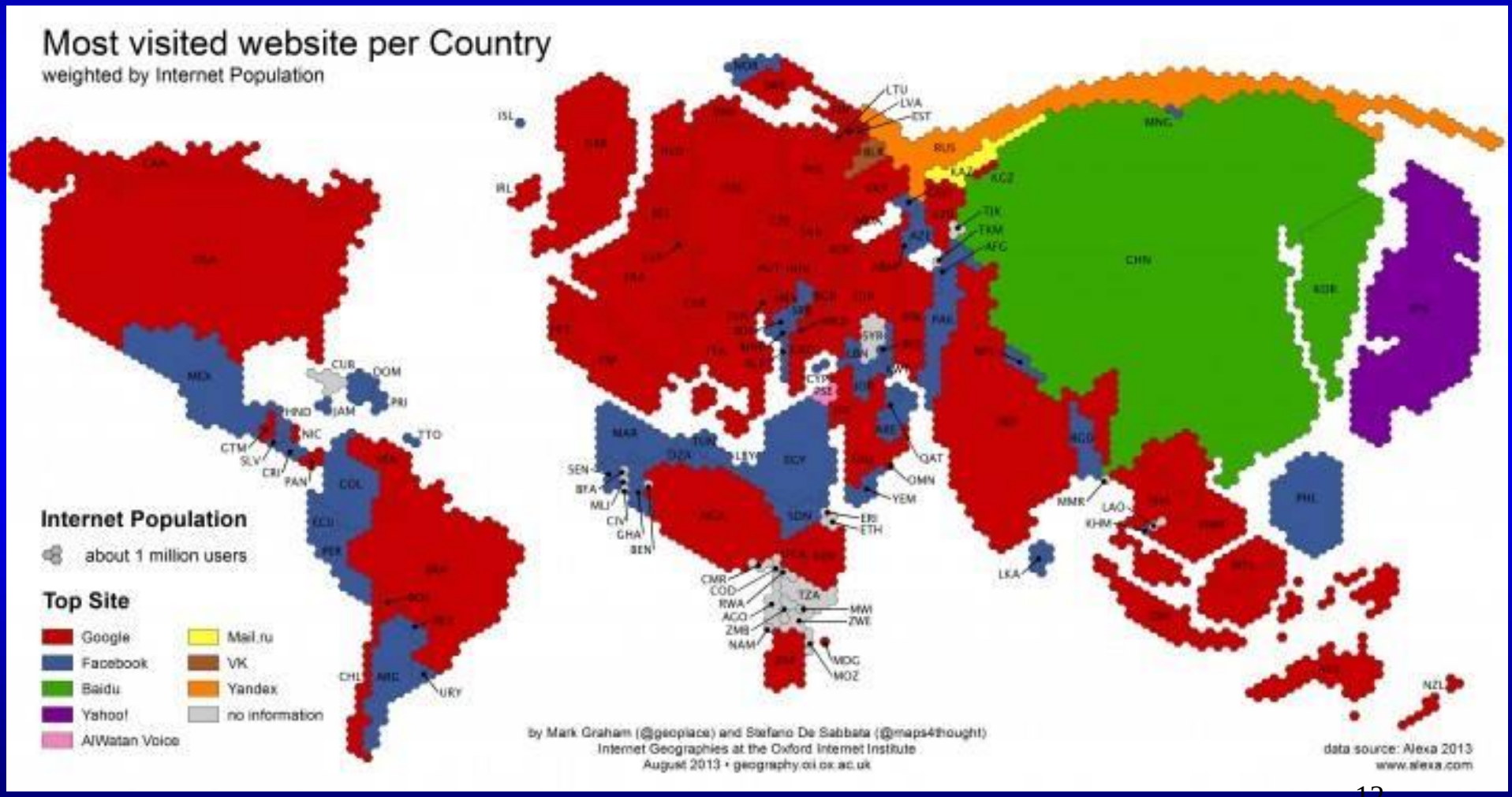
показали потенциал веб-сервисов нового поколения как ПЯТОЙ власти в мире.

В соцсетях (их свыше 100 000- более 60 типов) в 2012-2013 гг. создано 75% глобального контента



Соцсети – база краудсорсинга (основан на законе Джоя: в любой сфере деятельности больше знаний находится за пределами любой действующей в этой сфере структуры и «парадоксе Нейсбитта»: чем сильнее глобализация, тем сильнее ее единицы (Сноуденгейт)

Оксфордский институт интернета: Internet Population and Penetration (Населенность и мера проникновения интернета)



- «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». (Утверждены Президентом РФ 24 июля 2013 г. Пр-1753)
-
- **К числу основных приоритетов отнесено участие России в формировании механизмов международного сотрудничества в области противодействия угрозам использования ИКТ в террористических и экстремистских целях, в т.ч. для вмешательства во внутренние дела суверенных государств.**
- **В целом Основы закрепляют стремление Российской Федерации к масштабному сотрудничеству в деле укрепления мер доверия в сфере применения ИКТ и повышения эффективности переговорного процесса в области формирования системы международной информационной безопасности (МИБ).**

Основные угрозы в области международной информационной безопасности

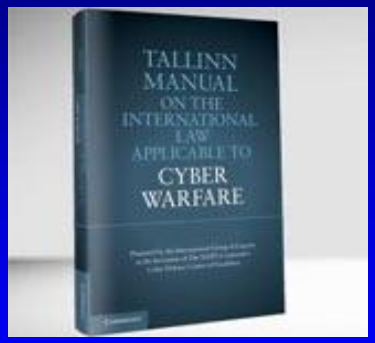
Использование ИКТ в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности

Использование ИКТ для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию

Использование ИКТ в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников

Использование ИКТ для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ

"Таллинское руководство" НАТО о кибервойнах - это их легализация

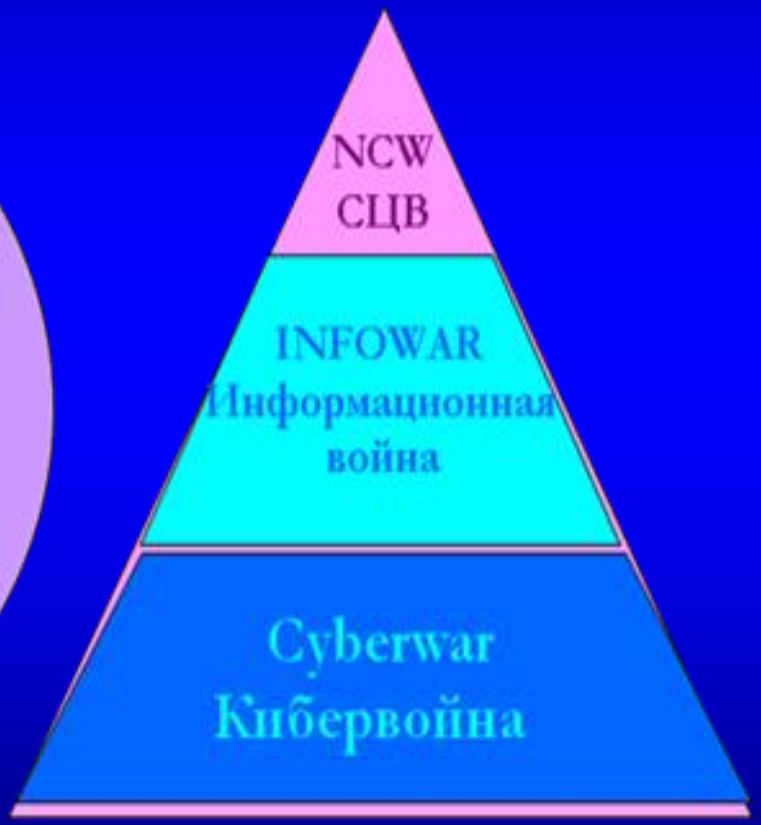


Объединенный центр передового опыта по кибероборонe НАТО (Cooperative Cyber Defense Center of Excellence) разработал первое в мире руководство (2013.300 с.) о применении положений действующего международного права к кибервойнам

Разработано 95 правил, в т.ч.:

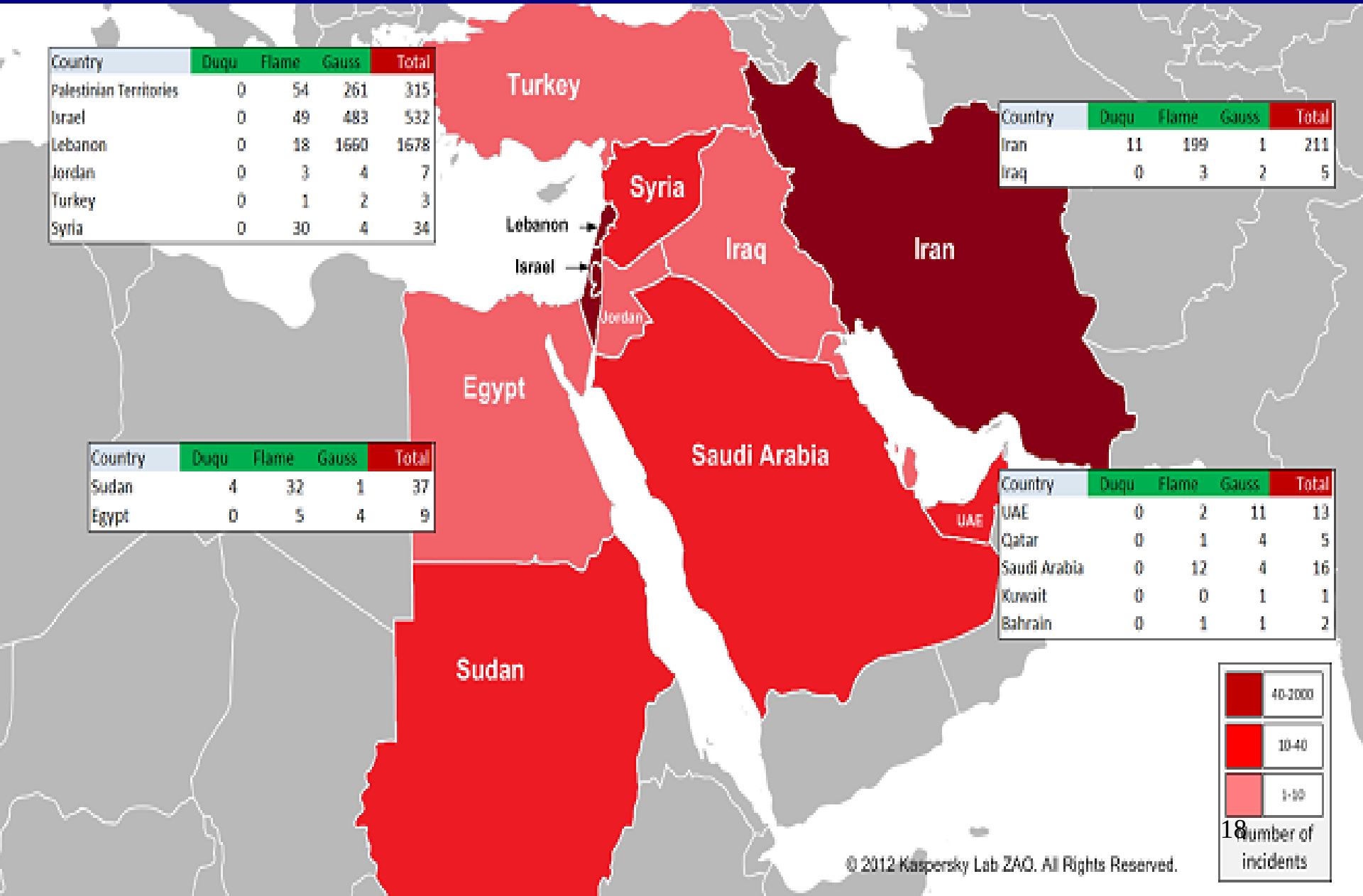
- ответить на атаку государство может либо привлекая агрессора к ответственности, либо "пропорциональными контрмерами"
- Считая атаку "вооруженным нападением", правомерна самооборона , в т.ч. и с использованием традиционного оружия
- кибератаки по силе воздействия следует приравнять к применению химического, биологического и радиологического оружия
- вооруженным нападением не могут быть признаны кибершпионаж, киберкражи и атаки на сайты (кроме ущерба в

Три сферы обращения информации- три вида информационных войн



Алгоритмы составляющих концептов действующих в США доктрин глобального доминирования в XXI веке.
-прямые воздействия «по восходящей» траектории;
- обратные воздействия - «по нисходящей»

Карта обнаруженных лаб. Касперского программ для кибердиверсий и кибершпионажа в регионе



Country	Duqu	Flame	Gauss	Total
Palestinian Territories	0	54	261	315
Israel	0	49	483	532
Lebanon	0	18	1660	1678
Jordan	0	3	4	7
Turkey	0	1	2	3
Syria	0	30	4	34

Country	Duqu	Flame	Gauss	Total
Iran	11	199	1	211
Iraq	0	3	2	5

Country	Duqu	Flame	Gauss	Total
Sudan	4	32	1	37
Egypt	0	5	4	9

Country	Duqu	Flame	Gauss	Total
UAE	0	2	11	13
Qatar	0	1	4	5
Saudi Arabia	0	12	4	16
Kuwait	0	0	1	1
Bahrain	0	1	1	2

Сетевая структура НПО, работающих против России. Иностранные НПО– это эвфемизм подрывной работы

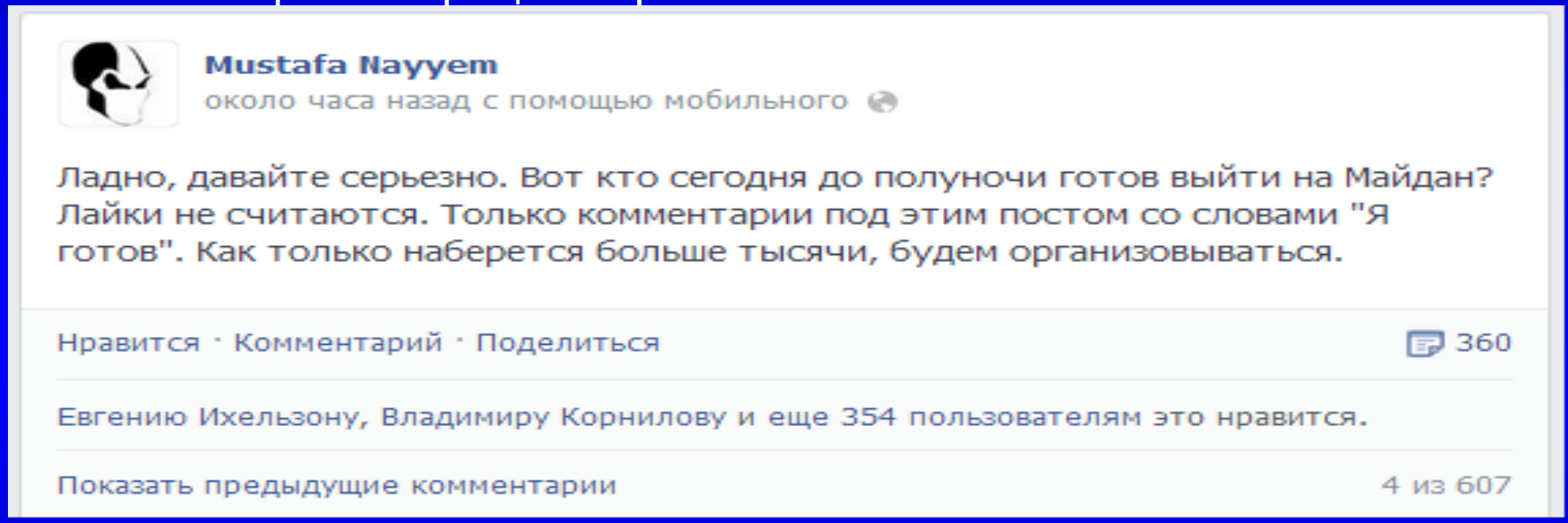
Пример информационного управления в социальной сети

X - Объект целевого воздействия
(Цель – создать требуемое мнение
в сетевом сообществе)

- Использует модели соцсетей
и алгоритмы для поиска влиятельных пользователей
в сети или создания новых агентов
- Оказывает воздействие на влиятельных пользователей
- Требуемое общественное мнение

Пуштун Мустафа Найем позвал на Майдан

21 ноября 2013, 21:22 | 20 хвилин
Известный украинский журналист и блогер Мустафа Найем призвал в Фейсбуке выйти на Майдан Незалежности в знак протеста против остановки евроинтеграции Украины.

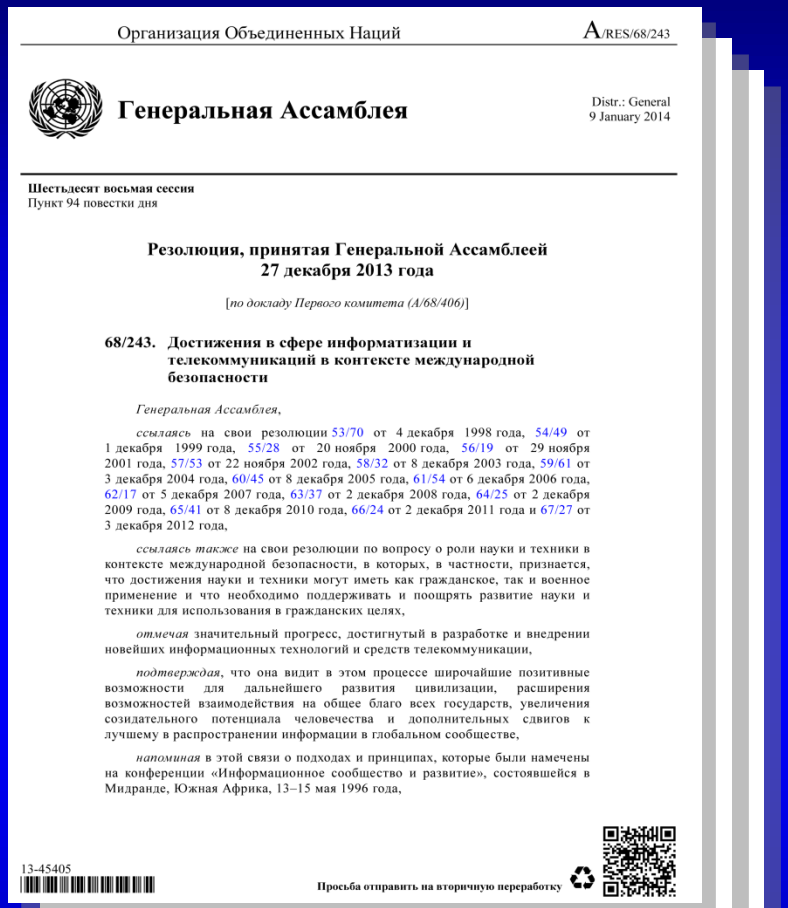


Через час после публикации, количество комментариев перевалило за 600, а желающих выйти на Майдан — более тысячи.
Позже появилось ссобщение: «Встречаемся в 22:30 под монументом Независимости…..

G8 в Сев. Ирландии (Лох-Эрн, 17.06. 2013 г.) президенты РФ и США приняли заявление

- отметили понимание угроз в сфере использования ИКТ: военно-политического, криминального и террористического характера
- объявили о заключении трех «прорывных» договоренностей по системе мер доверия между РФ и США на трех уровнях:

ПРЕДПОСЫЛКИ К ФОРМИРОВАНИЮ КОМПЛЕКСНОЙ СИСТЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Организация Объединенных Наций A/RES/68/243

Генеральная Ассамблея

Distr.: General
9 January 2014

Шестьдесят восьмая сессия
Пункт 94 повестки дня

Резолюция, принятая Генеральной Ассамблеей 27 декабря 2013 года

[*по докладу Первого комитета (A/68/406)*]

68/243. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Генеральная Ассамблея,

ссылаясь на свои резолюции 53/70 от 4 декабря 1998 года, 54/49 от 1 декабря 1999 года, 55/28 от 20 ноября 2000 года, 56/19 от 29 ноября 2001 года, 57/53 от 22 ноября 2002 года, 58/32 от 8 декабря 2003 года, 59/61 от 3 декабря 2004 года, 60/45 от 8 декабря 2005 года, 61/54 от 6 декабря 2006 года, 62/17 от 5 декабря 2007 года, 63/37 от 2 декабря 2008 года, 64/25 от 2 декабря 2009 года, 65/41 от 8 декабря 2010 года, 66/24 от 2 декабря 2011 года и 67/27 от 3 декабря 2012 года,

ссылаясь также на свои резолюции по вопросу о роли науки и техники в контексте международной безопасности, в которых, в частности, признается, что достижения науки и техники могут иметь как гражданское, так и военное применение и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

отмечая значительный прогресс, достигнутый в разработке и внедрении новейших информационных технологий и средств телекоммуникации,

подтверждая, что она видит в этом процессе широчайшие позитивные возможности для дальнейшего развития цивилизации, расширения возможностей взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе,

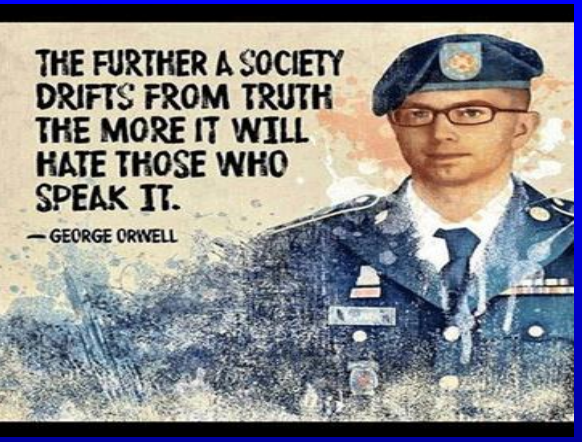
напоминая в этой связи о подходах и принципах, которые были намечены на конференции «Информационное сообщество и развитие», состоявшейся в Мидранде, Южная Африка, 13–15 мая 1996 года,

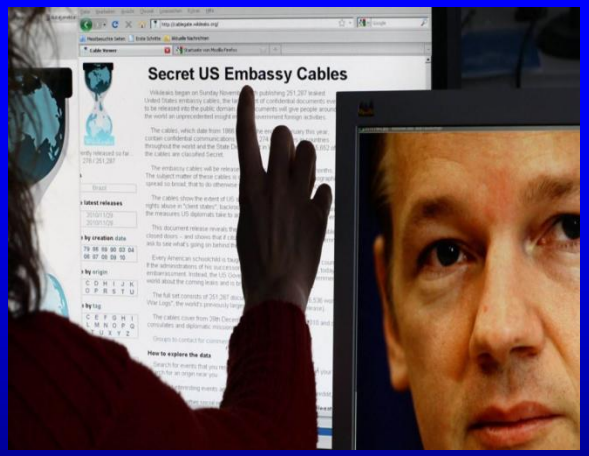
13-45405

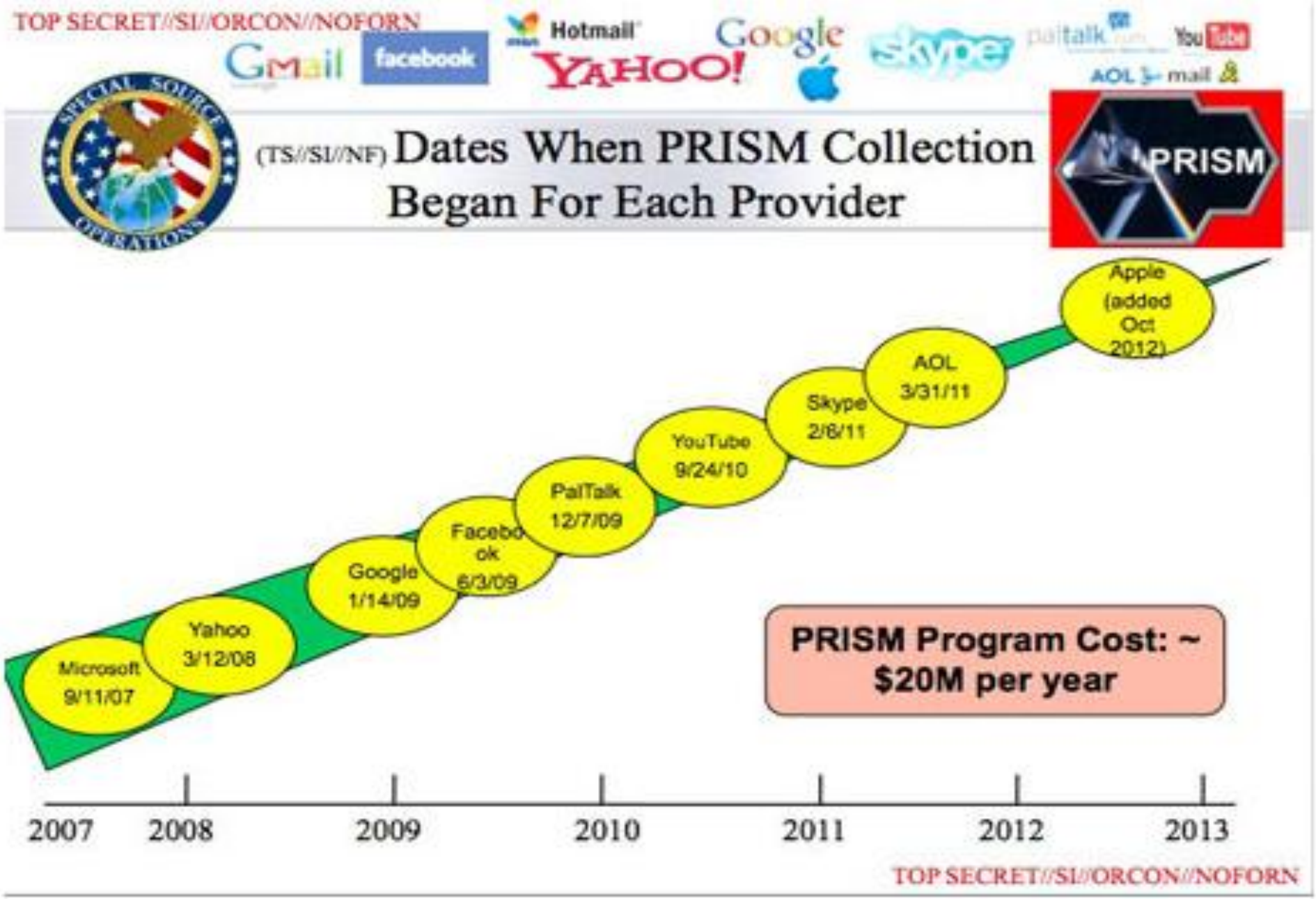
Просьба отправить на вторичную переработку

«SNOWDENGATE»:
судьба в США Мэннинга, Асанжа и Сноудена как подтверждение мысли Дж. Оруэлла:

В дальнейшем общество будет дрейфовать от правды. Оно будет все больше ненавидеть тех, кто её произносит







The extent and nature of the data collected from each company varies.

26 ноября 2013 г. Третий комитет ООН (социальные и гуманитарные проблемы) принял резолюцию предложенную Германией и Бразилией, по прекращению кибершпионажа

Шпионаж в онлайне приравнен к шпионажу в офлайне!

Резолюция будет рассматриваться на Генассамблее (как правило автоматически).

Однако резолюции ООН носят рекомендательный характер.

В силу этого государства-участники могли бы стать инициаторами подготовки юридически обязывающего документа ООН по проблематике МИБ

Сноуден разоблачил «цифровой фашизм» США по отношению ко всему миру

Указ Президента России о создании Национального центра управления обороной государства (НЦУОГ) 10 декабря 2013 г.

- В январе 2014 г. Министр обороны РФ Сергей Шойгу заложил камень начала строительства НЦУОГ. Создаваемый центр станет основным звеном в системе управления военной организацией государства, связывающим действующие в России ведомственные (силового блока) системы управления и мониторинга.

- В НЦУОГ, совместно с федеральными органами исполнительной власти, будут приниматься решения в области обороны, управления повседневной деятельностью Вооруженных Сил, других войск и воинских формирований, а также их всестороннего обеспечения.

Нормативные основы создания системы распределенных ситуационных центров

• Указ
Президента Российской Федерации
от 12 мая 2009 г. № 537
“О стратегии национальной безопасности Российской Федерации до 2020 года”

…

107. Информационная и информационно-аналитическая поддержка **реализации настоящей Стратегии** осуществляется при координирующей роли Совета Безопасности Российской Федерации **с использованием системы распределенных ситуационных центров (СРСЦ), работающих по единому регламенту взаимодействия.**

108. Для развития системы распределенных ситуационных центров в среднесрочной перспективе потребуется **преодолеть технологическое отставание** в важнейших областях информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности, разработать и **внедрить технологии информационной безопасности в системах государственного и военного управления**, системах управления экологически опасными производствами и **критически важными объектами,** а также обеспечить условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами.

Система ситуационных центров

СЦ Администрации Президента РФ

СЦ Контрольного управления Президента РФ

СЦ полномочных представителей Президента РФ

СК главных федеральных инспекторов

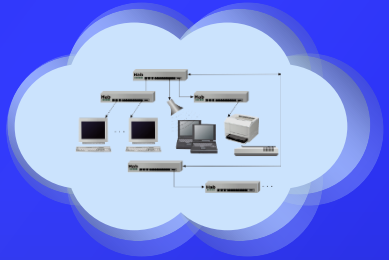
Президент РФ

СЦПР

Мобильный СЦ

Выносной мультимедийный комплекс

Защищенная транспортно-коммуникационная система



СЦ Правительства РФ

Мобильный СЦ

Выносной мультимедийный комплекс

СЦ Президента Белоруссии

СЦ Президента Казахстана

СЦ СБ РФ

СЦ ФСО России

СЦ ФСБ России

СЦ МИД России

СЦ МЧС России

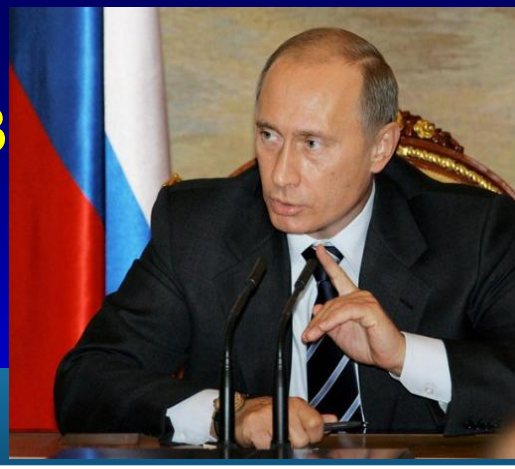
СЦ мэров городов

СЦ глав субъектов РФ

СЦ министерств и ведомств

СЦ предприятий

Концепция общественной безопасности в РФ утверждена Президентом РФ 20.11.2013



Президент России

Новости | Стенограммы | Документы | Поручения | Поездки | Визиты | Телеграммы | Фото | Видео | Аудио

Концепция общественной безопасности в Российской Федерации

20 ноября 2013 года, 13:20

Ключевые слова: правопорядок

Президент утвердил Концепцию общественной безопасности в Российской Федерации.

I. Общие положения

1. Настоящая Концепция представляет собой систему взглядов на обеспечение общественной безопасности как части национальной безопасности Российской Федерации.

2. Настоящей Концепцией определяются основные источники угроз общественной безопасности в Российской Федерации (далее также – общественная безопасность), цели, задачи, принципы и основные направления деятельности уполномоченных государственных органов, а также органов местного самоуправления, иных органов и организаций, принимающих участие в обеспечении общественной безопасности на основании законодательства Российской Федерации (далее – силы обеспечения общественной безопасности). Концептуальные подходы к обеспечению общественной безопасности разработаны в соответствии с положениями Стратегии национальной безопасности Российской Федерации до 2020 года и Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года.

3. Настоящая Концепция является основополагающим документом стратегического планирования, определяющим государственную политику в сфере обеспечения общественной безопасности, а также основой для конструктивного взаимодействия в этой сфере сил обеспечения общественной безопасности и

государственная система мониторинга состояния общественной безопасности (СМОБ)

г) государственная система мониторинга состояния общественной безопасности – единая межведомственная многоуровневая автоматизированная информационная система наблюдения за состоянием общественной безопасности, предназначенная для выявления, прогнозирования и оценки угроз общественной безопасности, оценки эффективности государственной политики, проводимой в сфере обеспечения общественной безопасности, а также для формирования предложений по совершенствованию состояния общественной безопасности;

д) средства обеспечения общественной безопасности – технологии, а также технические, программные, лингвистические, правовые и организационные средства, включая телекоммуникационные каналы и автоматизированные системы управления процессами, используемые для сбора, формирования, обработки, передачи или приёма информации о состоянии общественной безопасности и мерах по её укреплению.

Предложения ГК «Ростех» по созданию СМОБ

1. Определить МВД в качестве Госзаказчика по созданию СМОБ для субъектов федерации России в координации с заинтересованными министерствами и ведомствами
2. Разработать и реализовать ФЦП «СМОБ», включающую создание региональных и муниципальных центров мониторинга и управления, их взаимодействия с существующими антитеррористическими комиссиями и комиссиями по чрезвычайным ситуациям, КАСУ ДЧ ГУ МВД региона и другими экстренными оперативными службами
3. Разработать типовую отечественную защищённую технологическую платформу для реализации региональных СМОБ на основе АТК и КЧС региона на базе разработок Госкорпорации «Ростех»

Создание технологической платформы на базе разработок ГК «Ростехнологии»

ГК «Ростехнологии имеет опыт реализации:

- КАС «Безопасный город» Красноярск
- Система обеспечения безопасного города (СОБГ) г. Москва
- КАСУБ ФСК ЕЭС, включая объекты Сочи-2014 и АТЭС
- Ситуационные центры ФСБ, ФСО, Совета Безопасности РФ,
- губернаторов Санкт-Петербурга, Красноярского края

Имеется:

- Мощная технологическая и производственная база
- Опыт решения вопросов информационной безопасности

СМОБ создается путем интеграции уже действующих и вновь создаваемых систем в сфере общественной безопасности – Система-112, «Безопасный город», ЭРА-ГЛОНАСС, РНИИС, ЦБДД, ИТС, ТП РСЧС, системы полиции КАСУ ДЧ («02»), АС ЦУИС противопожарной службы («01»), скорой медицинской помощи («03»), аварийной газовой службы («04») и др.

Цель создания СМОБ

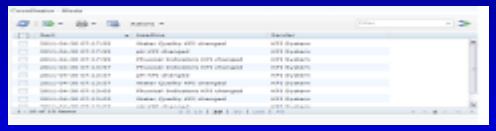
Комплексная модернизация инфраструктуры и процессов обеспечения общественной безопасности региона, которая позволит создать для жителей безопасные и комфортные условия жизни и работы, за счет применения новейших ИКТ

Состав сегментов СМОБ и основные задачи

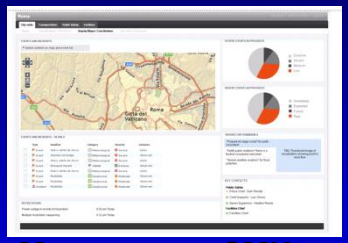
	Подсистема видео наблюдения	Подсистема Мониторинга Подвижных объектов	Подсистема Экстренного оповещения	ДДС и другие Подсистемы СМОБ	Система 112
 Сегмент администрации региона(района), ЖКХ (Умный город)	●	●	○	●	●
 Правоохранительный сегмент МВД (КАСУ ДЧ	●	●	○	●	●
 Сегмент МЧС, ТП РСЧС			●	●	●
 Сегмент служб медицинской помощи		●	●	●	●
 Сегмент управления общественным Транспортом (ИТС)	●	●		●	●
 Сегмент служб ФСКН и ФМС	●	●	●	●	●
Сегменты ТЭК и других структур	●				●

Состав компонентов технологической платформы создания СМОБ

Видеонаблюдение



Аналитика – выявление взаимосвязи событий



Мониторинг СМИ и блогов

Executiv

Система-112

ДДС МВД, МЧС, АТЦ

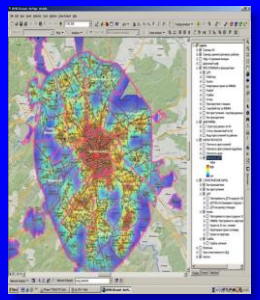
Управление доступом

Оповещение (SMS, Phone, E –mail)

Интеллектуальная транспортная система

Областной Центр мониторинга и Управления (АТК, КЧС)

Тепловые карты

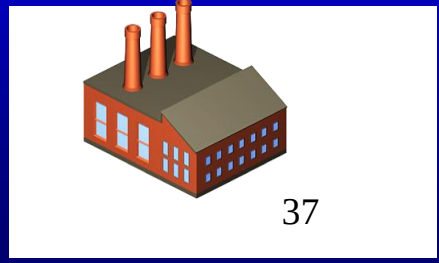


Контакт-Центр 311

ЖКХ

Паспорта объектов

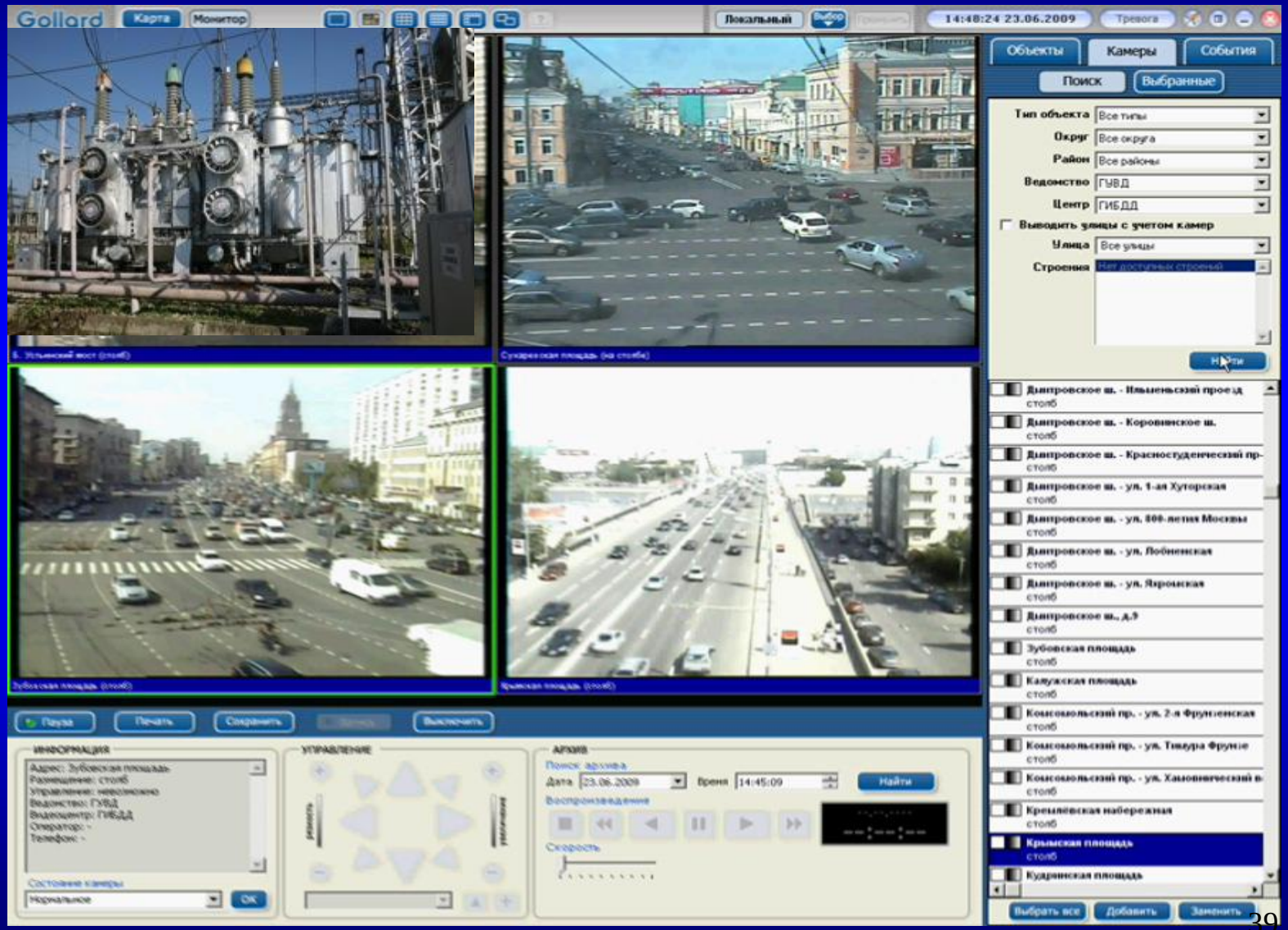
ДДС Объекты Критической Инфраструктуры



Инфраструктурные Компоненты СМОБ

- Защищённая телекоммуникационная сеть передачи данных
- Единая областная картографическая основа
- Единая база данных событий
- Система информационной безопасности
- Региональный Центр мониторинга и управления
- Муниципальный Центр мониторинга и управления

Видеоаналитика – основа функционирования интеллектуальной системы видеонаблюдения



Мониторинг ресурсного обеспечения объектов региона

ОЦОУ

Сообщения о несоответствии параметров ресурсообеспечения

ОКИ

Предоставляемые ресурсы

- Тепло
- Газ
- Электричество
- Водоснабжение

Параметрические сигналы

- Тнв= - 40С, Т1<60С
- Нет электричества
- U>240В
- Нет давления

Система мониторинга социальной обстановки. RTECAiqumena

Система обеспечивает автоматическое отслеживание текущего состояния социальной обстановки посредством оперативного получения данных из электронных СМИ, социальных сетей, блогов, форумов, телефонных и интернет-опросов (Мультимедийный Контакт-Центр)

Интернет

- Электронные СМИ
- Google, Yandex, Rambler
- Интернет-Блоги, форумы
- Социальные сети (Twitter, Facebook)

Контакт-центр и Система оповещения населения (СОН) типа 311

СОН функционирует в двух режимах:

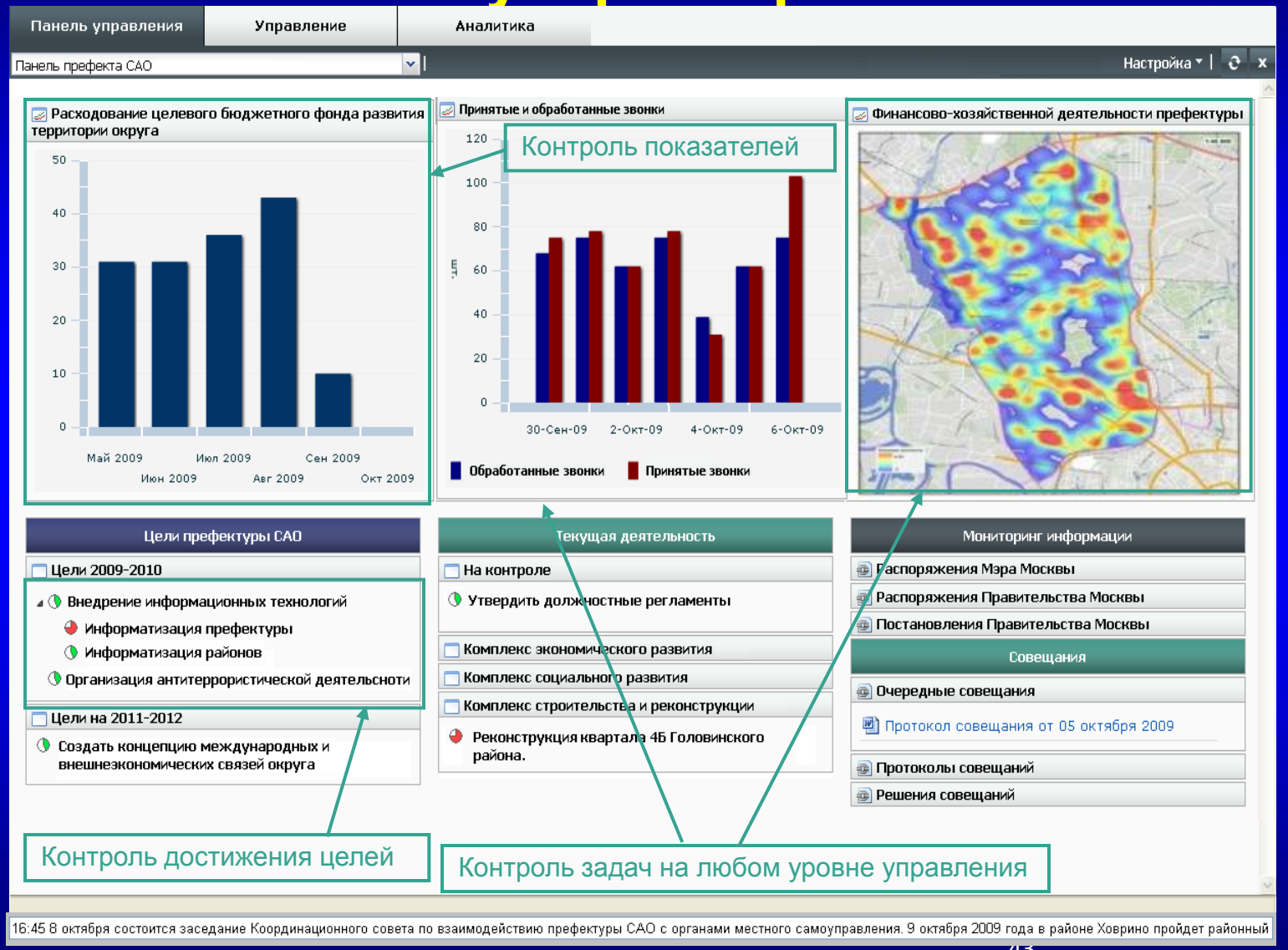
Штатный режим: трансляция сообщений различного характера, в том числе в режиме реального времени и на основе местоположения

Режим ЧС: Взаимодействие с Системой Оповещения МЧС

СОН позволяет оповещать население по различным каналам:

- **Телефон**
- **SMS**
- **Интернет**
- **Телевидение**
- **Радиотрансляция**
- **Электронные табло и SOS-терминалы**
- **Общественный транспорт**

Портал общественной безопасности губернатора



Эффекты от внедрения - Безопасность

- Мониторинг социальной обстановки и общественного мнения в режиме online, мониторинг инцидентов
- Превентивные меры противодействия массовым беспорядкам
- Эффективное противодействие террористическим угрозам

Эффекты от внедрения – в цифрах

50% ↓ число дорожно-транспортных происшествий со смертельным исходом

10-15% ↑ пропускная способность улично-дорожной сети

20-25% ↓ вредные выбросы

5% ↓ количество краж

25% ↓ потребление тепла

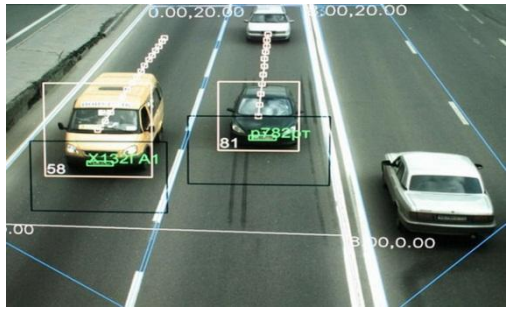
20% ↓ количество аварий

Пример: План перехват

до внедрения

задействован весь личный состав органов внутренних дел (более 1тыс. человек)

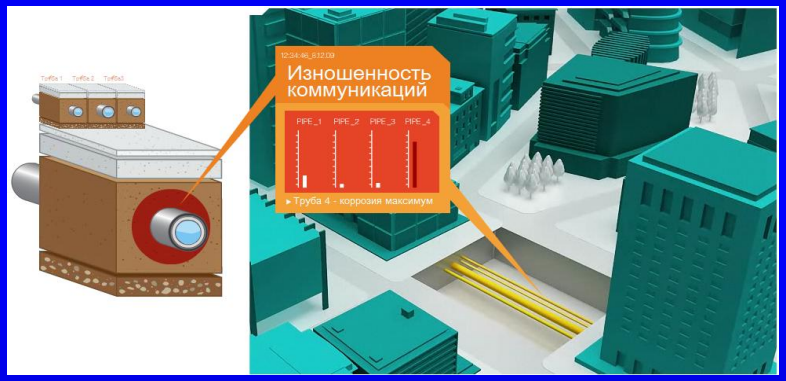
после внедрения



автоматическая идентификация и слежение за подозреваемым

Эффекты от внедрения – Сервисы, оповещения, транспорт, ЖКХ

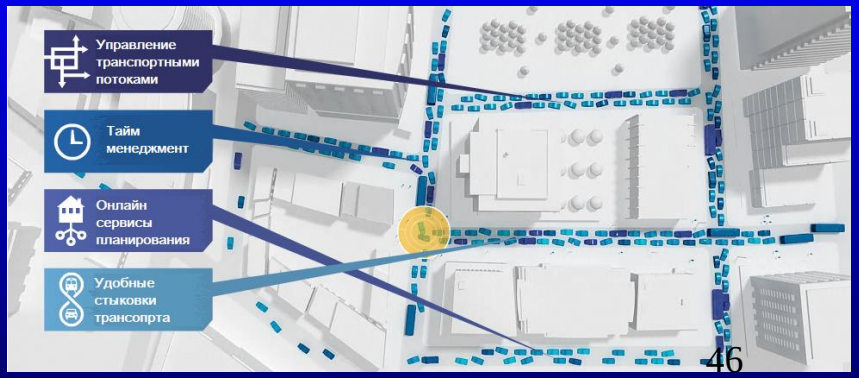
50% ↑ Оперативное оповещение служб региона и населения о ЧС



Эффективный инструмент управления и мониторинга состояния ЖКХ

10-15% ↑

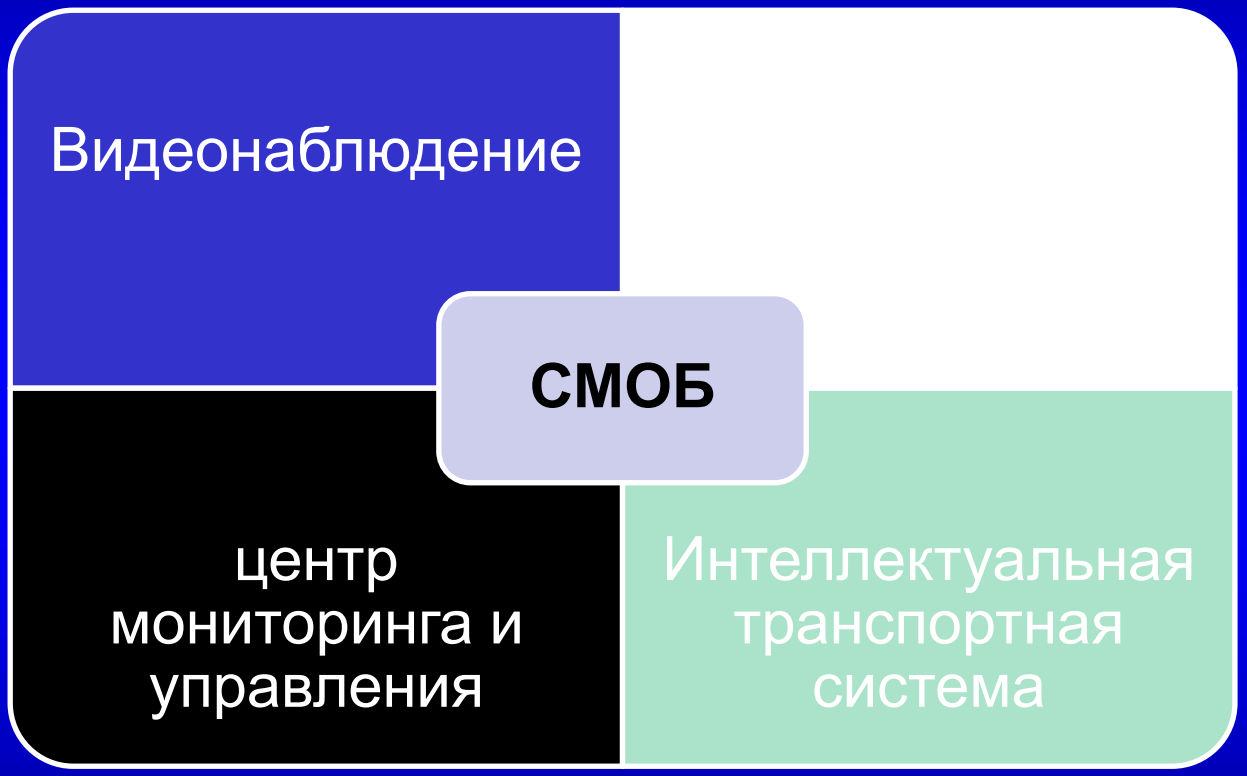
35% ↑ Мониторинг транспортной сети региона в режиме реального времени



Примерные технические параметры СМОБ региона

30 000 камер видеонаблюдения и видео фиксаций нарушений

Оптическая сеть 40 Гб/с,
Облачные технологии



1 500 кв. метров,
3-х этажное здание с 2-мя ситуационными залами(ИТС и РЦМУ)

умные перекрёстки,
100%-ный охват транспорта GPS/GLONASS трекингом

Преимущества проекта

1. Максимальное использование готовых отечественных решений и компонентов
2. Инвестирование в российские разработки, создание конкурентоспособной на мировом рынке продукции в области общественной безопасности
3. Обеспечение информационной безопасности
4. Постороение национальной системы управления общественной безопасностью

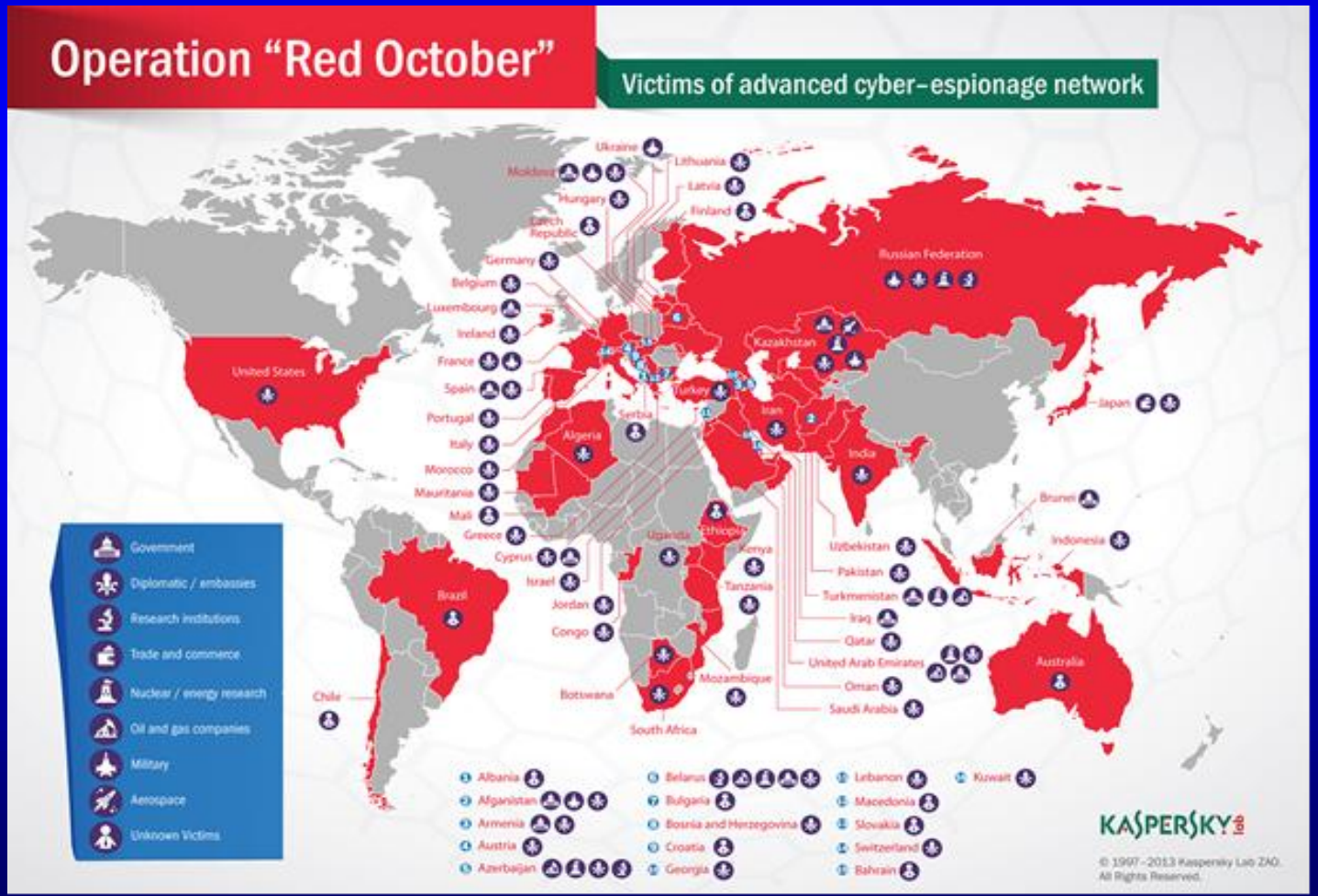
В. Путин на заседании коллегии ФСБ России (07.04.2014):

- ФСБ России сфокусируется на пресечении действий злоумышленников и усилении защищённости нацинформресурсов, линий связи, баз данных органов власти и управления, содержащих гостайну.
- В 2013 г. было обнаружено и пресечено более 9 млн. воздействий на интернет-сайты и нформсистемы органов госвласти России.
- Нужно быть готовыми к тому, что такие попытки вторгнуться в наше информационное поле будут продолжаться….

Кризис на Украине привел к взрывному росту кибердиверсий:

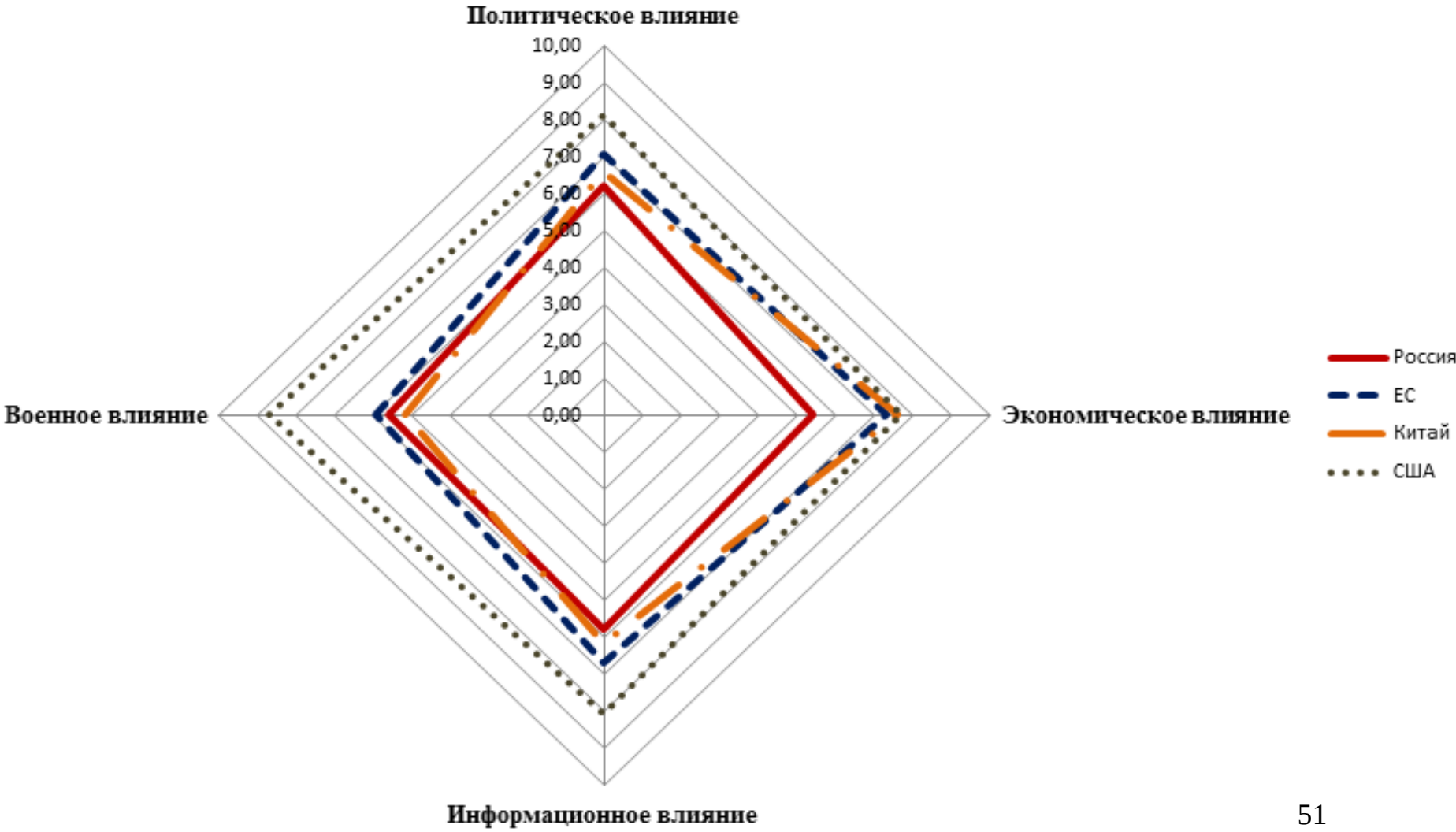
- DDoS-атаки на системы НАТО хакеров «КиберБеркут», кибератаки на сайты Президента РФ, МИД России, Центробанка, крупных СМИ и агентств, РЭБ-атаки на российские телеспутники на западе Украины…
- Возросла опасность распределенных атак на госинформсистемы, кредитно-банковские структуры, объекты в экономической и социальной сферы, систем жизнеобеспечения и других КВО. Еще в 2011 г. ведущие державы мира создали свой киберарсенал.

'Red October' –
кибершпионаж против дипломатических и госучреждений
Указ Президента РФ от 15.01.2013 №31 с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"



НИИГЛОБ: «Глобальная безопасность в цифровую эпоху: стратагемы для России» (дроби Фишберна)

Рис.13. Структура сетевого влияния



Об авторах

СМИРНОВ Анатолий Иванович -
Президент Национального института исследований глобальной безопасности (НИИГлоБ), член Президиума Российской академии естественных наук, доктор исторических наук, профессор, Чрезвычайный и Полномочный Посланник Российской Федерации в отставке, Почетный доктор Северного (Арктического) федерального университета имени М.В.Ломоносова

КОХТЮЛИНА Ирина Николаевна -
Ответственный секретарь Научного совета Национального института исследований глобальной безопасности (НИИГлоБ), член-корреспондент Российской академии естественных наук, кандидат политических наук

Глобальная безопасность и "мягкая сила 2.0": вызовы и возможности для России

А.И.Смирнов
И.Н.Кохтюлина

НАЦИОНАЛЬНЫЙ ИНСТИТУТ
ИССЛЕДОВАНИЙ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

А.И.СМИРНОВ
И.Н.КОХТЮЛИНА

ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ и "МЯГКАЯ СИЛА 2.0":

ВЫЗОВЫ И ВОЗМОЖНОСТИ ДЛЯ РОССИИ

www.niiglob.ru

СПАСИБО ЗА ВНИМАНИЕ!

Якутск_лекция

aismirnov@niiglob.ru

http://niiglob.ru/