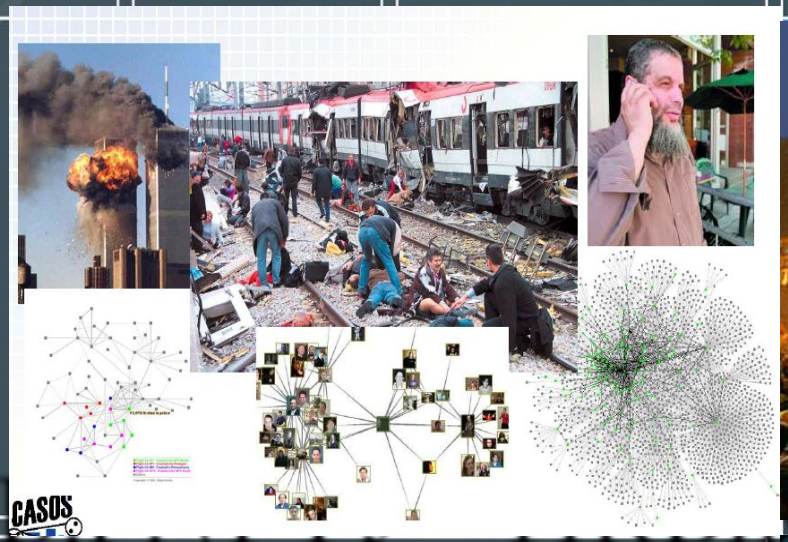
НАЦИОНАЛЬНАЯ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Лекция № 2)

Российский технологический университет -МИРЭА
(Институт комплексной безопасности и специального приборостроения)



Григорьев В.Р. (РТУ - ИКБиСП)
зав. кафедрой «Информационное противоборство», зам. директора ИКБСП
к.т.н., доцент, член-корр. РАЕН

Раздел 3.
Информационная безопасность и информационное противоборство в системе обеспечения национальной безопасности Российской Федерации

Защита информации в информационно-технической сфере

Устойчивая работа информационных систем, средств коммуникаций и связи, их защищенность имеют для страны стратегическое значение. Это важный фактор обеспечения суверенитета, обороноспособности страны, безопасности государства. Нужно учитывать, что уровень угроз в информационном пространстве повышается, число рисков увеличивается, а негативные последствия разного рода кибератак носят уже не локальный, а действительно глобальный характер и масштаб.

…Внешнее вторжение в электронные системы в сфере обороны и госуправления, жизнеобеспечивающие инфраструктуры, финансов, утечка электронных документов могут обернуться самыми тяжелыми последствиями. Следует повысить безопасность и устойчивость работы инфраструктуры российского сегмента Интернета. При этом подчеркну, речь не может идти об ограничении доступа законопослушных граждан к ресурсам глобальной сети, каких-то тотальных барьерах и фильтрах.

Владимир Путин.

Структурно-функциональные компоненты системы информационно-технологического обеспечения органов государственного управления

Электронный документооборот

ЗНАЧИТЕЛЬНО СОКРАЩАЕТ СРОКИ ПОДГОТОВКИ И СОГЛАСОВАНИЯ ДОКУМЕНТОВ, УПРОЩАЕТ ПРОЦЕДУРУ ИХ ПОИСКА, ОБЕСПЕЧИВАЕТ СОХРАННОСТЬ ДОКУМЕНТОВ

Информационно-управляющие системы

ПОЗВОЛЯЮТ ПРОВОДИТЬ МНОГОМЕРНЫЙ АНАЛИЗ ДАННЫХ, ОПРЕДЕЛЯТЬ ПРОБЛЕМНЫЕ ОБЛАСТИ, ОПЕРАТИВНО ФОРМИРОВАТЬ АГРЕГИРОВАННЫЕ ОТЧЕТЫ

Система ситуационных центров

ОБЕСПЕЧИВАЕТ ИНФОРМАЦИОННУЮ И ИНТЕЛЛЕКТУАЛЬНУЮ ПОДДЕРЖКУ ДЕЯТЕЛЬНОСТИ РУКОВОДИТЕЛЕЙ ОГВ, КОЛЛЕКТВНУЮ ПОДГОТОВКУ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ НА ОСНОВЕ НОВЕЙШИХ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Сеть видеоконференцсвязи

ОБЕСПЕЧИВАЕТ ОПЕРАТИВНЫЙ ИНФОРМАЦИОННЫЙ ОБМЕН И НЕПОСРЕДСТВЕННОЕ УЧАСТИЕ РУКОВОДИТЕЛЕЙ ОГВ и ГРУПП СПЕЦИАЛИСТОВ В ОПЕРАТИВНОМ УПРАВЛЕНИИ, в т.ч. при проведении мероприятий в необорудованных местах и удаленных регионах

Централизованные государственные регистры

РЕАЛИЗУЮТ БЫСТРЫЙ ДОСТУП К ВСЕОБЪЕМЛЮЩЕЙ И ТОЧНОЙ ИНФОРМАЦИИ ОБ ОСНОВНЫХ ОБЪЕКТАХ УПРАВЛЕНИЯ

Электронные закупки для государственных нужд

ОБЕСПЕЧИВАЮТ СНИЖЕНИЕ ЦЕН НА ПРИОБРЕТАЕМУЮ ПРОДУКЦИЮ ЗА СЧЕТ УПОРЯДОЧИВАНИЯ И ПОВЫШЕНИЯ ПРОЗРАЧНОСТИ ПРОЦЕССОВ

Взаимодействие граждан и бизнеса с государством

СОКРАЩАЕТСЯ ВРЕМЯ ГРАЖДАН И ОРГАНИЗАЦИЙ НА ВЗАИМОДЕЙСТВИЕ С ОРГАНАМИ ВЛАСТИ ЗА СЧЕТ УМЕНЬШЕНИЯ КОЛИЧЕСТВА БУМАЖНЫХ ДОКУМЕНТОВ, ПОДАВАЕМЫХ И ПОЛУЧАЕМЫХ ИЗ ГОСУЧРЕЖДЕНИЙ, УМЕНЬШАЕТСЯ КОЛИЧЕСТВО И СОКРАЩАЕТСЯ ВРЕМЯ ПОСЕЩЕНИЙ ГОСУЧРЕЖДЕНИЙ

Из лекции д.т.н, профессора А.Н.Павлов, РАНХиГС «Государственная политика в области создания информационного общества»

Из лекции д.т.н, профессора А.Н.Павлов, РАНХиГС «Государственная политика в области

Структура организации управления РФ

21 министерство

8 федеральных округов

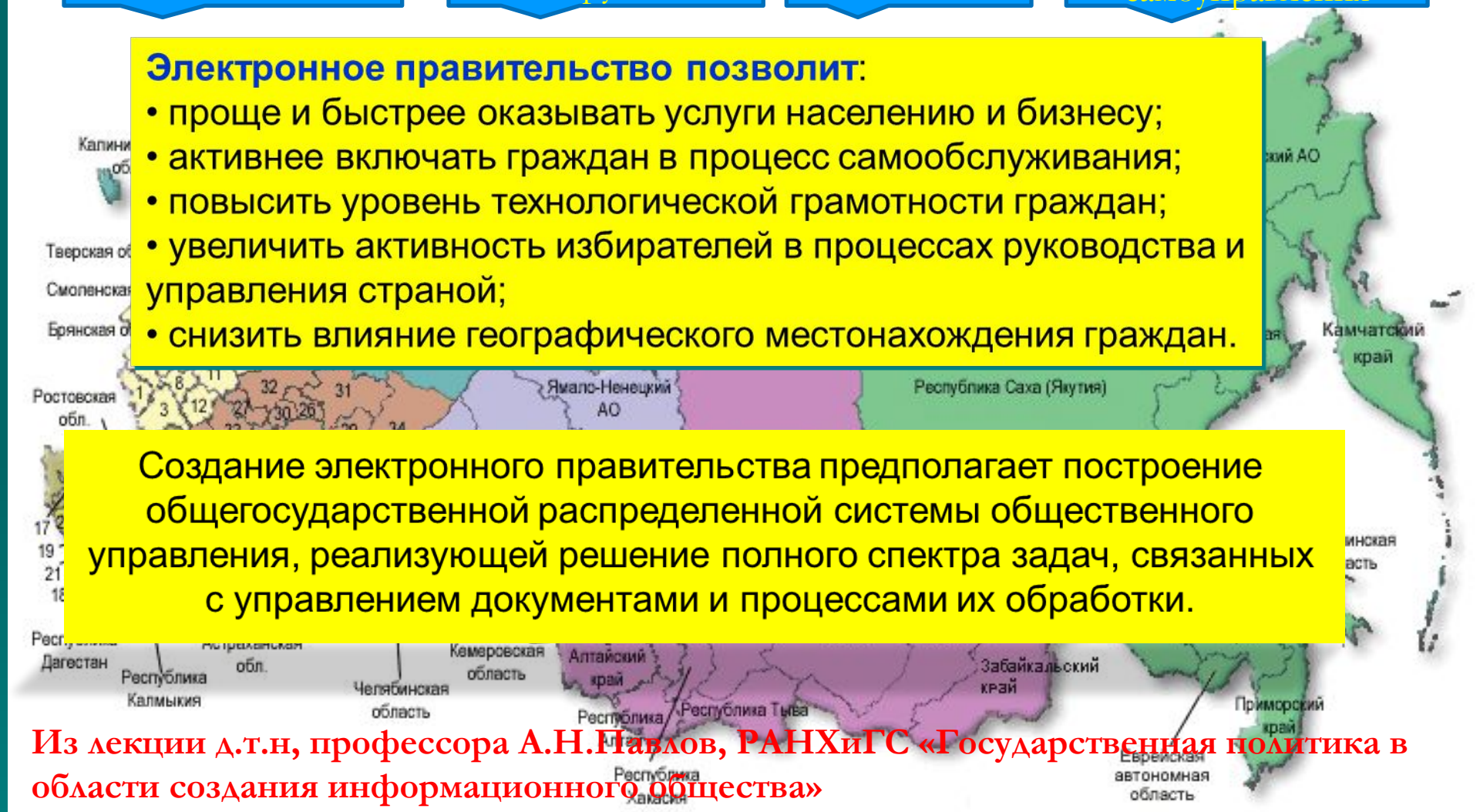
84 субъекта

24000 органов местного самоуправления

Электронное правительство позволит:

- проще и быстрее оказывать услуги населению и бизнесу;
- активнее включать граждан в процесс самообслуживания;
- повысить уровень технологической грамотности граждан;
- увеличить активность избирателей в процессах руководства и управления страной;
- снизить влияние географического местонахождения граждан.

Создание электронного правительства предполагает построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки.



Из лекции д.т.н, профессора А.Н.Павлов, РАНХиГС «Государственная политика в области создания информационного общества»

Цели создания инфраструктуры электронного правительства

Информационная и телекоммуникационная инфраструктура обеспечивает:

- ***повышение доступности*** **электронных способов взаимодействия с органами государственной власти для организаций и граждан;**
- ***уменьшение времени*** **затрачиваемого населением на взаимодействие с органами государственного управления;**
- ***снижение затрат*** **государственного бюджета на выполнение однотипных функций общегосударственной важности благодаря централизованной их реализации;**
- ***снижение затрат*** **органов государственного управления на предоставление государственных услуг и выполнение государственных функций в электронном виде;**
- ***создание единой технологической платформы*** **для оперативного защищенного информационного обмена между органами государственной власти.**

Из лекции д.т.н, профессора А.Н.Павлов, РАНХиГС «Государственная политика в области создания информационного общества»

Классически считалось, что обеспечение безопасности информации складывается из трех составляющих: Конфиденциальности, Целостности, Доступности. Точками приложения процесса защиты информации к информационной системе являются аппаратное обеспечение, программное обеспечение и обеспечение связи (коммуникации). Сами процедуры (механизмы) защиты разделяются на защиту физического уровня, защиту персонала и организационный уровень

ОБОБЩЕННАЯ МОДЕЛЬ МОНИТОРИНГА УГРОЗ

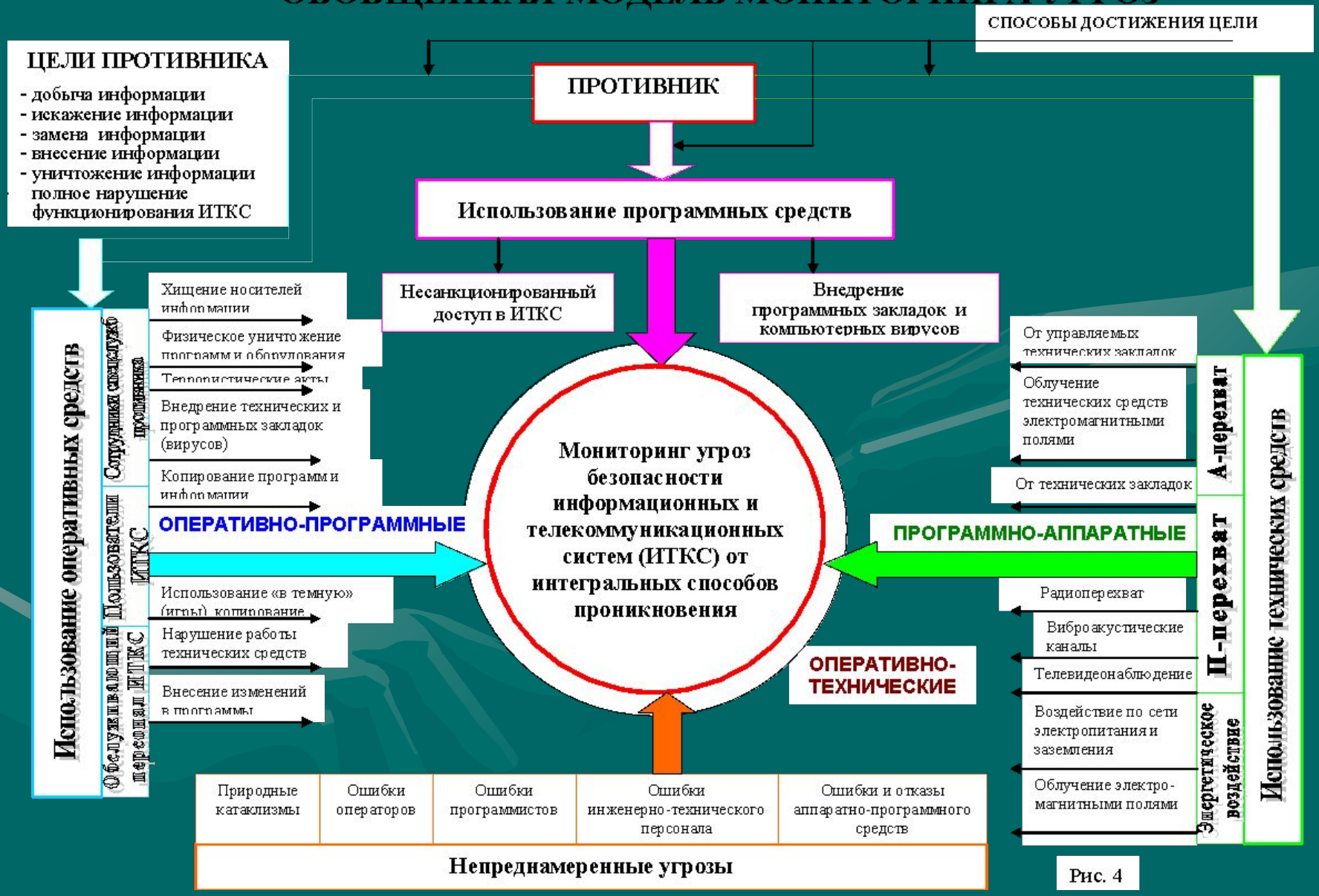


Рис. 4

Интегральный показатель защищенности информации

- В общем случае интегральный показатель защищенности информации *Z* определяется в следующем виде:

$$Z(T) = \Phi[K, R(T)]$$

где *K* - показатель полноты учёта возможных стратегий нападения, на противостояние которым нацелено СЗИ при её разработке;

R - показатель эффективности применения конструктивно заложенных в СЗИ стратегий защиты информации на интервале от *0* до *t*,

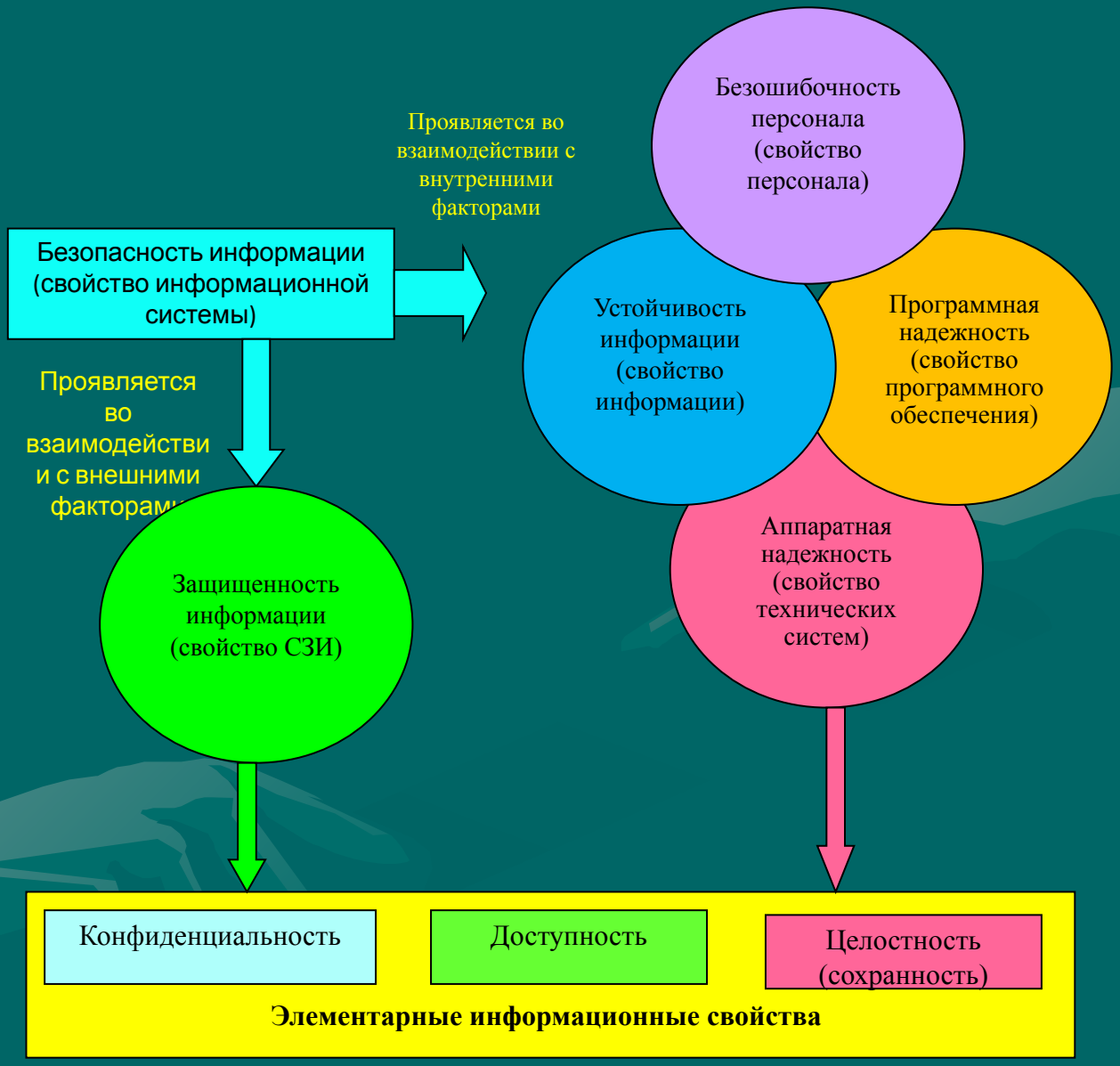
R с позиции теории эффективности может интерпретироваться как вероятность выполнения задачи в информационной системе в условиях информационного противоборства при ограничениях на другие возмущающие факторы (отказы, ошибки и т. д.).

Если известно распределение вероятностей d_i применения СИН всех стратегий нападения, то возможна трактовка показателя учёта стратегий нападений *K* следующим образом:

$$K = \sum_{i=1}^{n} d_i,\ n > k$$

где *n* — это количество стратегий нападения, учитываемых в данной СЗИ.

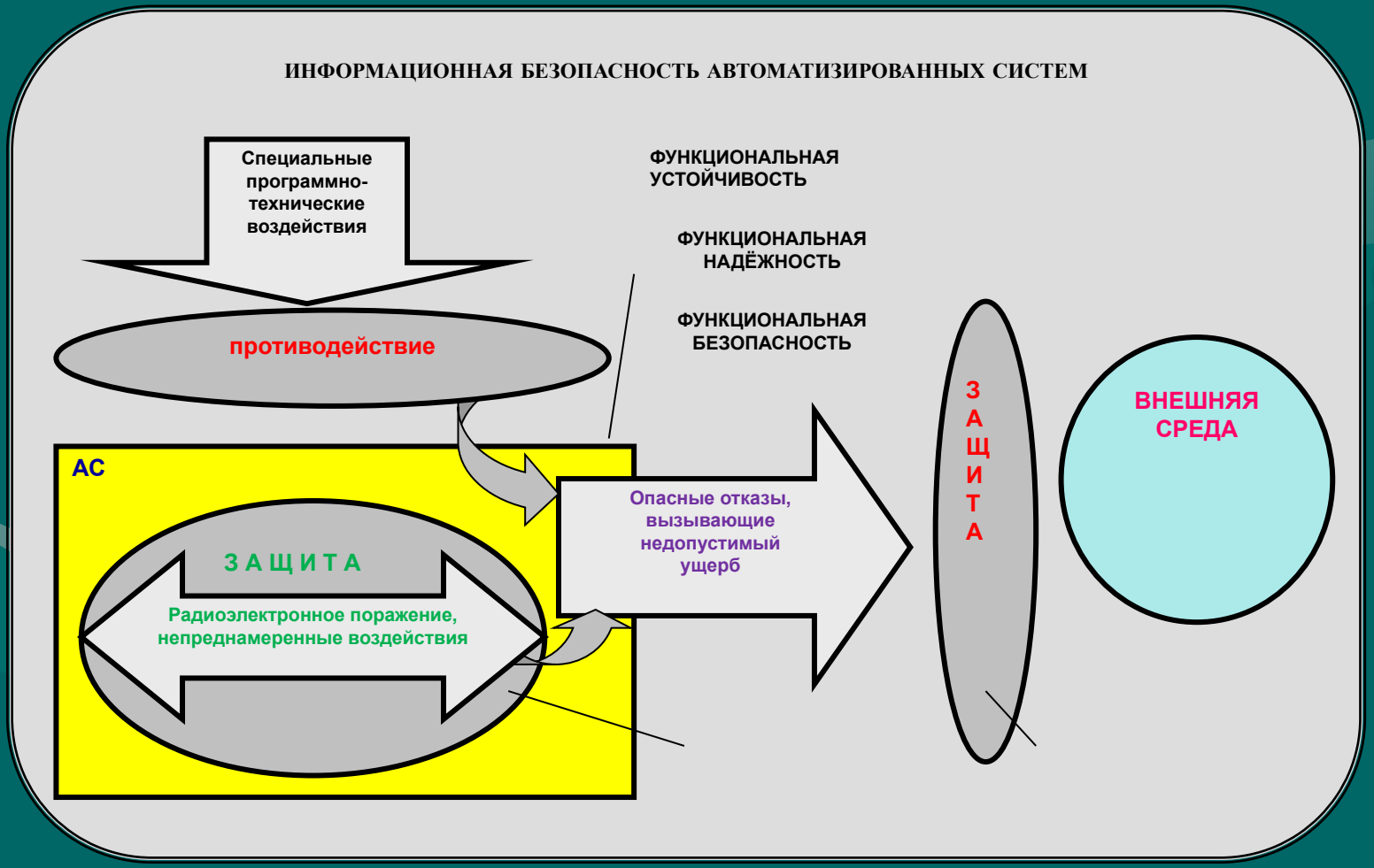
Иерархическая взаимосвязь основных свойств информационной системы АСУ



Выделяют и другие категории модели безопасности:

- неотказуемость или апеллируемость — невозможность отказа от авторства;
- подотчётность — обеспечение идентификации субъекта доступа и регистрации его действий;
- достоверность — свойство соответствия предусмотренному поведению или результату;
- аутентичность или подлинность — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Существенные свойства АС, связанные с их информационной безопасностью



Нормативно-правовая база обеспечения информационной безопасности информационно-технической сферы в Российской Федерации

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

Предметом регулирования данного Закона являются общественные отношения, возникающие в трех взаимосвязанных направлениях:

- формирование и использование информационных ресурсов;
- создание и использование информационных технологий и средств их обеспечения;
- защита информации, прав субъектов, участвующих в информационных процессах и информатизации.

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

В Законе также отражены вопросы, связанные с порядком обращения с персональными данными, сертификацией информационных систем, технологий, средств их обеспечения и лицензированием деятельности по формированию и использованию информационных ресурсов.

Федеральный закон "О безопасности" от 28.12.2010 № 390-ФЗ

ФЗ-390 регулирует принципы обеспечения безопасности:

- личной;
- общественной;
- государственной;
- экологической;
- национальной.

Федеральным законом №390 устанавливаются полномочия и функции государственных органов в сфере сохранности.

Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ

Основными принципами обеспечения безопасности являются:

1. соблюдение и защита прав и свобод человека и гражданина;
2. законность;
3. системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
4. приоритет предупредительных мер в целях обеспечения безопасности;
5. взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "**особой важности**", "**совершенно секретно**" и "**секретно**".

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»

Государственную тайну составляют:

1. сведения в военной области;
2. сведения в области экономики, науки и техники;
3. сведения в области внешней политики и экономики;
4. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер

Не подлежат отнесению к государственной тайне сведения:

1.о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

2.о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

3.о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

4.о фактах нарушения прав и свобод человека и гражданина;

5.о размерах золотого запаса и государственных валютных резервах Российской Федерации;

6.о состоянии здоровья высших должностных лиц Российской Федерации;

7.о фактах нарушения законности органами государственной власти и их должностными лицами.

Вместе с тем, в соответствии со статьей 7 Закона РФ "О государственной тайне", не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

- о фактах нарушения прав и свобод человека и гражданина;

- о размерах золотого запаса и государственных валютных резервах Российской Федерации;

- о состоянии здоровья высших должностных лиц Российской Федерации;

- о фактах нарушения законности органами государственной власти и их должностными лицами.

Нормативные документы о безопасности КИИ

Федеральное законодательство

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности КИИ РФ»
- Федеральный закон от 26.07.2017 года № 193-ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»
- Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

Подзаконные нормативные акты

Указы Президента РФ

- Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины ИБ РФ»
- Указ Президента РФ от 25.11.2017 № 569 «О внесении изменений в Положение о ФСТЭК»
- Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании ГосСОПКА»

Подзаконные нормативные акты

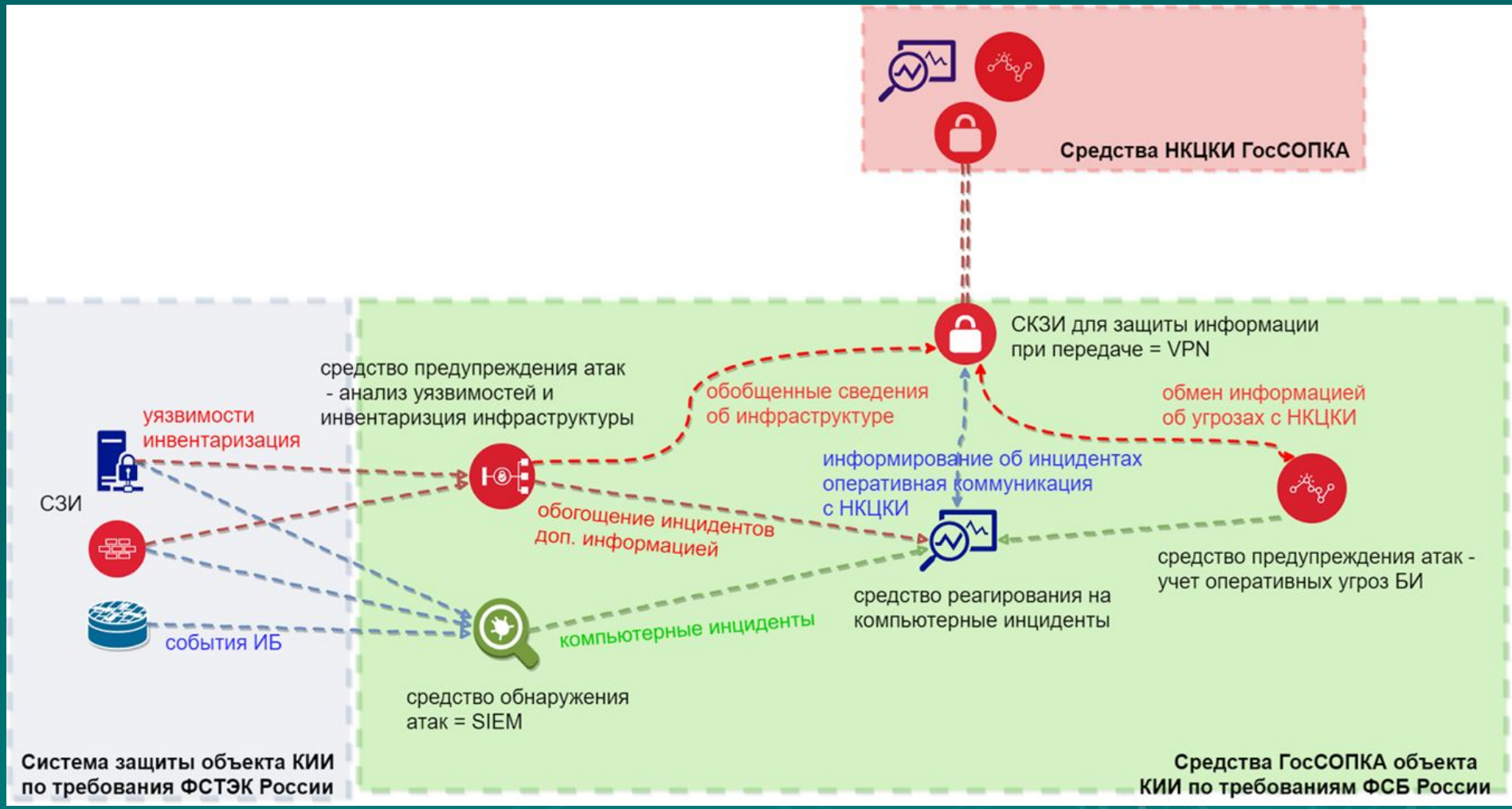
Постановления Правительства РФ

- Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
- Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»
- Постановление Правительства РФ №743 от 08.06.2019 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ»

Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

Под **критической информационной инфраструктурой** РФ (КИИ) подразумевается совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов РФ и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, а также ИТ-систем и сетей связи, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка.


Субъекты КИИ
Гос. органы
Гос. учреждения
Юридические лица
ИП
Которым принадлежат
Которые обеспечивают взаимодействие
Информационные системы
Информационно-телекоммуникационные сети
Автоматизированные Системы Управления
Работающие в отраслях
Объекты КИИ
ПРОМЫШЛЕННОСТЬ
Оборонная
Ракетно-космическая
Горно-добывающая
Металлургическая
Химическая
Энергетика
Атомная энергетика
ТЭК
Связь
Банки
Финансовая сфера
Наука
Транспорт
Здравохранение


Средства НКЦКИ ГосСОПКА
СКЗИ для защиты информации
при передаче = VPN
средство предупреждения атак
- анализ уязвимостей и
инвентаризция инфраструктуры
обобщенные сведения
об инфраструктуре
обмен информацией
об угрозах с НКЦКИ
уязвимости
инвентаризация
СЗИ
информирование об инцидентах
оперативная коммуникация
с НКЦКИ
обогощение инцидентов
доп. информацией
средство предупреждения атак -
учет оперативных угроз БИ
средство реагирования на
компьютерные инциденты
события ИБ
компьютерные инциденты
средство обнаружения
атак = SIEM
Система защиты объекта КИИ
по требования ФСТЭК России
Средства ГосСОПКА объекта
КИИ по требованиям ФСБ России

Указ Президента Российской Федерации от 22.12.2017 № 620 "О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации“ (ГосСОПКА)

2. Установить, что задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации являются:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Другие федеральные законы

- Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 27.12.2018) "О связи"
- Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) "О персональных данных"
- Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи“

Технологии обеспечения информационной безопасности

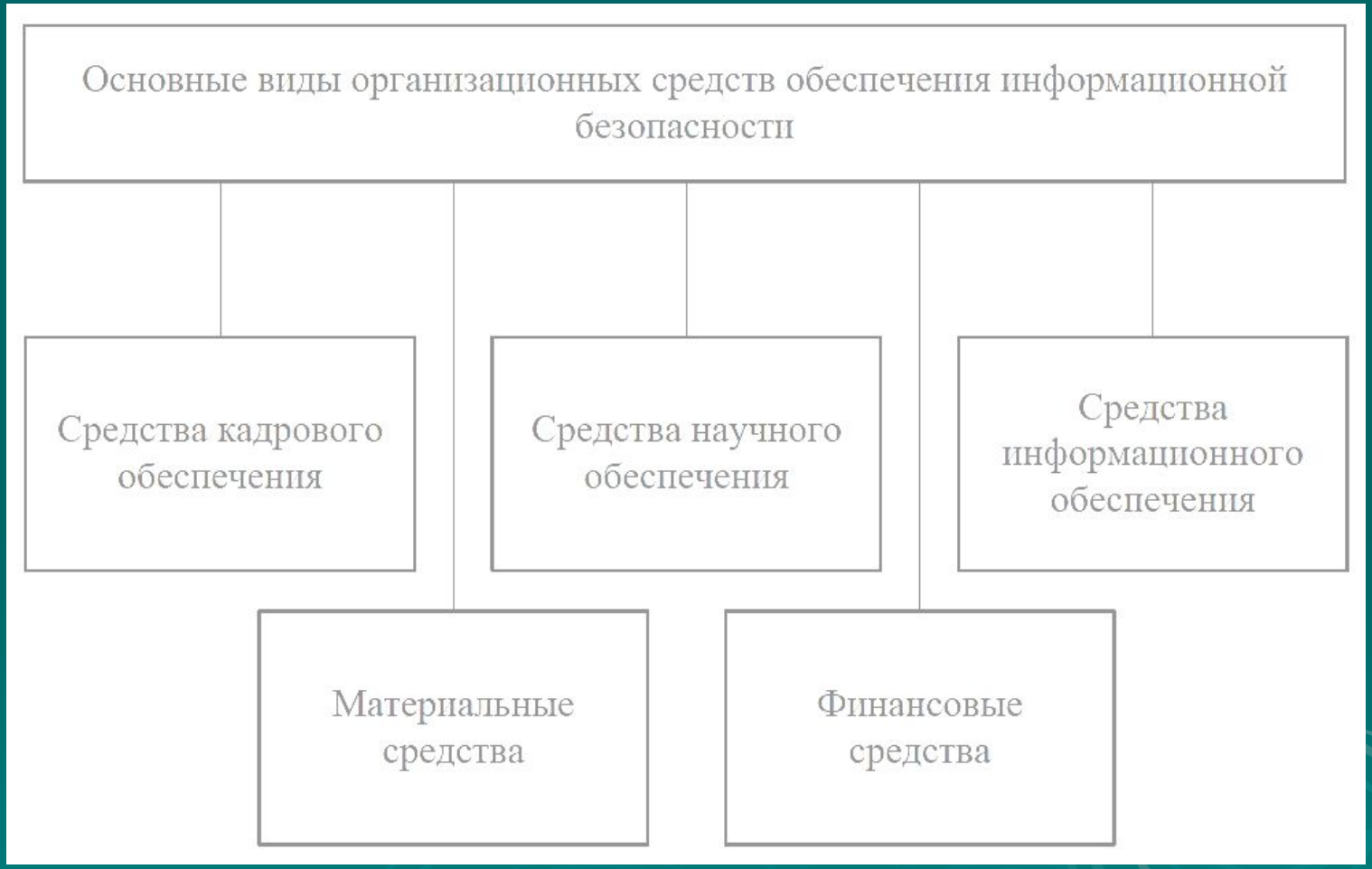
Общая схема обеспечения информационной безопасности

Структура понятия «обеспечение информационной безопасности»

- Таким образом, **обеспечение информационной безопасности** есть совокупность деятельности по недопущению вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности.
- ***Деятельность по обеспечению информационной безопасности*** - комплекс планируемых и проводимых в целях защиты информационных ресурсов мероприятий, направленных на ликвидацию угроз информационной безопасности и минимизацию возможного ущерба, который может быть нанесен объекту безопасности вследствие их реализации.

- Под **субъектами обеспечения информационной безопасности** понимаются государственные органы, предприятия, должностные лица, структурные подразделения, принимающие непосредственное участие в организации и проведении мероприятий по обеспечению информационной безопасности.
- ***Средства, с помощью которых достигаются цели деятельности по обеспечению информационной безопасности***, - это системы, объекты, способы, методы и иные механизмы непосредственного решения задач обеспечения информационной безопасности. Прежде всего, они представляют собой совокупность правовых и организационных средств обеспечения информационной безопасности.

Основные виды организационных средств обеспечения информационной безопасности



Основные направления защиты информации

Основные направления организационной защиты информации

Основные принципы организационной защиты информации

- Принцип комплексного подхода заключается в использовании сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факто-ров, ослабляющих или усиливающих угрозу возможной утечки конфиденциальной информации.
- Принцип оперативности принятия управленческих решений существенно влияет на эффективность функционирования и гибкость системы защиты ин-формации и отражает целеустремленность должностных лиц на решение задач защиты информации.
- Принцип персональной ответственности заключается в наиболее эффективном и полном распределении сил структурных подразделений предприятия, участвующих в процессе защиты информации.

Структура системы защиты информации

Система защиты информации должна отвечать совокупности следующих основных требований, то есть быть:

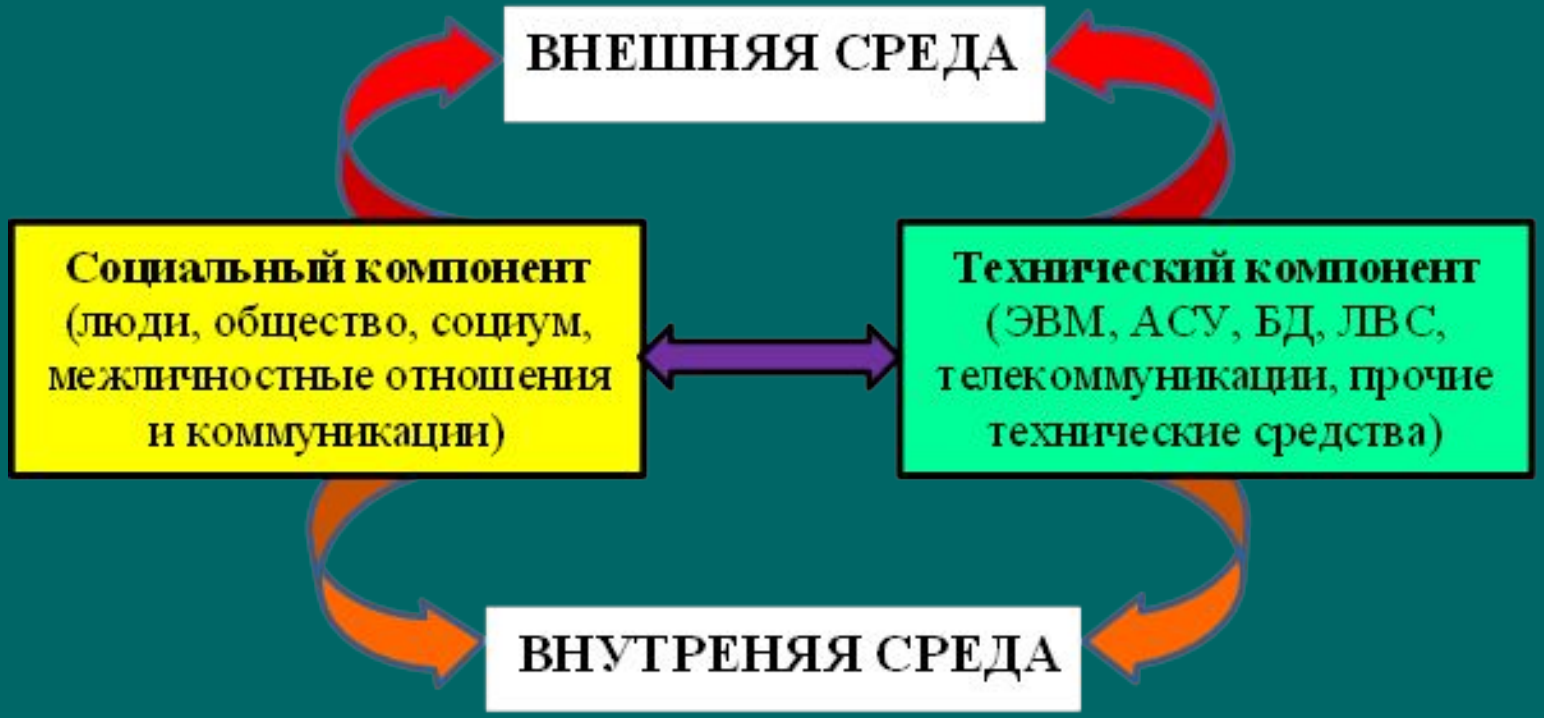
- ***централизованной*** - соответствующей эффективному процессу управления системой со стороны руководителя и ответственных должностных лиц по направлениям деятельности предприятия;
- ***плановой*** - объединяющей усилия различных должностных лиц и структурных подразделений при их участии в организации и обеспечении выполнения задач, стоящих перед предприятием;
- ***конкретной и целенаправленной*** - защите должны подлежать абсолютно конкретные информационные ресурсы, представляющие интерес для конкурирующих организаций;
- ***активной*** - обеспечивать защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;
- ***надежной и универсальной*** - охватывать весь комплекс деятельности предприятия, связанной с созданием и обменом информацией.

Структура перечня сведений, составляющих государственную тайну

Раздел 4.

Методы и средства обеспечения информационной безопасности социотехнических систем

Состав социотехнической системы



Социотехническая информационная система (СТИС) – совокупность информационно-технической и социальной инфраструктур ИС. Социотехнической является любая ИС, где социальная инфраструктура, то есть «человеческий фактор», оказывает непосредственное влияние на эффективность использования компьютерной техники. Человеческий фактор также затрагивает стадии функционирования всей ИС, такие как проектирование, разработка, внедрение, эксплуатация.

Система специального информационного обеспечения органов государственной власти

НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

по реализации комплексной безопасности социальных ресурсов Интернет

Социальные сети и «цветные технологии»

Задачи

Разработка систем обнаружения ... (СОА) в СС

Разработка техно... противодействия... эпи...

...а технологий ...и ресурсов ...ей

Систем... осведомл... технологий ...

...ользования ...чения ...ю-

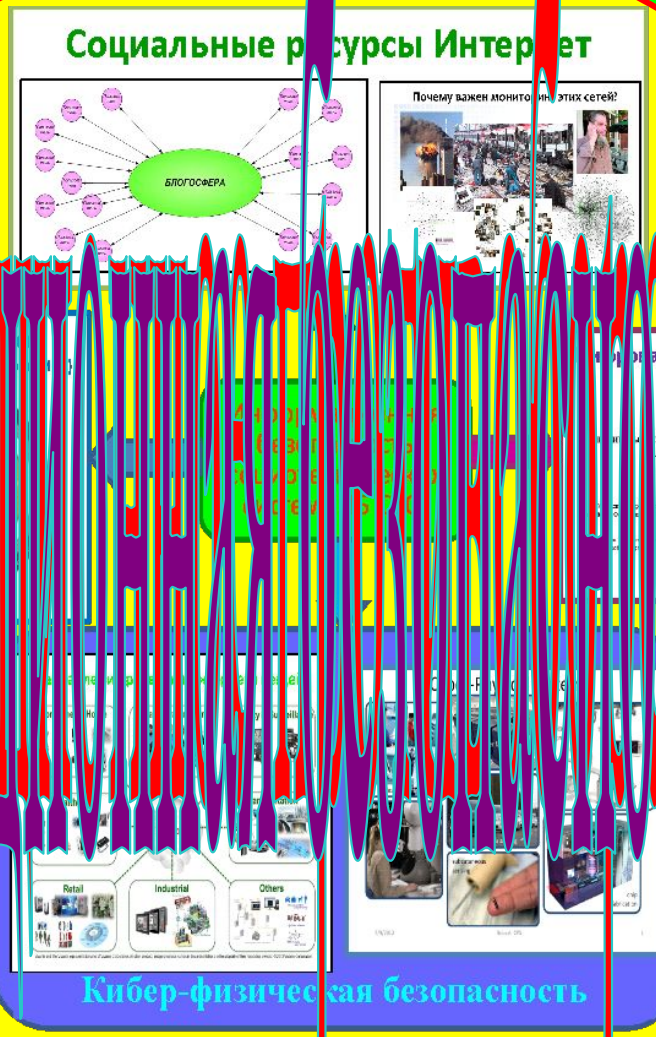
...гий ...доступа

...имизации СС, ...ии стеганографии ...OR, I2P и др.)

...многоуровневой ...противо... контента терро... в откры...

Защищенные технологии виртуализации и облачные вычисления

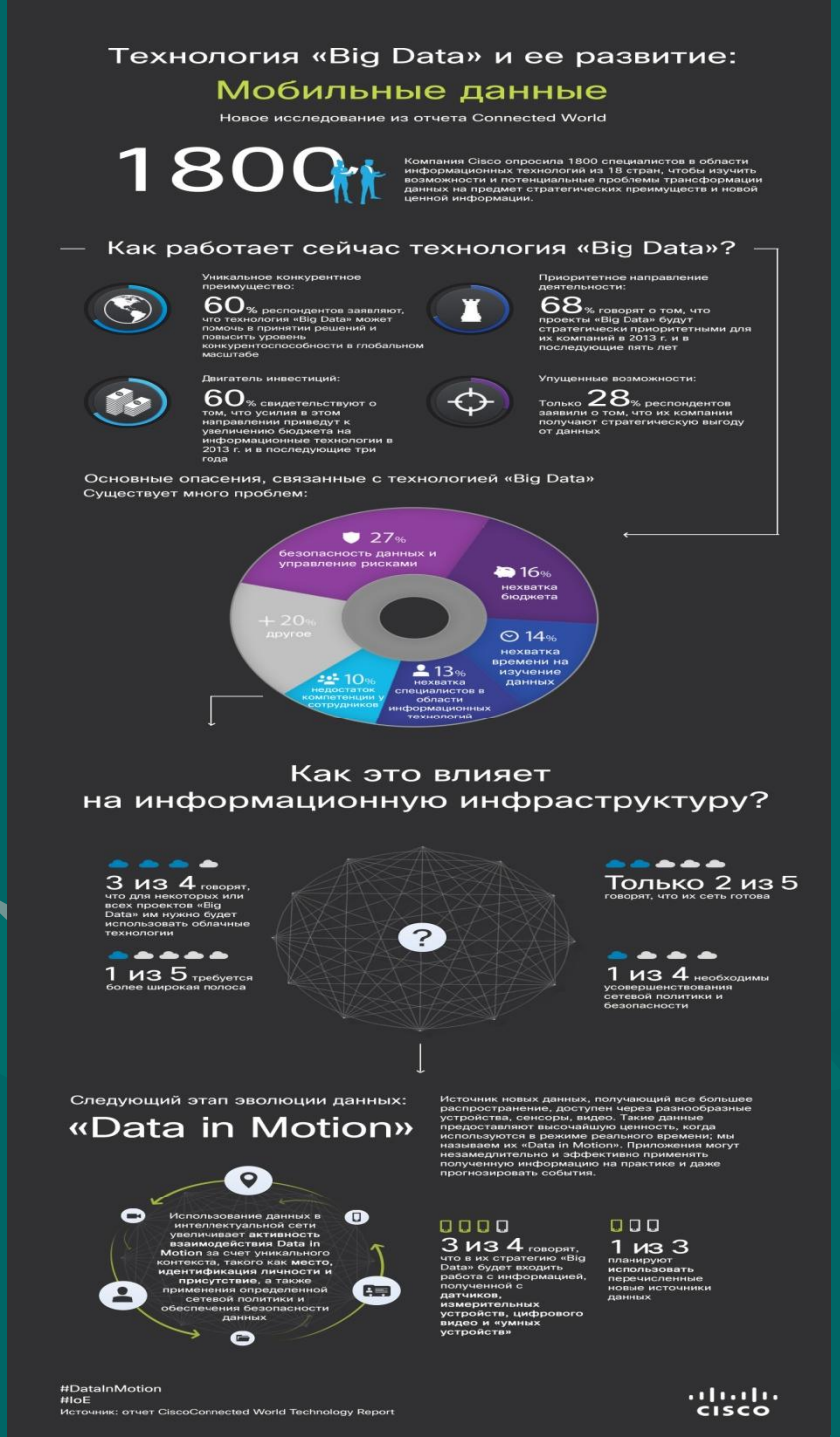
Интернет-зависимость как социальная проблема в сети

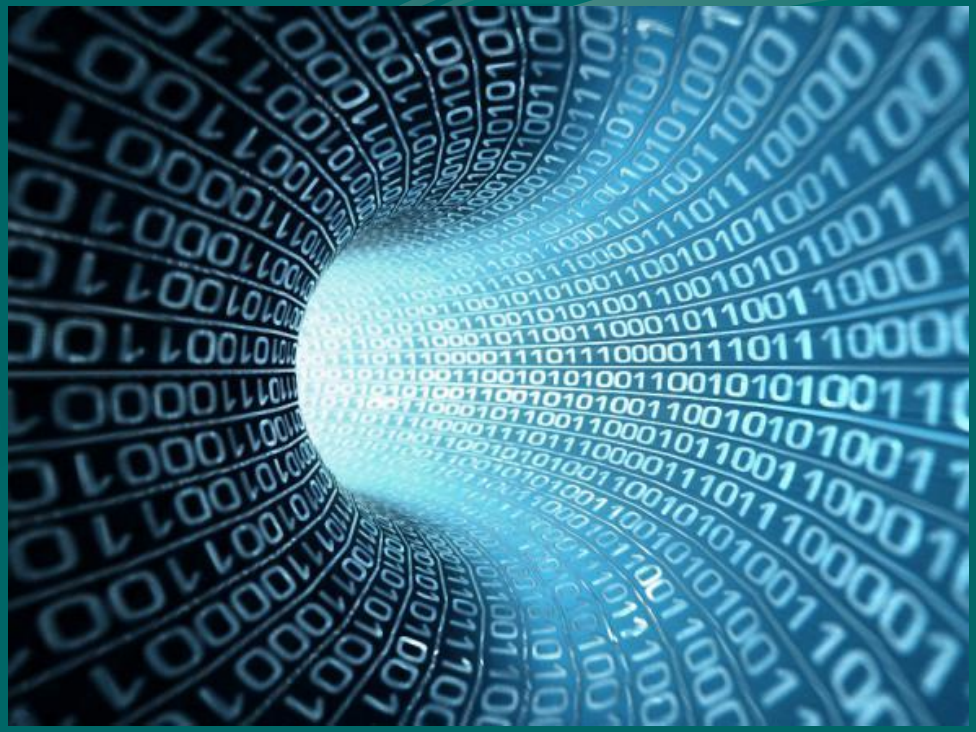


Обеспечение безопасности в информационно-психологической сфере социотехнических систем

Свобода СМИ, право граждан на получение и распространение информации – это базовые принципы любой демократической власти, любого демократического государства и общества. Их необходимо неукоснительно соблюдать, и мы будем делать именно это. Еще раз хочу подчеркнуть: никаких необоснованных ограничений, тотальных тем более, не только не будет – мы даже этого не рассматриваем.

Технология «Big Data»: ее развитие и ожидания бизнес-сообщества





Вступление в эпоху больших данных (Big Data)

(Из выступления Директора по технологиям ЦРУ Айра Гас Хант (Ira Gus Hunt) о своем видении Big Data на службе ЦРУ, а также возникающих при этом задачах и методах их решения. (конференция GigaOM Structure:Data 2013, 20 марта 2013 г., Нью-Йорк).

Эпоха коренных перемен

Типы ресурсов в формате Web 2.0

- Социальные закладки (social bookmarking) - создают список закладок или популярных веб-сайтов. Используются для поиска пользователей с общими интересами (Delicious).
- Социальные каталоги (social cataloging) ориентированы на научную сферу для работы с базами данных, цитатами из научных статей. (Academic Search Premier, LexisNexis, Academic University, CiteULike, Connotea).
- Социальные библиотеки - ссылки на их книги, аудиозаписи и т. п. с системой рейтингов и т. п. (discogs.com, IMDb.com).
- Соцсети вебмастеров - ссылки на их посты, общение и т. п. Часто имеют рейтинги или рекомендации.
- Многопользовательские сетевые игры (Massively Multiplayer Online Games) имитируют виртуальные миры с различными системами победителей и проигравших (World of Warcraft).
- Геосоциальные сети - геолокации, например GPS, для определения местоположение пользователя, а также создавать профайлы мест, где они сейчас находятся
- Профессиональные соцсети для поиска работы, развития деловых связей (Доктор на работе, Профессионалы.ру, LinkedIn,

Базовые понятия и термины

- ***Социальная сеть*** от англ. *social networking service*) — платформа, онлайн-сервис, предназначенные для построения, отражения и организации социальных взаимоотношений.

- С Web 2.0 социальные сети стали порталами и веб-сервисами.

- Соцсети стартовали в 1995 году с портала в США Classmates.com («Одноклассники» - его русский аналог). Проект оказался успешным и стал началом бума социальных сетей в 2003 - 2004 годы, когда были запущены LinkedIn (для деловых контактов), MySpace и Facebook (**для человеческой потребности в самовыражении**).

- **В соответствии с «пирамидой Маслоу», именно самовыражение является высшей потребностью человека**

Иерархия потребностей по Maslow

Самореализация

Эстетические

Когнитивные

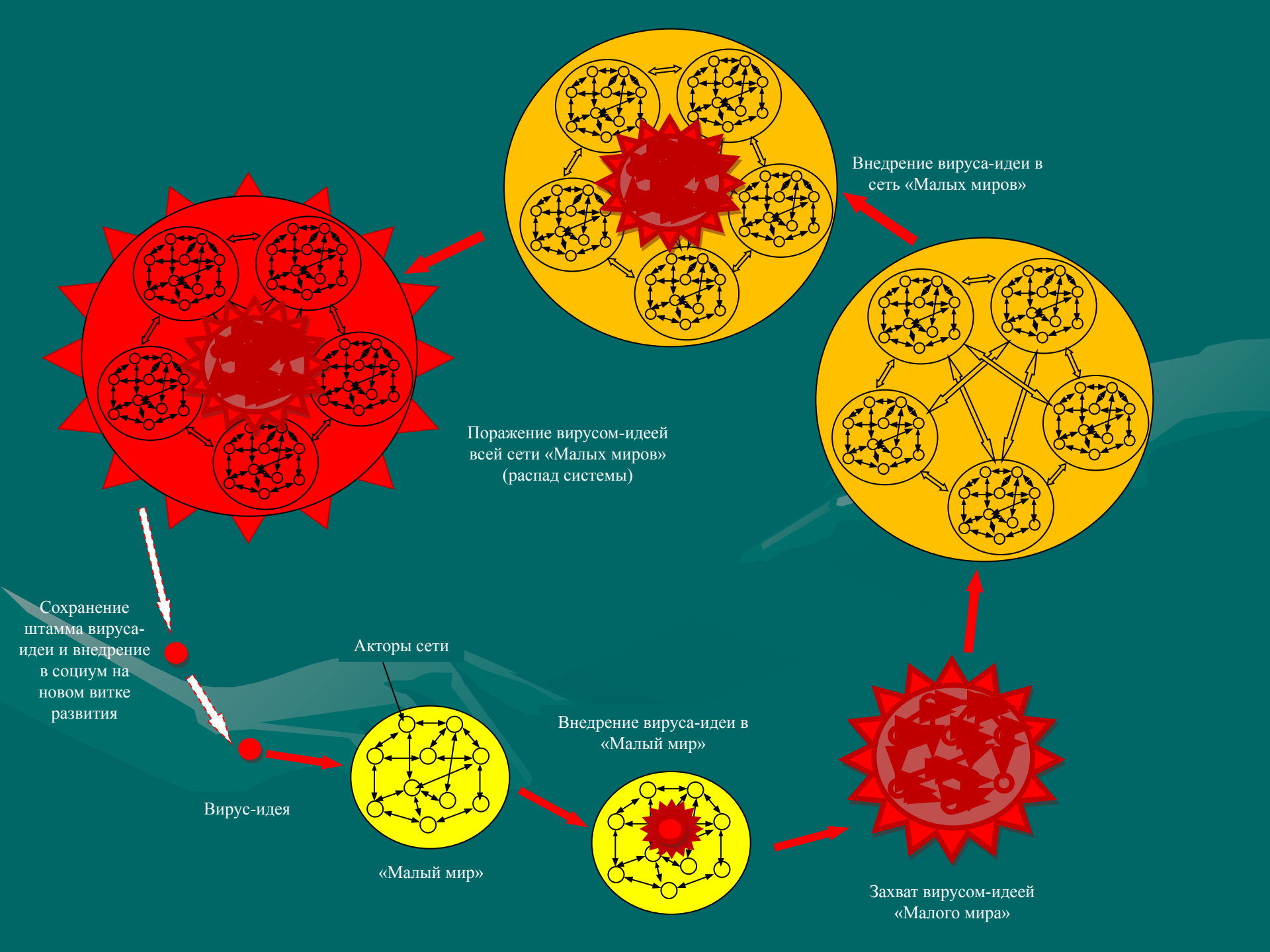
Оценка себя

Имущество

Здоровье

Потребности Роста

Потребности защиты


Внедрение вируса-идеи в сеть «Малых миров»
Поражение вирусом-идеей всей сети «Малых миров» (распад системы)
Сохранение штамма вируса-идеи и внедрение в социум на новом витке развития
Акторы сети
Вирус-идея
«Малый мир»
Внедрение вируса-идеи в «Малый мир»
Захват вирусом-идеей «Малого мира»

Использование специального ПО для возбуждения сети

Практические действия США по управлению социальными ресурсами Интернет в своих геополитических целях

Broad Agency Announcement

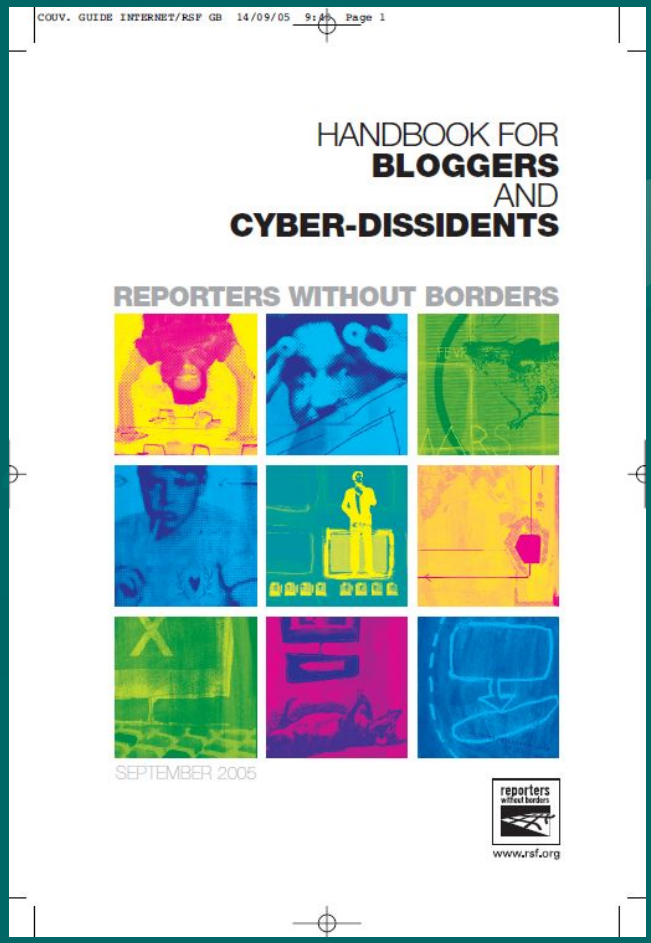
Social Media in Strategic Communication (SMISC)

DARPA-BAA-11-64

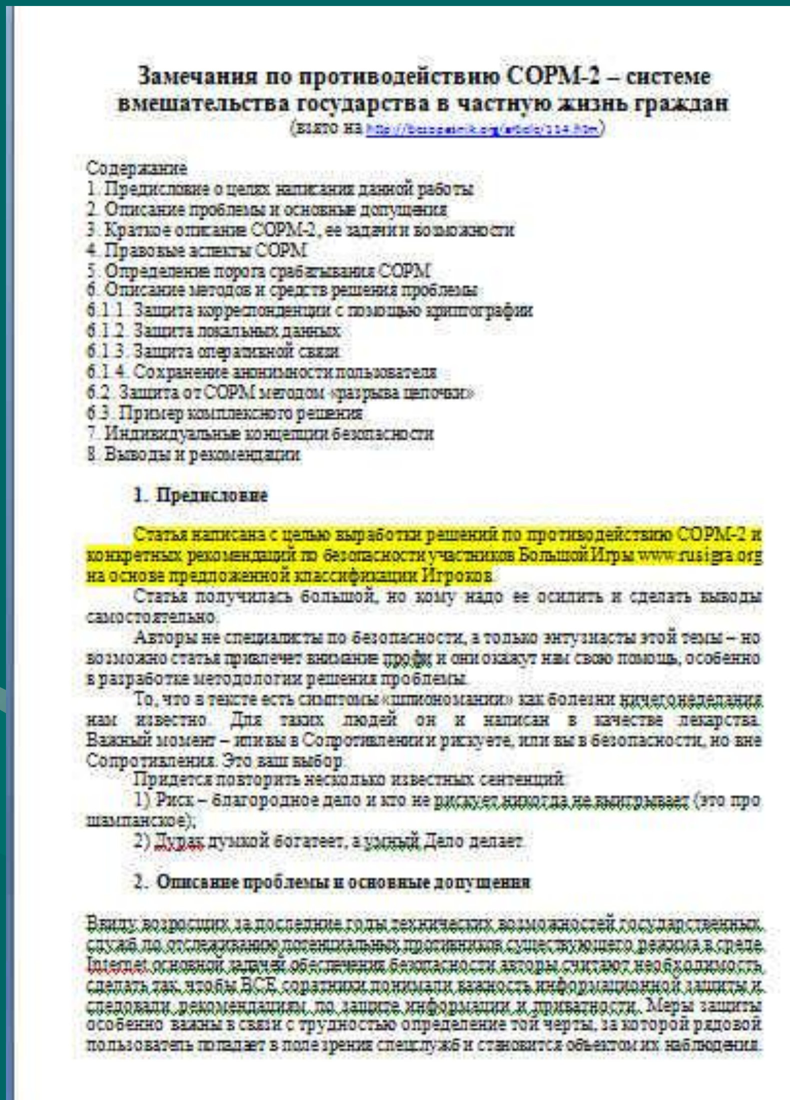
July 14, 2011

DARPA

Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington, VA 22203-1714



Инструкция «социальным бойцам» по противодействию СОРМ-2



Замечания по противодействию СОРМ-2 – системе вмешательства государства в частную жизнь граждан

(взято на http://bezopasnik.org/article/114.htm)

Содержание

1. Предисловие

Статья написана с целью выработки решений по противодействию СОРМ-2 и конкретных рекомендаций по безопасности участников Большой Игры www.rusigra.org на основе предложенной классификации Игроков.

Статья получилась большой, но кому надо ее осилить и сделать выводы самостоятельно.

Авторы не специалисты по безопасности, а только энтузиасты этой темы – но возможно статья привлечет внимание профи и они окажут нам свою помощь, особенно в разработке методологии решения проблемы.

То, что в тексте есть симптомы «шпиономании» как болезни ничегонеделания нам известно. Для таких людей он и написан в качестве лекарства. Важный момент – или вы в Сопротивлении и рискуете, или вы в безопасности, но вне Сопротивления. Это ваш выбор.

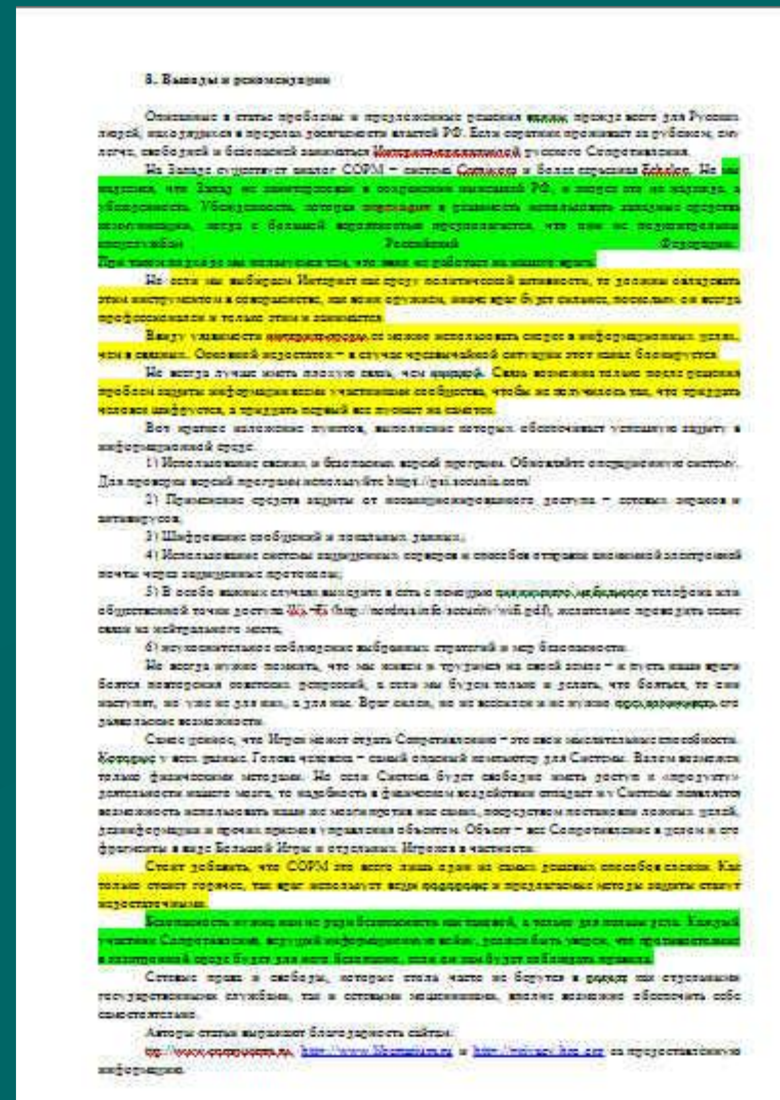
Придется повторить несколько известных сентенций:

1) Риск – благородное дело и кто не рискует никогда не выигрывает (это про шампанское);

2) Дурак думкой богатеет, а умный Дело делает.

2. Описание проблемы и основные допущения

Ввиду возросших за последние годы технических возможностей государственных служб по отслеживанию потенциальных противников существующего режима в среде Internet основной задачей обеспечения безопасности авторы считают необходимость сделать так, чтобы ВСЕ соратники понимали важность информационной защиты и следовали рекомендациям по защите информации и приватности. Меры защиты особенно важны в связи с трудностью определение той черты, за которой рядовой пользователь попадает в поле зрения спецслужб и становится объектом их наблюдения.



Организация тотальной слежки американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру, при помощи существующих информационных сетей и сетей связи (включая проект PRISM, а

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

TOP SECRET//SI//ORCON//NOFORN

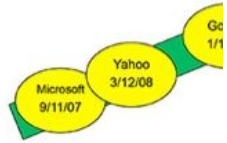
(TS//SI//NF) PRISM Collection Details

Current Providers

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice

- Microsoft (Hotmail, etc.)



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

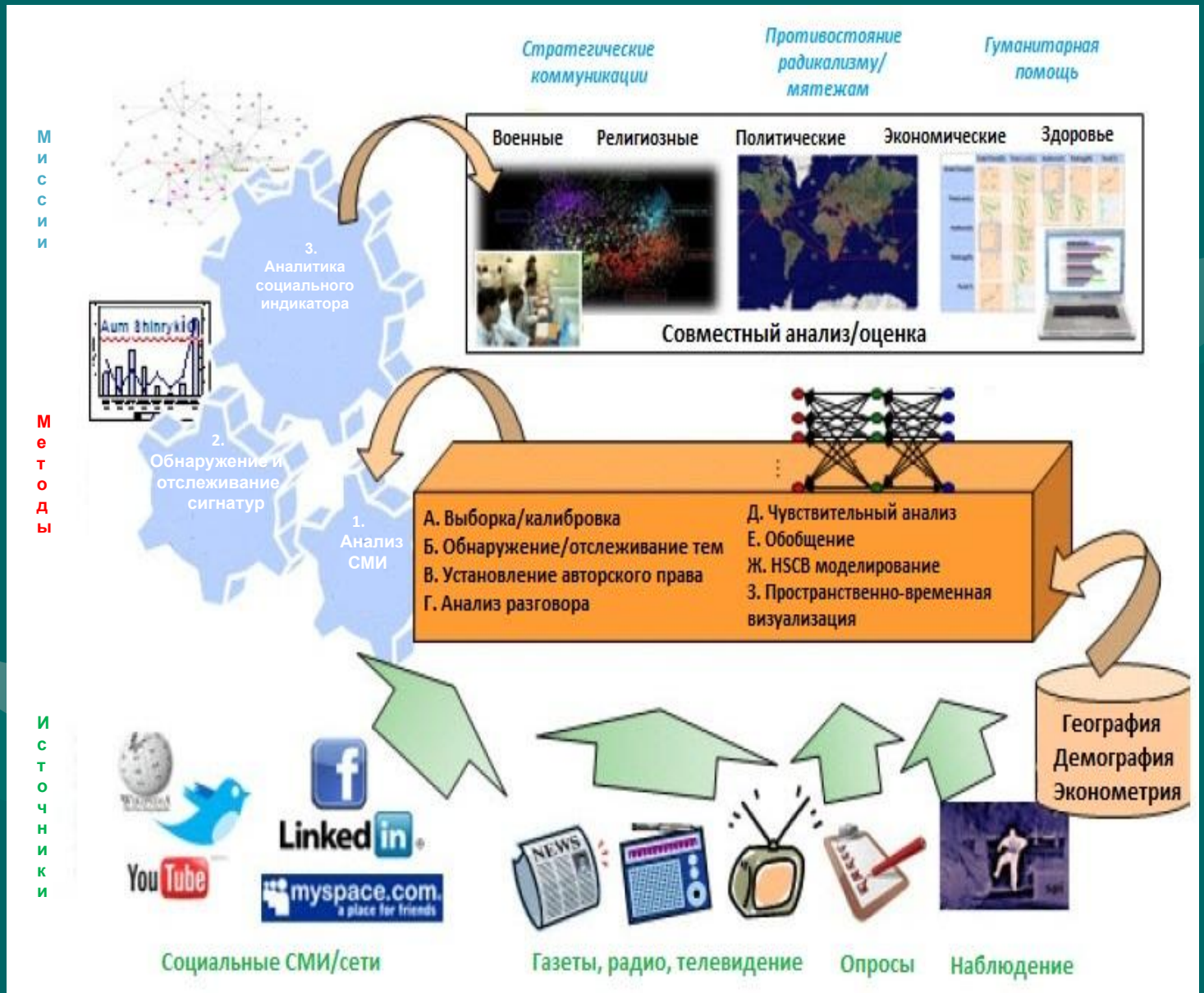
You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN

Архитектура социального радара



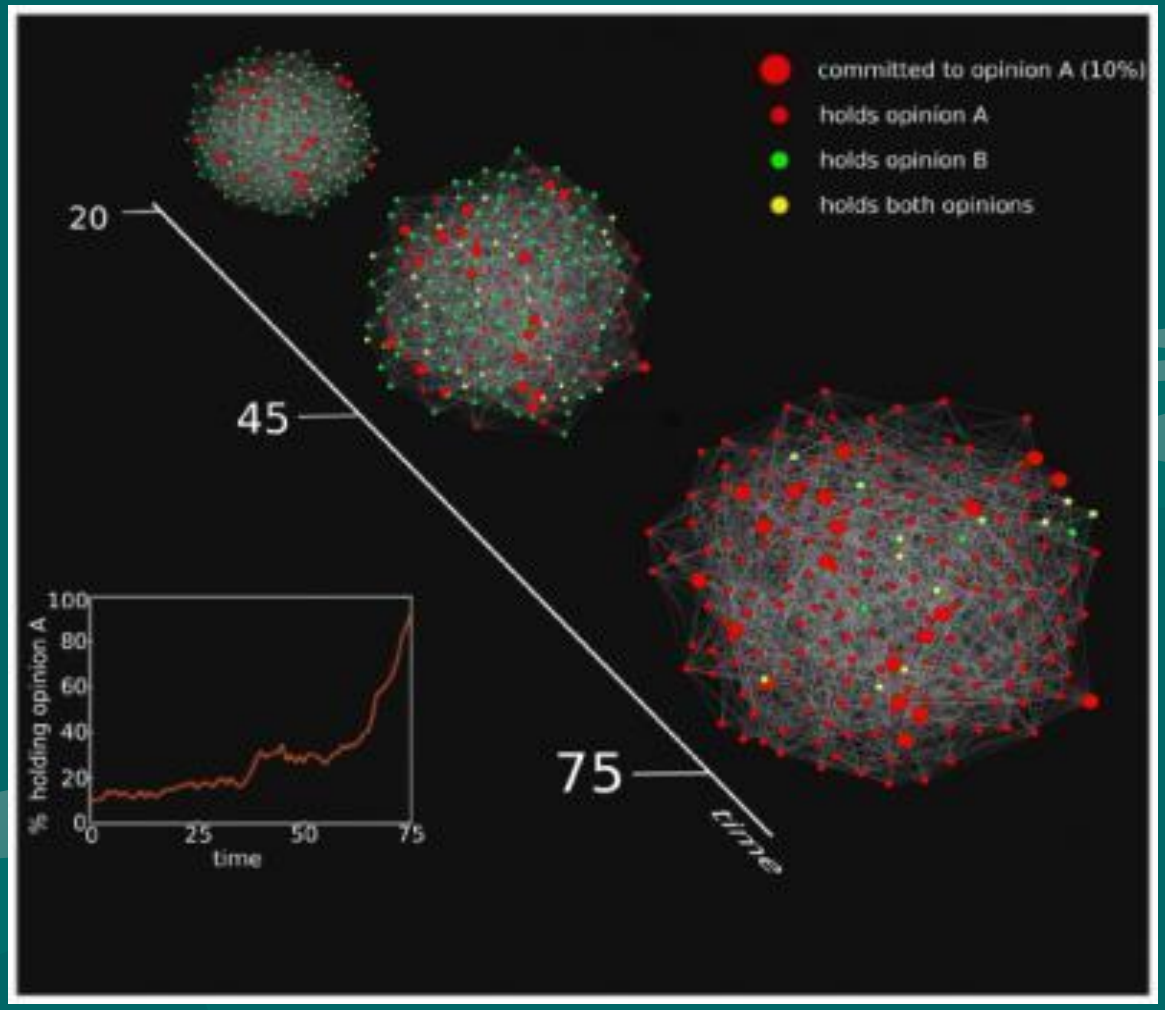
Задача: создать систему, которая позволит видеть то, что происходит в сердцах и умах людей»

- Такая система позволит получать слабые сигналы о только начинающихся процессах, распознавать зерна будущих конфликтов, определять тенденции, пока они еще не превратились в очевидные тренды. Создание системы стало возможным, благодаря ряду обстоятельств:
- во-первых, насыщению информационного пространства web1 структурированной и неструктурированной информацией, созданию программных продуктов, обеспечивающих эффективный поиск, мониторинг, кластеризацию и агрегацию структурированной и неструктурированной информации из видимого и невидимого web1;
- во-вторых, созданию гиперсоциальной сети web2, включающей в себя транснациональные сети типа Facebook, LinkedIn и т.п., а также различного рода национальные сети, повсеместному распространению платформы Twitter и соответствующих средств мониторинга гиперсети, извлечения, агрегации и многоконтурной обработки полученной из нее информации;

- в-третьих, экспоненциальному росту аудио и видео контента в сети, происходящему в первую очередь за счет контента, поступающего с различного рода мобильных устройств, ставших доступными для широких масс не только в развитых, но и развивающихся государствах, и даже самых отсталых странах;
- в-четвертых, опережающему росту в интернете данных, полученных от различного рода устройств, подключенных к интернету, начиная от видеокамер, установленных во все большем числе точек все большего числа населенных пунктов мира и кончая так называемыми «умными» домами, подключению к интернету не только телевизоров, но и другой бытовой техники. Вместе с привязкой практически всех программ и социальных сетей к геолокации это позволяет в режиме реального времени получать картину событий, относящихся не только к определенным группам и территориям, но даже отдельным людям и местам;

- в-пятых, переход на цифру всех печатных СМИ, а также процесс оцифровки всех ранее изданных книг, журналов, газет и т.п.
- в-шестых, дальнейшему развитию систем, типа «Эшелон», позволяющих вести тотальный мониторинг всех телекоммуникационных систем мира.
- в-седьмых, созданию и практической отработке, в том числе в гражданской сфере систем, позволяющих агрегировать для анализа и синтеза структурированные и неструктурированные информационные потоки в любых форматах и из любых источников. Одним из примеров такой платформы является система Palantir.

Правило доминирования искусственным мнением меньшинства (порядка 10%) в механизмах управления общественным мнением



На этой картинке мы видим переломный момент, когда мнение меньшинства (показано красным цветом) быстро становится мнением большинства. С течением времени мнение меньшинства растет . Как только мнение меньшинства охватит 10 процентов населения, сеть быстро меняет свое состояние, поскольку мнение меньшинства начинает превалировать над изначальным мнением большинства (показано зеленым цветом)

(Credit: SCNARC / Rensselaer Polytechnic Institute)

Основные этапы разработки возможного воздействия на сложную социальную сеть в рамках «мягкой» модели («цветных революций») (по Дж. Шарпу)

- Выявление конфликтного потенциала различных социальных групп на основе противоречий в интересах.
- Выделение социальных групп, политических объединений, способных стать стихийным инициатором (проводником) волны протеста.
- На эту роль могут подходить «легко воспламеняемые» группы (например, молодежь). Поэтому на первый план здесь выходит анализ психологических особенностей групп или отдельных личностей (наиболее актуально в случае сравнительно малых масштабов сети – например, террористической организации).
- Комплексная подготовка выделенных групп к дальнейшим активным действиям, определение концентраторов в рамках групп (в случае социальных сетей речь идет о де-факто лидерах, активистах).

- Адаптация реальных целей в соответствии с мерой понимания выбранных групп и их концентраторов (возможно, навязывание ложных целей). Они должны быть уверены в практической осуществимости поставленных задач.
- Обеспечение информационного превосходства навязываемых идей (использование СМИ, социальных ресурсов Интернет, вбрасывание информации в целевую среду и т.д.).
- Дальнейшее расширение контингента активных участников операции за счет обострения конфликтной ситуации (повышение «градуса озлобления» на действия правоохранитель-ных органов,«вербовка» новых «несогласных» элементов, повышение активности старых).
- Оказание воздействий на систему защиты целевой сети с целью сокращения ее возможностей и, в идеале, полного блокирования.
- Перевод целевой системы в бифуркационное состояние с возможным влиянием на ход ее дальнейшего развития.
- После перехода системы в новое состояние (выгодное инициатору воздействий) ранее подогреваемые конфликты сводятся на нет, в том числе, с помощью «непопулярных» мер.

Таблица 1. Упрощённый алгоритм «классической» революции

Фаза	Содержание
«Подготовка»	Масштабная пропагандистская кампания манипуляции общественным мнением и террора с целью дискредитации, демора-лизации и делигитимизации действующей власти, доказательства ущербности государства; вербовка и обучение.
«Осуществление»	Организованный всплеск насилия, взрыв массовой активности, энтузиазма и воодушевления; культивирование чувства сопричастности, могущества, силы, надежды и смысла жизни массы, трансформированной в манипулируемую толпу и свергающую действующую власть.
«Изменения»	Радикальные, фундаментальные, эпохаль-ные быстрые изменения во всех сферах общества, коренная трансформация ценностей, мифов, символов и верований, смена элит и характера политического лидерства, перераспределение статуса и богатства.

Таблица 2. Сценарии «цветных революций»

Условное обозначение	Содержание	Характерный пример, год
«Выборы»	Переворот, приуроченный к выборам, инициирование кризиса легитимности власти.	Грузия (2003); Украина (2004); Молдова (2009); Беларусь (2006, 2010).
«Штурм»	Насилие, штурм «цитадели режима».	Азербайджан (2003); Киргизия (2005, 2010); . Украина (2013).
«Заговор»	Заговор части правящей элиты в отношении лидера.	Азербайджан (2005).
«Марш периферии»	Экспорт революции из периферии в столицу, возможно культивирование этнических конфликтов.	Киргизия (2005, 2010); Узбекистан (2005).

Информационная безопасность и «цифровая экономика»

Национальная программа «Цифровая экономика Российской Федерации»

В рамках реализации Указа Президента Российской Федерации от 7 мая 2018 г № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», в том числе с целью решения задачи по обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством Российской Федерации на базе программы «Цифровая экономика Российской Федерации» сформирована национальная программа «Цифровая экономика Российской Федерации» утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

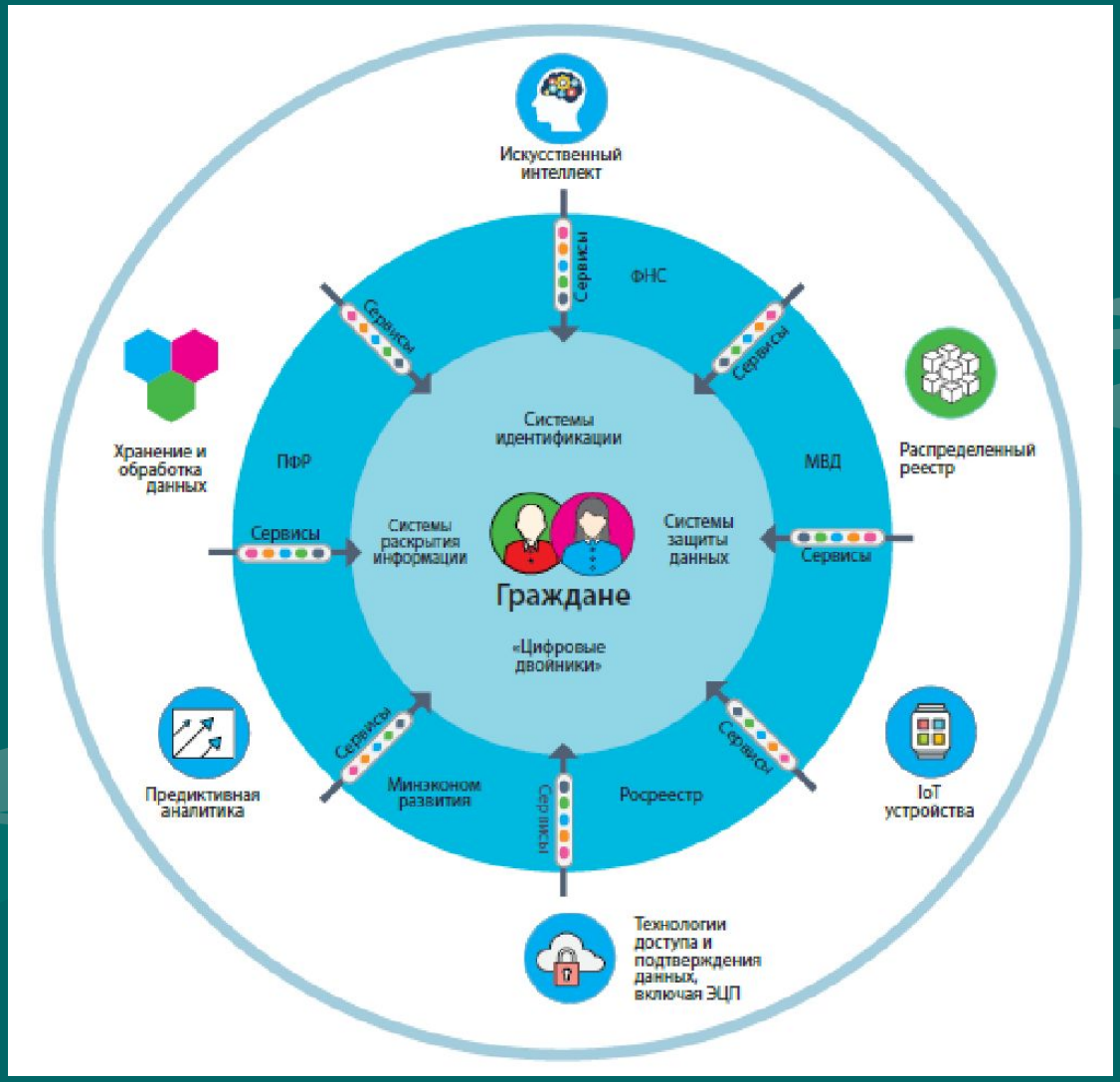
В состав Национальной программы «Цифровая экономика Российской Федерации» входят следующие федеральные проекты, утвержденные протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28 мая 2019 г. № 9:

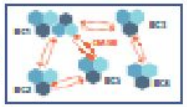
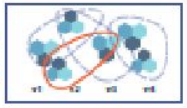
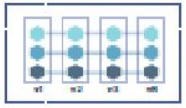
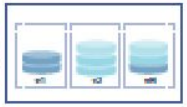
- «Нормативное регулирование цифровой среды»
- «Кадры для цифровой экономики»
- «Информационная инфраструктура»
- «Информационная безопасность»
- «Цифровые технологии»
- «Цифровое государственное управление»

Создание национальной или наднациональной платформы управления «цифровой экономикой»?

Подходы к созданию цифровых платформ

Взаимодействие человека и ГкП



ЕСТЬ СЕЙЧАС		БУДЕТ	
Более 250 тысяч сайтов органов власти и государственных, муниципальных учреждений			Единая фронтальная система с омниканальностью (включая чат-бот)
Отдельные ведомственные системы, соединенные через СМЭВ			Экосистема микросервисов на едином массиве данных
Неструктурированные, разрозненные, ошибочные, противоречивые данные			Эталонные данные в единой метамодели, непрерывный процесс мониторинга качества данных
Самостоятельное управление ИТ в отдельных федеральных ведомствах. Независимые ИТ-бюджеты			Вице-премьер по цифровой трансформации. Главный ИТ-архитектор и CDO в каждом ведомстве, подчиненные вице-премьеру по цифровой трансформации
Отсутствуют единые правила и принципы создания государственных ИТ систем. Технологическое противоречие и отставание			Единые архитектурные принципы и единый современный, легко обновляемый стек технологий
Большая часть государственных услуг оказывается в неэлектронном виде			Перевод всех востребованных услуг в электронную форму
Межведомственные процессы реализуются долго и с колоссальными организационными и финансовыми затратами			Непрерывные, интегрированные, цифровые и быстро перестраиваемые процессы
Множественные (десятки тысяч) государственные информационные системы			Опора на ключевые общие информационные ресурсы (единицы). Максимальная «облачность» сервисов
Многочисленные системы идентификации, основанные на различных принципах			«Цифровые двойники», цифровой профиль и удобная цифровая подпись на основе единой системы идентификации
Физическая идентификация (необходимо физическое присутствие)			Удаленная биометрическая единая система идентификации
Пользователь самостоятельно «компонует» необходимые ему разрозненные услуги постфактум			Проактивное предоставление интегрированных услуг
Решения принимаются госслужащими, возможен человеческий фактор и возникновение коррупции			Большинство решений человеконезависимы – алгоритмизованы, автоматизированы и принимаются средствами искусственного интеллекта

Сценарии цифровизации государственного управления

Утопия?

Бета-версия уже существует

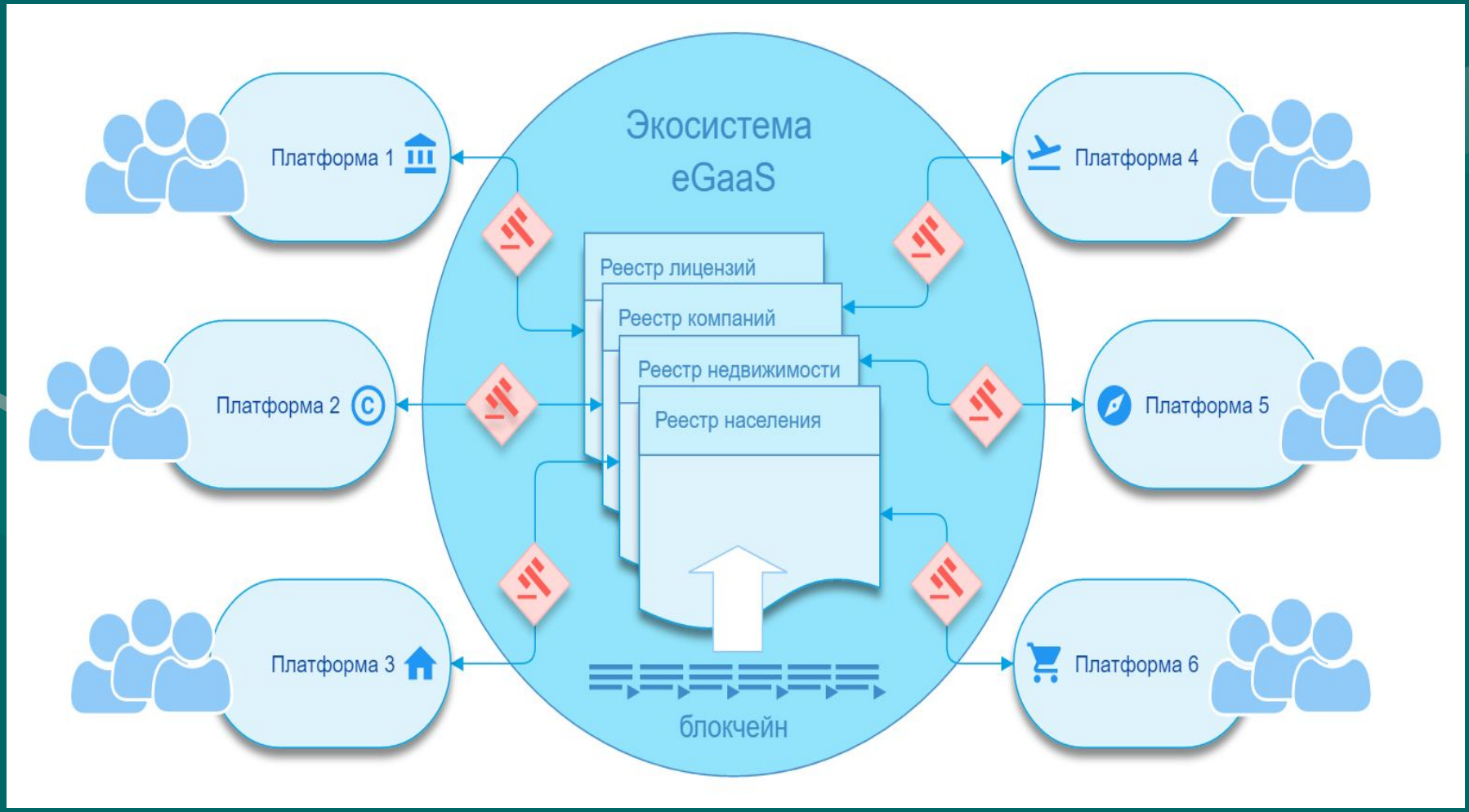
EGAAS
ELECTRONIC GOVERNMENT AS A SERVICE

Экономия в масштабах мира оценивается в 6.1 трлн. долл. США

Компьютеризация работы правительства и представительных органов: **решения для всех функций работы правительства**

- **Создает и поддерживает систему распределенных реестров:** организация финансовых систем
- Помогает организовать бизнес-отношения **на основании смарт-контрактов**
- **Обеспечивает честные выборы**
- Позволяет регулировать **все отношения между частными и юридическими лицами, а также государством на основании смарт-права**
- Автоматически **предотвращает незаконные операции и коррупцию**
- Предоставляет ЦБ **новые, более совершенные инструменты управления монетарной политикой**
- **Создает единый протокол финансового и правового взаимодействия** между государствами и международными бизнесами
- Удобный интерфейс, включая приложение для телефона, позволяющей проводить **самые разные операции** (обмен валюты, покупка/ продажа, регистрация недвижимости, голосование) **в одно касание**

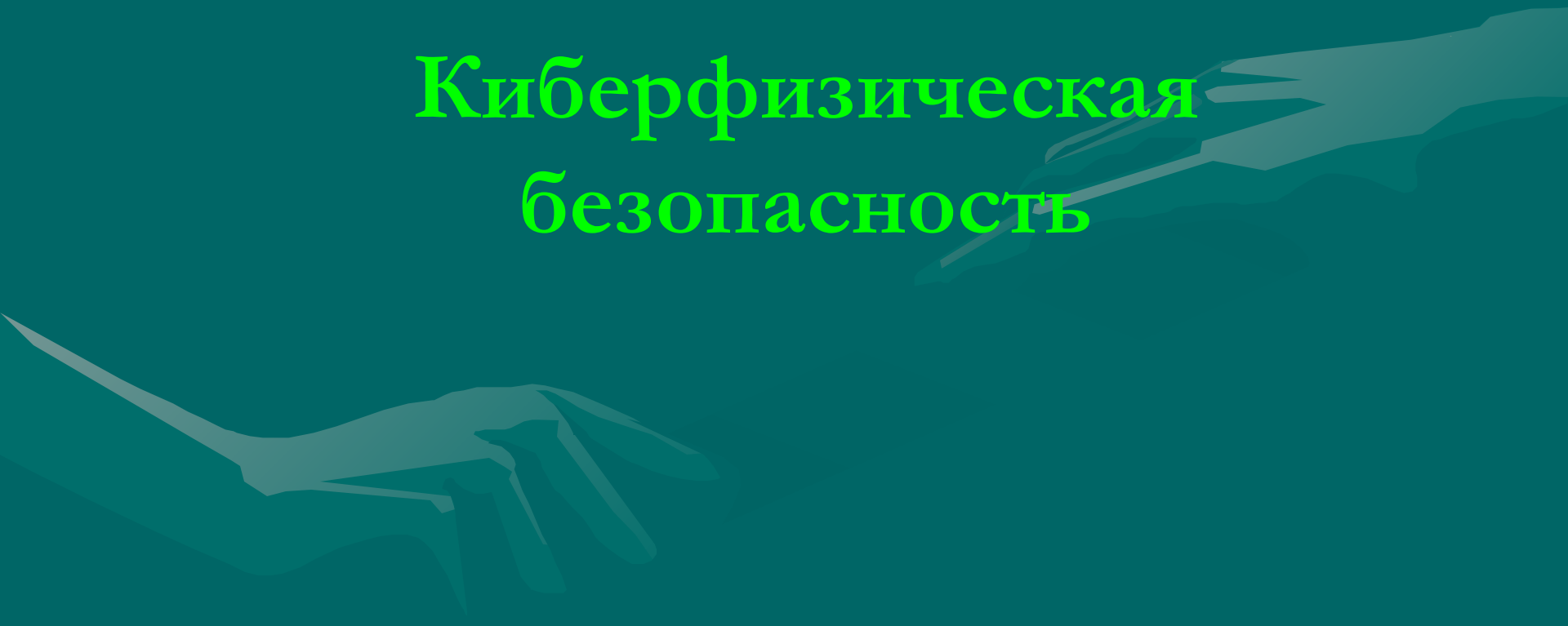
eGaaS (Electronic Government as a Service) — это цифровая экосистема, спроектированная для реализации идеи электронного правительства

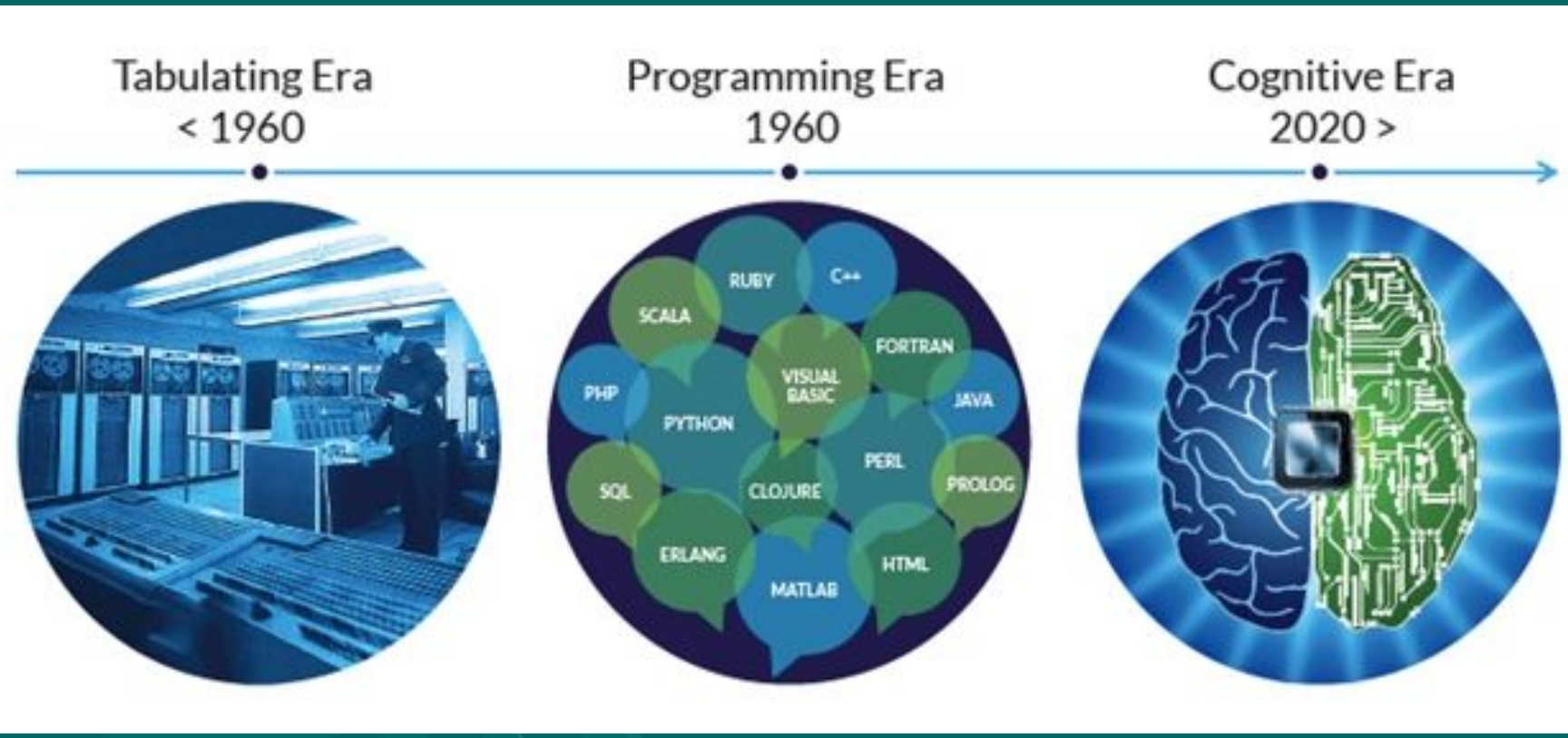


Уровни управления ОС

УРОВЕНЬ УПРАВЛЕНИЯ	ОБЪЕКТ УПРАВЛЕНИЯ	ИСПОЛЬЗУЕМАЯ ОПЕРАЦИОННАЯ СИСТЕМА	РЕЗУЛЬТАТ УПРАВЛЕНИЯ ОС	УГРОЗЫ
Микро	Отдельные ПЭВМ	ОС Windows (Microsoft)	1. Свыше 90 % используемых в госуправлении, бизнесе, промышленности, др. секторах а также в персональном поль-зовании ПЭВМ используют («сидят на игле») продукты Microsoft. 2. Сдерживание, а по большому счету, уничтожение отечественной отрасли сис-темного программирования. 3. Потеря внутреннего и внешних рынков для отечественного ПО. 4. Зависимость (полная привязка) к продуктовой линии Microsoft.	Применение программно-аппаратных вставок: • негласное считывание информации; • несанкционированное изменение процессов обработки, хранения и передачи информации; • несанкционированное изменение механизма управления процессами обработки, хранения и передачи информации; • несанкционированный доступ, изменение, уничтожение информации;
Макро	Экономика («в цифровой реализации») отдельного государства	EGAAS – наднацио-нальная *макрооперационная* платформа управления глобальной «цифровой экономикой» - макроинструментария трансграничного управления всеми национальными экономиками	1. Создание наднационального инструмента управления мировой торговлей, а, следовательно, мировой экономикой в новом цифровом формате. 2. Создание наднационального органа управления мировой торговлей, а, следовательно, мировой экономикой. 3. Создание мировой криптовалюты, эмитент которой будет находиться за рубежом. 4. Создание инструмента всемирного цифрового ЭКОНОМИЧЕСКОГО И ПОЛИТИЧЕСКОГО диктата.	1. Установление извне управления отечественной «цифровой экономикой». 2. Утеря приоритетов использования отечественных криптографических стандартов. 3. Потеря «цифрового суверенитета», а, следовательно, реального суверенитета. 4. Возможность «цифровых санкций» со стороны цифрового ВТО приведут к полной экономической, а, следовательно, политической изоляции России.

Киберфизическая безопасность




Tabulating Era
< 1960
Programming Era
1960
Cognitive Era
2020 >
RUBY
C++
SCALA
FORTRAN
VISUAL BASIC
PHP
JAVA
PYTHON
PERL
SQL
CLOJURE
PROLOG
ERLANG
HTML
MATLAB

ЧЕТВЕРТАЯ ПРОМЫШЛЕННАЯ РЕВОЛЮЦИЯ – INDUSTRY 4.0

- Перманентная информационная революция
- Промышленная компьютеризация
- Интеграция Internet-технологий с АСУ производства, энергетики, транспорта, медицины, банковской сферы, домашних устройств и систем безопасности

ПОНЯТИЕ КИБЕРФИЗИЧЕСКОГО ОБЪЕКТА (КФО)

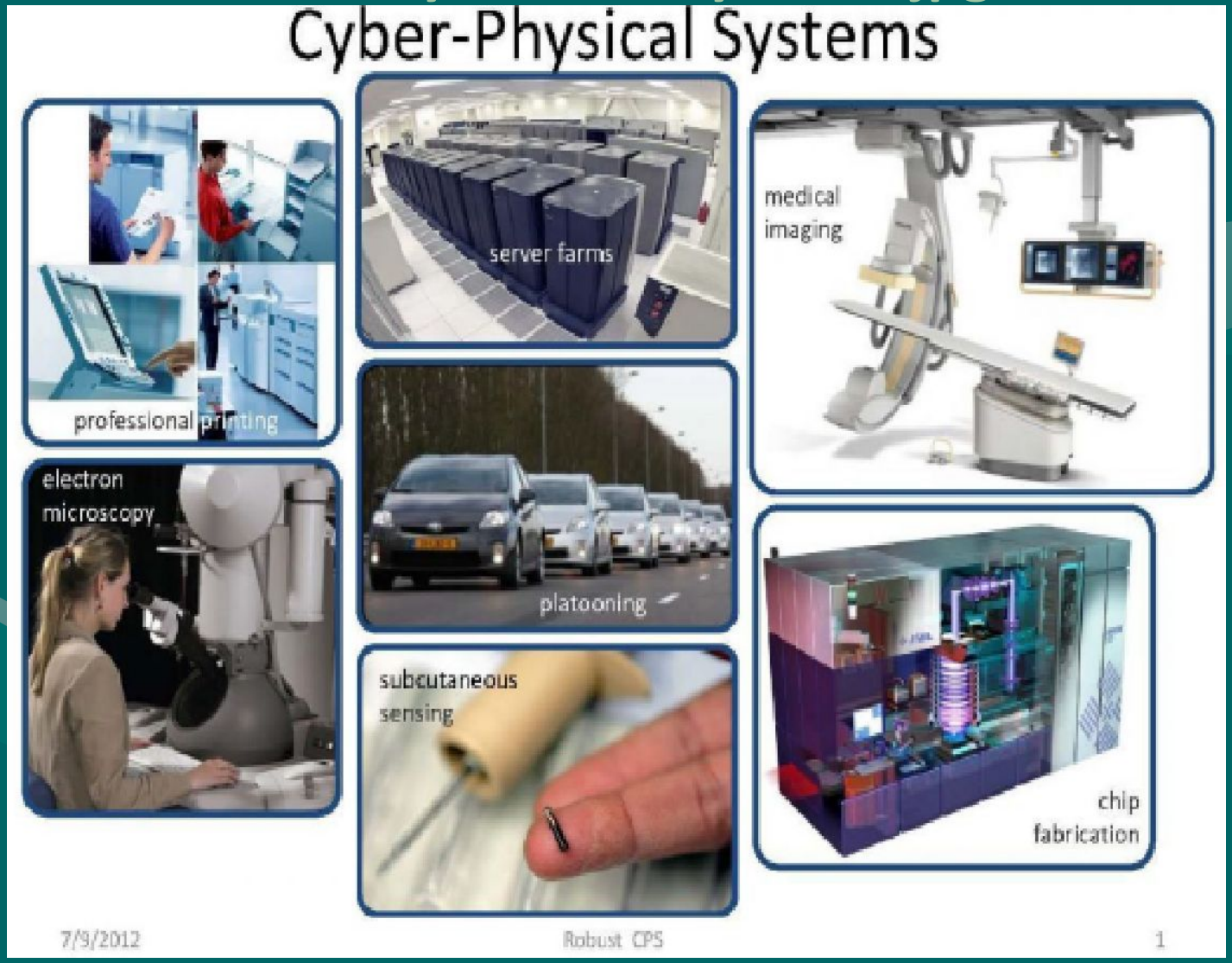
КФО – концептуальная парадигма представления производственных, технологических схем в виде конгломерата средств преобразования различных видов материи и энергии и информационно-телекоммуникационной среды, обеспечивающей как обмен информацией между компонентами так и устойчивое функционирование всей системы в условиях внешних воздействий с помощью автоматизированного управления.

К **КФО** можно отнести:

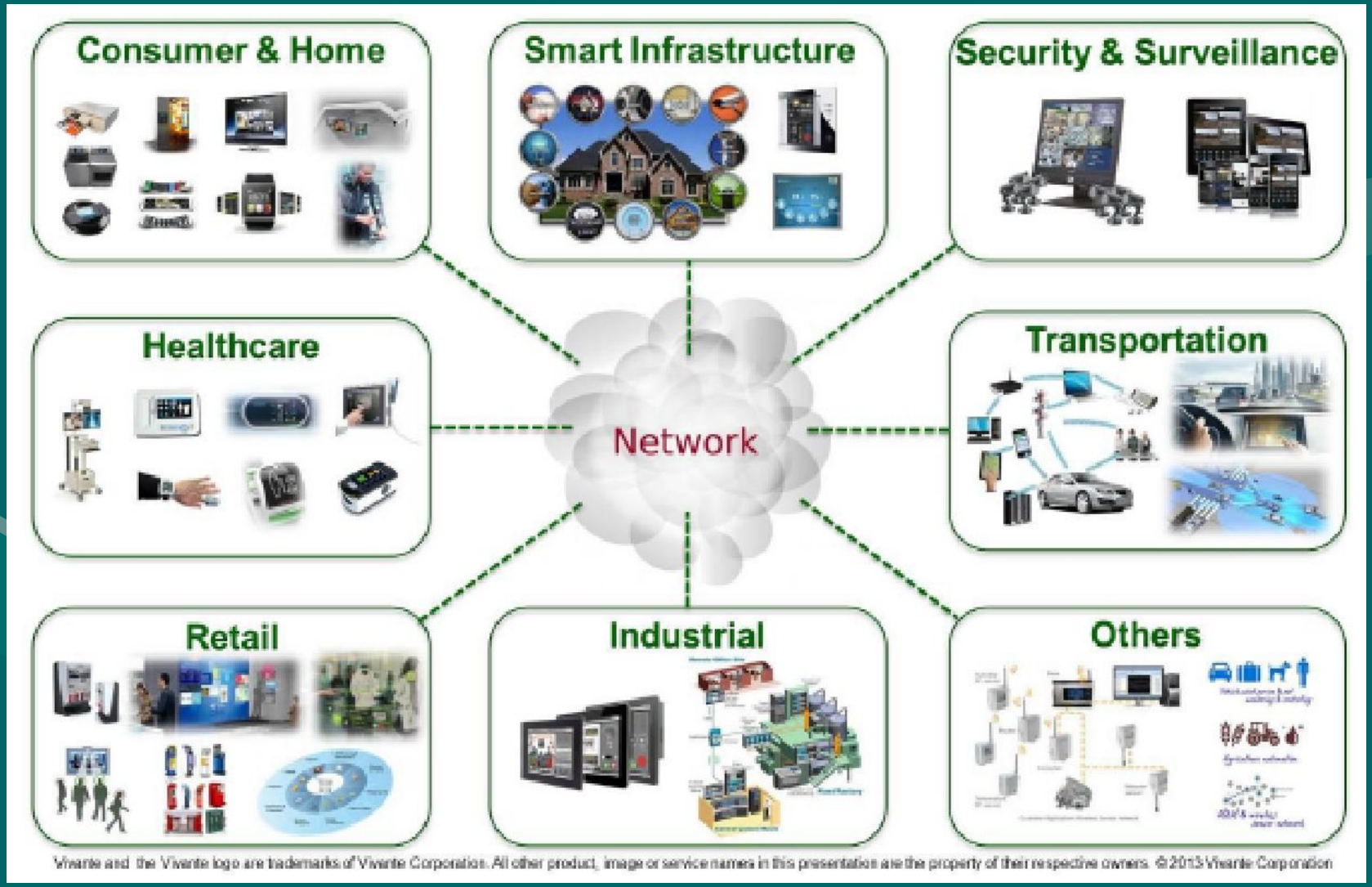
- Системы управления производством (АСУ ТП, SCADA-системы)
- Интернет вещей (Internet of Things, умный дом, умные вещи).
- Робототехнические системы критического назначения.
- Беспилотные летательные аппараты.
- Беспилотные автомобили.
- Системы военного назначения.

Сферы применения киберфизических систем

http://www.stw.nl/sites/stw.nl/files/20120711-Cyber-Physical%20Systems.jpg



Направления развития Интернета вещей



КАНАЛЫ ВОЗДЕЙСТВИЯ НА КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ

- Воздействия на подсистему управления
- Воздействия на человеко-машинный интерфейс
- Воздействия на устройства, входящие в состав киберфизических систем
- Воздействия на протоколы взаимодействия и сетевое оборудование

ТРУДНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КФС

Традиционные подходы не решают главную задачу

- Цель защиты КФС – обеспечение непрерывности процесса управления в условиях дестабилизирующих воздействий, а цель ИБ – обеспечение конфиденциальности, целостности, доступности данных

Непродуманность КФС с точки зрения безопасности

- Возможность идентификации киберфизических систем и ПО в локальных и глобальных сетях
- применение в современных КФС устаревших аппаратных и программных средств общего назначения
- Слабые средства авторизации и аутентификации («вшитые» в ПО аутентификационные данные по умолчанию, ненадежные алгоритмы и т.д.)
- Отсутствие шифрования в промышленных транспортных протоколах (modbus, s7comm и др.)
- Слабые средства аудита и регистрации событий

Негибкая архитектура КФС и АСУ ТП

- Невозможность внесения существенных изменений в системы
- Отсутствие обновлений операционных систем и приложений или невозможность их применить
- Высокий риск автоблокировки системы при внедрении средств защиты

Человеческий фактор

ОТЛИЧИТЕЛЬНЫЕ СВОЙСТВА КФС С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

ПРЕДЛАГАЕМАЯ СТРУКТУРА ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Аппарат оценки ИБ на основе конфиденциальной доступности, целостность для информационной составляющей включая:
   - *защищенность от атак из сети Internet*
   - *защиту внутренних протоколов*
   - *обнаружение уязвимостей по информационным и физическим компонентам.*
2. Оценка согласованности информационной и физической составляющей с учетом их взаимовлияния, свойств масштабируемости, интероперабельности, модульности на основе кросскорреляционных связей и оценки самоподобия, динамической устойчивости.
3. Оценка влияния информационных атак на систему управления (с учетом адаптивности) и способность к саморегуляции на основе фрактальных показателей устойчивости и способности к гомеостазу.
4. Оценка устойчивости структуры взаимосвязи элементов КФС на основе графовых методов оценки управляемости, масштабируемости, отказоустойчивости и константности функционирования в условиях информационных атак.
5. Разработка специфических критериев обнаружения атак на основе нарушения самоподобия и структурной устойчивости.

Показатели безопасности КФС (1)

	Интернет вещей	Многоагентные		SCADA, Системы в энергетике, медицине, производстве, обслуживание	Системы беспилотных движущихся средств	Интеллектуальные роботы
	Встроенные системы; WSN; RFID; NFS, M2M, Iot умный дом, Iot промышленный, виртуализированные системы	Биоинспирированные системы	Реконфигурируемые системы (гибкие)			
	Интернет ориентированные Человекоориентированные Семантикоориентированные			АСУ топологии производства; Удаленно управляемые агрегаты (эл. станции)	Дроны, беспилотные авто, системы видеокамер, спутники, средства разведки	Системы спутников, летательные станции, работы для чрезвычайных ситуаций, военные системы
Связь и механизмы взаимодействия	пассивная односторонняя двусторонняя наличие центра (ов) управления интернет подобия	Обмен со средой	Полный двусторонний обмен друг с другом	Взаимосвязи для выполнения технологических операций Использование модели механических исполнительных механизмов Согласованное управление информационной и исполнительной части в динамике Наличие центра мониторинга	Обмен со средой и с центром управления создание общего центра мониторинга и управления Полная двусторонняя связь друг с другом и центром управления	Автономные интеллектуальные системы, способные принимать решения без участия человека. Взаимодействие с внешним миром, другими комплексами Способность к самосохранению война роботов

Показатели безопасности КФС (2)

	Интернет вещей	Многоагентные		SCADA, Системы в энергетике, медицине, производстве, обслуживание	Системы беспилотных движущихся средств	Интеллектуальные роботы
	Встроенные системы; WSN; RFID; NFS, M2M, Iot умный дом, Iot промышленный, виртуализированные системы	Биоинспирированные системы	Реконфигурируемые системы (гибкие)			
Угрозы	▪ Атки на подсистему физических устройств для съема информации и хищения ресурсов, нарушения сети коммуникаций ▪ Атаки на протокол и технологии, сетевое оборудование, на RFID, Glowpan ▪ Атаки на сервер обработки, базы данных, веб-серверы, web-интерфейс			APT атаки на системы управления, исполнительные механизмы системы взаимодействия с использованием вывода из строя оборудования, отключение защитной автоматики	Атаки на сеть управления, на центр управления, доступ к системам и перехват управления через уязвимости wel-интерфейса и приложения	Информацион-ное противоборство
Системы управления КБС	Работа по заданной программе при минимальной обратной связи пассивный обмен, отсутствие мониторинга	Наличие системы мониторинга и обратной связи на параметрическом управлении Самоорганизация путем перенастройки и переконфигурации, самовосстановление	Обратная связь на параметрическом и сетевом уровне (переконфигурация) Наличие мониторинга и защиты Самооптимизация и проактивное восстановление	Адаптивное управление с несколькими уровнями обратной связи, мониторинг состояния, наличие активной аварийной защиты для медицинских систем Интеллектуальный мониторинг и управление роботами Контроль устойчивости исполнительных механизмов	Несколько уровней обратной связи, адаптивное управление приспособленной к окружающей среде программирования управления, использование гибкой системы коммуникации с управляемой архитектурой	Обеспечение гомеостаза на всех уровнях взаимодействия. Самосохранение Способность к рассуждению и антиципации (прогнозу)

Нормативно-правовая база обеспечения информационной безопасности информационно-психологической сферы в Российской Федерации

Закон РФ от 27 декабря 1991 г. N 2124-I "О средствах массовой информации"

- **Статья 1.** Свобода массовой информации

В Российской Федерации

- поиск, получение, производство и распространение массовой информации,
- учреждение средств массовой информации, владение, пользование и распоряжение ими,
- изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации,

не подлежат ограничениям, за исключением предусмотренных законодательством Российской Федерации о средствах массовой информации.

- **Статья 3.** Недопустимость цензуры

Цензура массовой информации, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей, - не допускается.

- **Статья 4.** Недопустимость злоупотребления свободой массовой информации
- Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности, или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань.
- Запрещается использование в радио-, теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье, а равно распространение информации об общественном объединении или иной организации, включенных в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 года N 114-ФЗ "О противодействии экстремистской деятельности" (далее - Федеральный закон "О противодействии экстремистской деятельности"), без указания на то, что соответствующее общественное объединение или иная организация ликвидированы или их деятельность запрещена.
- Запрещаются распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров, а также распространение иной информации, распространение которой запрещено федеральными законами.

- Порядок сбора информации журналистами на территории (объекте) проведения контртеррористической операции определяется руководителем контртеррористической операции.
- При освещении контртеррористической операции запрещается распространение в средствах массовой информации сведений о специальных средствах, технических приемах и тактике проведения такой операции, если их распространение может препятствовать проведению контртеррористической операции или поставить под угрозу жизнь и здоровье людей. Сведения о сотрудниках специальных подразделений, лицах, оказывающих содействие в проведении такой операции, выявлении, предупреждении, пресечении и раскрытии террористического акта, и о членах семей указанных лиц могут быть преданы огласке в соответствии с законодательными актами Российской Федерации о государственной тайне и персональных данных.
- Запрещается распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях сведений, содержащих инструкции по самодельному изготовлению взрывчатых веществ и взрывных устройств.
- Запрещается распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции.

Закон Яровой (пакет Яровой—Озерова)

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности

Принят Государственной Думой 24 июня 2016 года

Одобрен Советом Федерации 29 июня 2016 года

Статья 1

Внести в Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму» (Собрание законодательства Российской Федерации, 2006, № 11, ст. 1146; № 31, ст. 3452; 2008, № 45, ст. 5149; № 52, ст. 6227; 2009, № 1, ст. 29; 2010, № 31, ст. 4166; 2011, № 1, ст. 16; № 19, ст. 2713; № 46, ст. 6407; 2013, № 30, ст. 4041; № 44, ст. 5641; 2014, № 19, ст. 2335; № 23, ст. 2930; № 26, ст. 3385; 2015, № 1, ст. 58) следующие изменения:

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности

Принят Государственной Думой 24 июня 2016 года

Одобрен Советом Федерации 29 июня 2016 года

Статья 1

Внести в Уголовный кодекс Российской Федерации (Собрание законодательства Российской Федерации, 1996, № 25, ст. 2954; 1998, № 22, ст. 2332; № 26, ст. 3012; 1999, № 7, ст. 873; 2001, № 11, ст. 1002; № 26, ст. 2587, 2588; 2002, № 19, ст. 1793; № 30, ст. 3020, 3029; 2003, № 28, ст. 2880; № 50, ст. 4848; 2004, № 30, ст. 3091, 3092; 2005, № 1, ст. 13; 2006, № 31, ст. 3452; 2007, № 1, ст. 46; № 21, ст. 2456; № 31, ст. 4008; 2008, № 52, ст. 6235; 2009, № 1, ст. 29; № 31, ст. 3921; № 45, ст. 5263, 5265; № 52, ст. 6453; 2010, № 8, ст. 780; № 14, ст. 1553; № 19, ст. 2289; № 30,

Поправки, вносимые этим набором дополнений в федеральное законодательство, можно условно разделить на следующие части:

- расширение полномочий правоохранительных органов;
- новые требования к операторам связи и интернет-проектам;
- новые требования к перевозчикам-экспедиторам и операторам почтовой связи;
- усиление регулирования религиозно-миссионерской деятельности

Уголовный кодекс

Первый законопроект дополнил уголовный кодекс России тремя новыми составами преступления:

- **несообщение о преступлении террористического характера,**
- **содействие экстремистской деятельности и**
- **совершение акта международного терроризма.**

Хранение интернет-трафика

- Второй законопроект обязывает операторов связи хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев в соответствии с 64-й статьей федерального закона «О связи», а информацию о фактах приема, передачи, доставки и обработки сообщений и звонков — 3 года.
- Согласно проекту приказа Минкомсвязи, интернет-компании и сервисы должны хранить и предоставлять спецслужбам: псевдоним, дату рождения, адрес, фамилию, имя, отчество, паспортные данные, языки, которыми владеет пользователь, список его родственников, текст сообщений, аудио- и видеозаписи, адрес электронной почты, дату и время авторизации и выхода из информационного сервиса, наименование программы-клиента.
- 12 апреля 2018 года правительство РФ подписало постановление о том, что с 1 октября 2018 года операторы связи обязаны хранить в течение 30 суток текстовые, голосовые, видео- и другие сообщения пользователей. Далее оператор обязан увеличивать объем хранения на 15 процентов в год.

Средства шифрования

- Законопроект устанавливает запрет на использование несертифицированных средств кодирования (шифрования). За нарушение этого запрета нарушителю грозит штраф в размере от 3 000 до 5 000 руб. с конфискацией средств шифрования.

В Федеральной службе безопасности уточнили, что обязательная сертификация средств кодирования (шифрования) требуется только при передаче сведений, составляющих государственную тайну, поэтому сертификации систем мгновенного обмена сообщениями (месенджеров), таких как Telegram, WhatsApp и прочих при передаче сведений не составляющих гостайну, не требуется.

- Также «закон Яровой» обязывает организаторов распространения информации в интернете декодировать сообщения пользователей. По требованию ФСБ компании должны будут предоставлять ключи к зашифрованному трафику.

Деятельность религиозных организаций

- Закон также накладывает ограничения на деятельность религиозных организаций. В частности, устанавливается закрытый перечень мест, в которых допускается миссионерская деятельность, также вводится запрет миссионерской деятельности в жилых помещениях (кроме проведения религиозных обрядов и богослужений).
- При ведении миссионерской деятельности закон обязывает миссионеров иметь пакет документов, подтверждающих их полномочия. Вводится ограничение на участие иностранцев, въехавших в Россию по приглашению религиозной организации, на миссионерскую деятельность от имени иных религиозных организаций. Вводится запрет на миссионерскую деятельность, направленную против общественной безопасности, общественного порядка, прав и свобод личности и ряда иных целей

Аналоги

- С 2006 по 2014 год в ЕС действовала директива Еврокомиссии, предписывающая хранить минимум шесть месяцев метаданные (сведения о факте передачи информации: номера телефонов, с которых совершались звонки, IP-адреса, данные о базовых станциях, поблизости от которых находился абонент, и т. п.). В 2014 г. Европейский суд отменил эту директиву, и вопрос регулировался национальными законодательствами[45].
- В Великобритании в 2014 г. парламент одобрил Data Retention and Investigatory Powers Act 2014 (англ.)русск., обязывающий операторов связи хранить метаданные, но закон был оспорен в Высоком суде Лондона и суде Европейского союза. Стоимость создания и эксплуатации инфраструктуры для сбора и хранения метаданных в Великобритании оценивается в 170—180 млн £ за 10 лет.
- До начала 2016 г. в Германии операторы должны были хранить метаданные шесть месяцев, в начале 2016 г. в стране вступили в силу положения, снизившие срок хранения данных до 10 недель. Кроме того, сокращен перечень случаев, в которых правоохранительные органы могут истребовать эти данные.

Аналоги

- В Австралии с октября 2015 г. операторы должны хранить метаданные за последние два года. С учётом размера населения в 23 млн человек программа по сбору метаданных обходится в 400 млн австралийских долларов, операционные расходы — по 4 австралийских доллара на абонента в год. Правительство выделило 131 млн австралийских долларов в качестве грантов операторам связи на создание инфраструктуры, но не будет компенсировать операционные расходы.
- Бывший сотрудник спецслужб Эдвард Сноуден в 2013 г. передал СМИ информацию о разработанной Национальным агентством безопасности США системе PRISM, позволяющей негласно собирать любую информацию, передаваемую по сетям электросвязи. По оценкам The Washington Post, ежедневно системы сбора информации АНБ перехватывали и записывали около 1,7 млрд телефонных разговоров и электронных сообщений и около 5 млрд записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру[1].

Опыт Китая: «Золотой щит», он же «Великий китайский файрвол»

- **Проект «Золотой щит»** – система интернет-фильтрации, которая блокирует доступ к запрещенным коммунистической партией ресурсам из внешнего интернета. По всему миру «Золотой щит» известен также как «Великий китайский файрвол» (The Great Firewall of China). Цензура не распространяется на специальные административные районы Гонконг и Макао.

Разработка проекта была начата в 1998 г. (Шень Вей Гуан), **а в 2003 г. он был введён в эксплуатацию** по всей стране. Проект включает такие подсистемы, как:

- систему управления безопасностью,
- систему информирования о правонарушениях,
- систему контроля выхода и ввода,
- информационную систему мониторинга,
- систему управления трафиком.

- Китайская интернет-цензура не так проста, как это кажется на первый взгляд. Анализ фильтрации контента в социальных сетях показал, что ее цель – не тотальное искоренение какой-либо политической или общественной критики, а ***недопущение ее перерастания в политические выступление или движение, в том числе виртуальное***.

«Золотой щит» использует следующие методы фильтрации:

- Блокировка IP-адресов
- Фильтрация DNS-запросов и их переадресация
- Блокировка интернет-адресов (URL)
- Фильтрация на этапе пересылки пакетов
- Блокировка соединений, осуществляемых через VPN (*Virtual Private Network*)

Закон о защите российского сегмента сети Интернет от внешних угроз от 01.05.2019

- Согласно Федеральному закону оператор связи, оказывающий услуги по предоставлению доступа к сети Интернет, обязан обеспечивать установку в своей сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ сети Интернет и сети связи общего пользования, представлять информацию в Роскомнадзор о фактическом месте установки таких технических средств и соблюдать технические условия их установки, а также требования к сетям связи.
- Определен порядок управления сетями связи в случае возникновения угроз функционирования сети Интернет и сети связи общего пользования, а также порядок обеспечения устойчивого и безопасного использования в РФ доменных имен. В случае возникновения угроз Роскомнадзором может осуществляться централизованное управление сетью связи общего пользования. При этом лица, участвующие в централизованном управлении, обязаны выполнять правила маршрутизации сообщений электросвязи, установленные Роскомнадзором.
- Оператор связи не обязан ограничивать доступ к запрещенной информации, если доступ к такой информации в сети связи оператора связи ограничивается с помощью технических средств противодействия угрозам в порядке централизованного управления сетью связи общего пользования.

Федеральный закон от 01.05.2019 N 93-ФЗ "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации"

- **Определен порядок реализации запрета на распространение среди детей информации, содержащей изображение или описание сексуального насилия**
- Организатор зрелищного мероприятия (включая демонстрацию фильмов при кино- и видеообслуживании), посредством которого демонстрируется информационная продукция, содержащая такую информацию, обязан не допускать на такое мероприятие лиц, не достигших 18 лет.
- В целях выполнения указанной обязанности, а также в случае возникновения у лица, непосредственно осуществляющего реализацию входных билетов, приглашений и иных документов, предоставляющих право посещения зрелищного мероприятия (включая демонстрацию фильмов при кино- и видеообслуживании), посредством которого демонстрируется информационная продукция, содержащая такую информацию, или лица, контролирующего проход на такое зрелищное мероприятие, сомнения в достижении посетителем совершеннолетия лицо, осуществляющее реализацию входных билетов, или лицо, контролирующее проход на такое зрелищное мероприятие, вправе потребовать у него документ, удостоверяющий личность и позволяющий установить возраст этого посетителя. Перечень соответствующих документов будет устанавливаться уполномоченным Правительством РФ федеральным органом исполнительной власти.

- Порядок и условия присутствия (допуска) детей при проведении зрелищных мероприятий (включая демонстрацию фильмов при кино- и видеообслуживании) определяются локальным актом организатора зрелищного мероприятия.
- Установлен запрет допуска к распространению информационной продукции, содержащей указанную информацию, на расстоянии менее чем сто метров по прямой линии без учета искусственных и естественных преград от ближайшей точки, граничащей с территорией образовательных организаций, детских медицинских, санаторно-курортных, физкультурно-спортивных организаций, организаций культуры, организаций отдыха и оздоровления детей.

- Благодарю за внимание!

Стратегии защиты информации

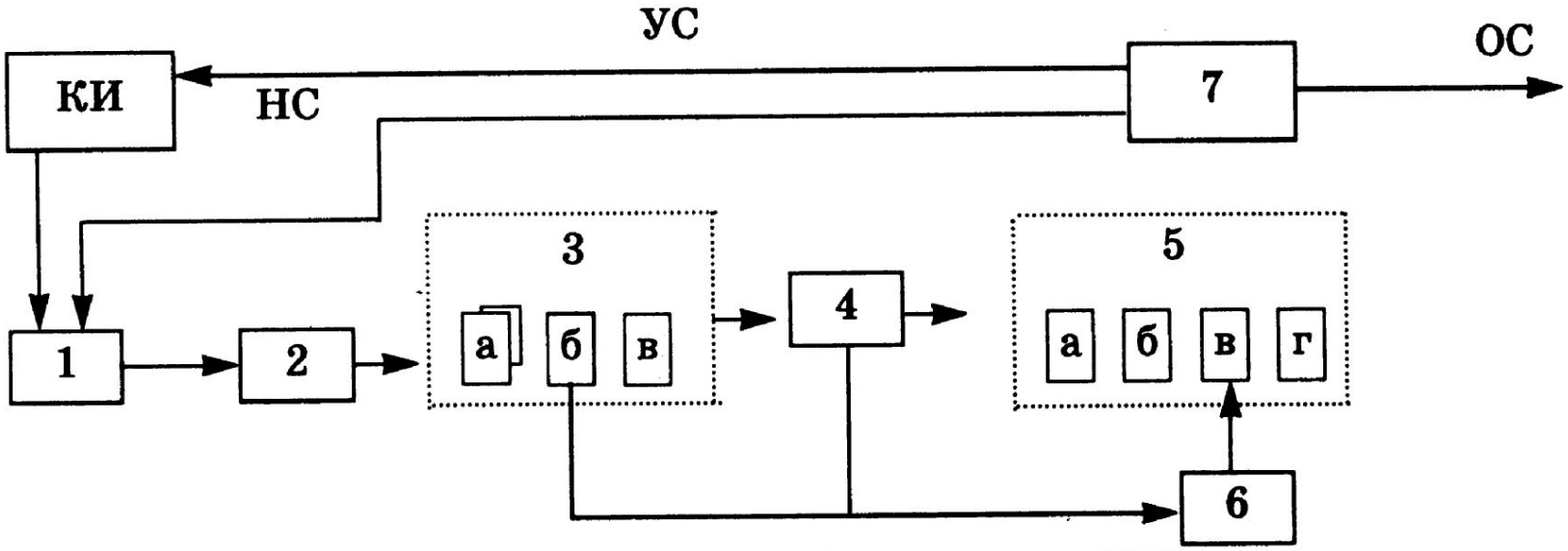


Рис. 2. Структура и общее содержание УКЗИ

КИ – концепции информатизации;
1 – среда защиты информации; 2 – методы структурирования среды защиты;
3 – методология оценки уязвимости информации: а – система показателей, б – система угроз, в – модели оценки;
4 – методология определения необходимого уровня защиты;
5 – система концептульных решений по защите: а – функции, б – задачи, в – средства, г – система;
6 – требования к концептуальным решениям; 7 – условия повышения эффективности защиты;
ОС, НС, УС – стратегия защиты (оборонительная, наступательная, упреждающая соответственно)

Подзаконные нормативные акты

- **Документы ФСТЭК России**
- Приказ Федеральной службы по техническому и экспортному контролю от 06.12.2017 №227 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»
- Приказ Федеральной службы по техническому и экспортному контролю от 11.12.2017 №229 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»
- Приказ Федеральной службы по техническому и экспортному контролю от 21.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»
- Приказ Федеральной службы по техническому и экспортному контролю от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
- Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Создание систем мониторинга и анализа социальных сетей, обеспечивающих:

- получение комплексного представления о текущей ситуации в конкретном регионе или государстве, выделение и оценка основных индикаторов, указывающих на нарастание социальной напряженности, прогнозирование динамики развития кризисных тенденций, оценка политических настроений населения;
- выявление террористических сетей (ТС) и экстремистских сетей (ЭС) (структуры сети, степени связности узлов, диаметра сети и т.д.);
- отслеживание идей, концепций, оппозиционных настроений, информационно-пропагандистских кампаний, слухов и дезинформации, распространяемых в социальных сетях, оценка степени их влияния на аудиторию, определение источников распространения информации, выявление иерархической структуры и географии протестного движения, прогнозирование времени начала протестных выступлений;
- наблюдение за деятельностью отдельных личностей, сетевых сообществ и общественных организаций, оппозиционных по отношению политике правительства;
- составление досье на интересующих участников социальных сетей (область интересов, привычки, психологические особенности т.д.) с целью безличного изучения потенциальных кандидатов на вербовку, объектов проникновения, секретоносителей, оппозиционных активистов, представителей бизнеса и СМИ и т.д.;
- выявление лиц и группировок, подозреваемых в подготовке террористических актов.

Характерные черты «цветных» революций

- Формой революции являются массовые митинги, демонстрации и забастовки, которые проводятся оппозицией после проведения выборов, по результатам которых оппозиция объявляется проигравшей. Оппозиция в таком случае утверждает, что были допущены нарушения избирательного законодательства, исказившие волю народа. Массовые протесты приводят либо к проведению повторного голосования (Украина), либо к силовому захвату зданий органов власти толпой (Югославия, Грузия, Киргизия) и бегству руководителей государства с последующим проведением новых выборов. В обоих случаях оппозиция приходит к власти.
- Революция проходит под антикоррупционными и радикально-демократическими лозунгами. Ключевыми являются идеи народного суверенитета Руссо, где народ (сознательно вышедшие на улицу граждане) противопоставляется манипулируемой режимом массе (Тунис, Египет, Йемен).
- Революции предшествует формирование молодёжных организаций (Пора, Отпор и т. д.), которые образуют т. н. «полевые отряды революции».
- Революция носит подчёркнуто бескровный характер. Здесь отзвук движения Ганди и хиппи, которые раздавали полицейским цветы (*flower power*). Отсюда характерный бренд революции — неагрессивный цвет (не красный и не чёрный) или цветок. Однако в Киргизии в результате столкновений с полицией и погромов магазинов после силового захвата зданий органов власти толпой были пострадавшие (убитых не было).
- Решающую роль в успехе революции играет сдержанность силовых структур («не допустить пролития крови»).
- Некоторые говорят о связях уличных протестов с грантами или стипендиями таких фондов как фонд Дж. Сороса «Открытое общество», Гарвардский университет, институт Альберта Эйнштейна, Международный республиканский институт и Национальный демократический институт (США), Международный центр ненасильственных конфликтов, Международный институт стратегических исследований в Лондоне и т. д.
- Проамериканская политика после революции — даже если считать, что прямых действий со стороны США, в виде денежной и консультационной помощи, не было, сложно отрицать факт, что после цветных революций политический курс становился подчёркнуто проамериканским, иногда построенным на антироссийской риторике. В свою очередь, США открыто поддерживает эти режимы. Наиболее яркими представителями такой политики являются Грузия и Украина. Учитывая сильные экономические связи с Российской Федерацией, особенно у Украины, это приводит к регулярным сбоям в торговых отношениях и, косвенно, приводит к ухудшению экономического положения таких стран.
-

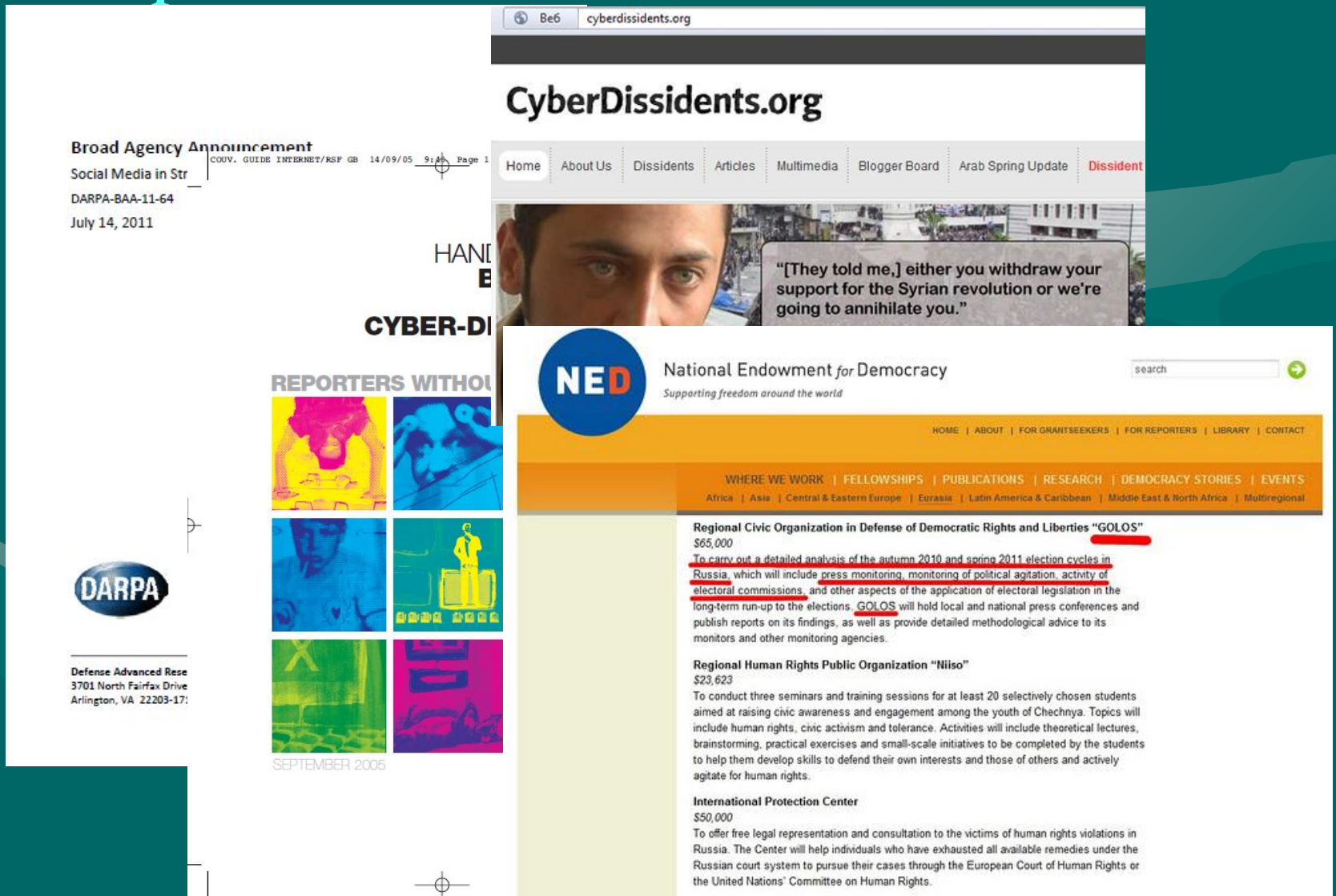
ОСНОВНЫЕ ЗВЕНЬЯ ТЕХНОЛОГИИ «БАРХАТНЫХ РЕВОЛЮЦИЙ»

1. *Выявляется энергетический конфликтный потенциал различных об щественных групп.*
2. *Определяются социальные группы и в том числе политические объединения, способные стать стихийным движителем политического протеста.*
3. *Готовятся в военизированных молодежных лагерях с помощью специальных тренингов, семинаров, загранстажировок и т. п. ударные силы революции и ее «менеджеры». Накапливается и разогревается энергетический потенциал молодежи и других граждан — потенциальных участников антиправительственного протеста.*
4. *Для того чтобы побудить своих возможных или уже реальных сто ронников к действиям, провозглашаемые цели должны стать реально ося заемыми и казаться вполне достижимыми, а также быть редуцированы, сведены к одной (иногда к нескольким) практической цели. Поэтому они максимально упрощаются и приближаются, т.е. сводятся к задачам, которые кажутся реально решаемыми.*
5. *Обеспечивается преимущество оппозиции в электронных СМИ и, прежде всего, на телевидении.*

1. *С помощью использования уже имеющихся и создания новых канальных факторов, побуждающих всех недовольных к социальной активности все большее число людей втягиваются в политические действия.*
2. *Вначале с помощью показного миролюбия и умиротворяющего словесного камуфляжа* (отсюда и названия: «бархатная революция», «революция красных гвоздик», «революция алых роз» и т. п.), *а затем и посредством психологического и иного террора по отношению к представителям власти и силовых структур, а также членам их семей парализуется деятельность правоохранительных органов. Посредством пропаганды и массовых про тивоправных действий общество приводится в бифуркационное состояние* (беспорядки, хаос, анархия).
3. *Весь процесс «бархатной революции» тщательно организуется и уп равляется специально подготовленными специалистами. Хорошо организованные группы стремятся подтолкнуть бифуркирующее, находящееся в состоянии шаткого хаотичного равновесия общество в нужном направлении.*
4. *В случае захвата власти данные ранее наиболее важные для людей обещания забываются. Сохраняется массовая бедность и фактическое бесправие большинства населения. Проводятся негласные чистки в госу дарственном аппарате. Почти полностью блокируется доступ недовольных к СМИ, особенно телевидению.*

«Информационная безопасность»

Практические действия США по управлению социальными ресурсами Интернет в своих геополитических целях



NED

National Endowment *for* Democracy

Supporting freedom around the world

search

HOME | ABOUT | FOR GRANTSEEKERS | FOR REPORTERS | LIBRARY | CONTACT

WHERE WE WORK | FELLOWSHIPS | PUBLICATIONS | RESEARCH | DEMOCRACY STORIES | EVENTS

Africa | Asia | Central & Eastern Europe | Eurasia | Latin America & Caribbean | Middle East & North Africa | Multiregional

Regional Civic Organization in Defense of Democratic Rights and Liberties "GOLOS"

$65,000

To carry out a detailed analysis of the autumn 2010 and spring 2011 election cycles in Russia, which will include press monitoring, monitoring of political agitation, activity of electoral commissions, and other aspects of the application of electoral legislation in the long-term run-up to the elections. GOLOS will hold local and national press conferences and publish reports on its findings, as well as provide detailed methodological advice to its monitors and other monitoring agencies.

Regional Human Rights Public Organization "Niiso"

$23,623

To conduct three seminars and training sessions for at least 20 selectively chosen students aimed at raising civic awareness and engagement among the youth of Chechnya. Topics will include human rights, civic activism and tolerance. Activities will include theoretical lectures, brainstorming, practical exercises and small-scale initiatives to be completed by the students to help them develop skills to defend their own interests and those of others and actively agitate for human rights.

International Protection Center

$50,000

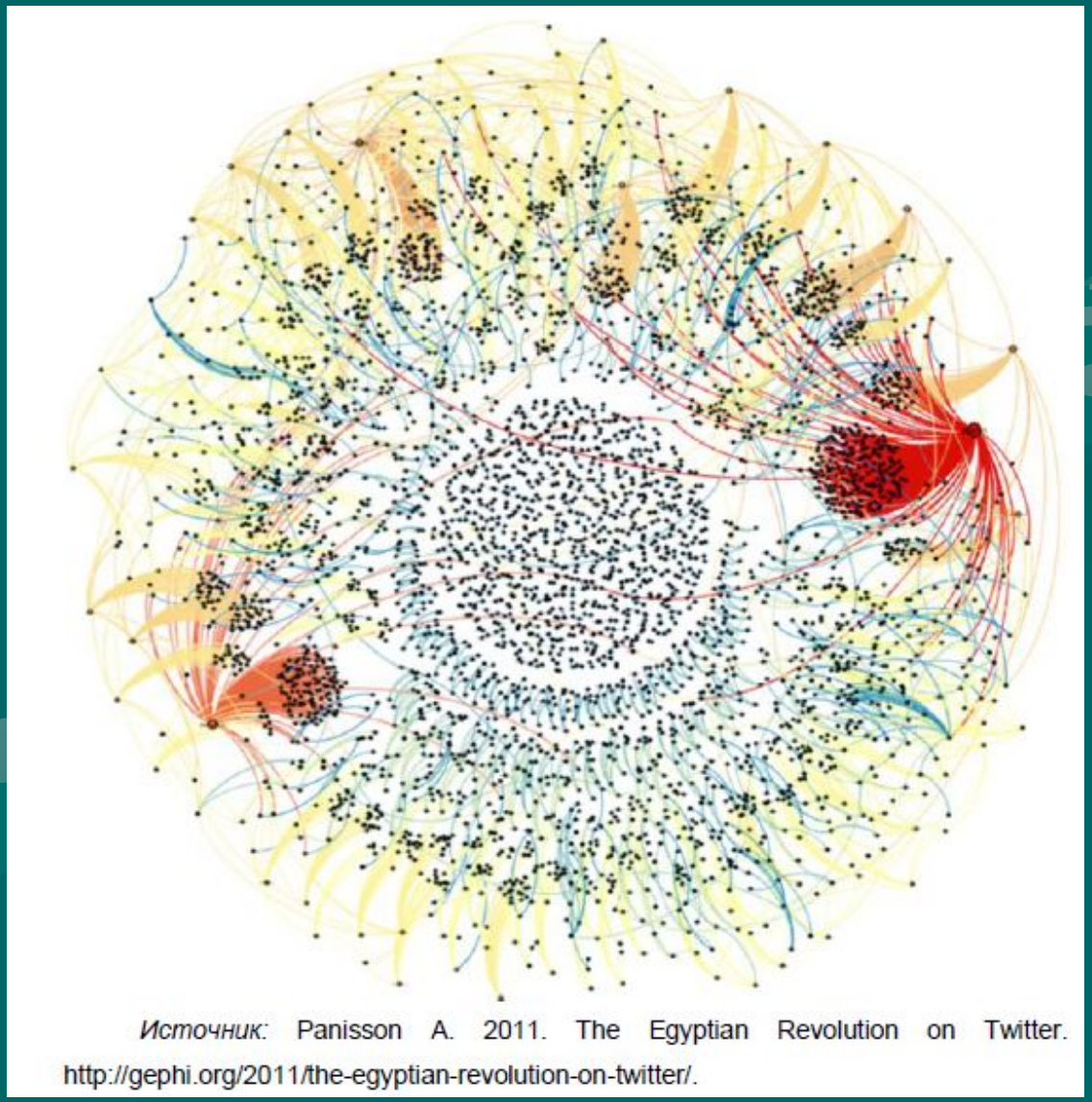
To offer free legal representation and consultation to the victims of human rights violations in Russia. The Center will help individuals who have exhausted all available remedies under the Russian court system to pursue their cases through the European Court of Human Rights or the United Nations' Committee on Human Rights.

Основные этапы разработки возможного воздействия на сложную социальную сеть в рамках «мягкой» модели (по Джину Шарпу)

- Выявление конфликтного потенциала различных социальных групп на основе противоречий в интересах.
- Выделение социальных групп, способных стать стихийным инициатором (проводником) волны протеста.
- Комплексная подготовка выделенных групп к дальнейшим активным действиям, определение концентраторов в рамках групп.
- Адаптация реальных целей в соответствии с мерой понимания выбранных групп и их концентраторов (возможно, навязывание ложных целей).
- Обеспечение информационного превосходства навязываемых идей (использование СМИ, вбрасывание информации в целевую среду и т.д.).

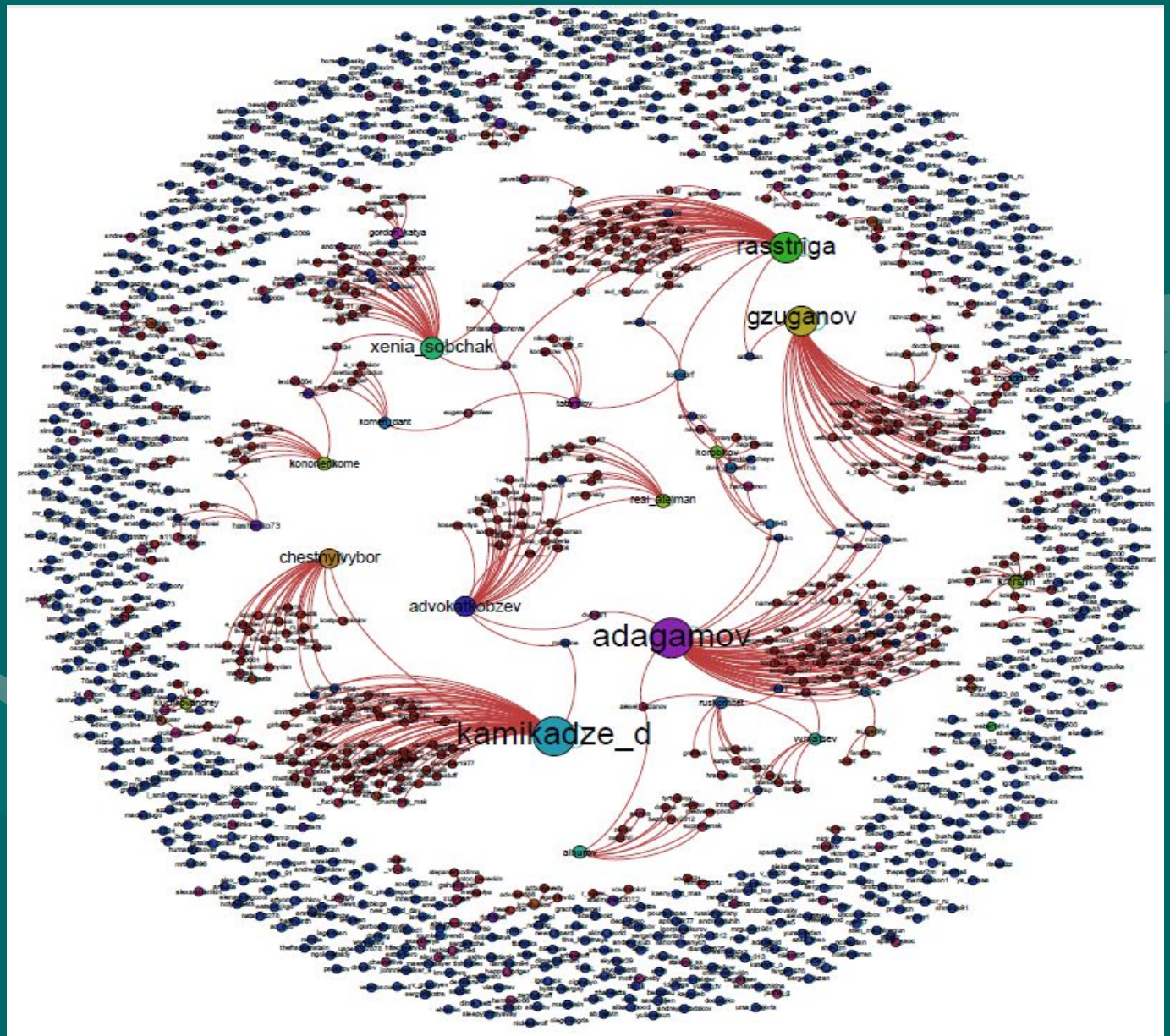
- Дальнейшее расширение контингента активных участников операции за счет обострения конфликтной ситуации («вербовка»).
- Оказание воздействий на систему защиты целевой сети с целью сокращения ее возможностей и, в идеале, полного блокирования.
- Перевод целевой системы в бифуркационное состояние с возможным влиянием на ход ее дальнейшего развития.
- После перехода системы в новое состояние (выгодное инициатору воздействий) ранее подогреваемые конфликты сводятся на нет, в том числе, с помощью «непопулярных» мер.

Топология социальной сети в Твиттере во время объявления отставки Президента Египта Х.Мубарака



Источник: Panisson A. 2011. The Egyptian Revolution on Twitter. http://gephi.org/2011/the-egyptian-revolution-on-twitter/.

Топология социальной сети в Twitter во время митинга на Болотной площади. Алгоритм Yifan Hu.



ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ: МОДЕЛИРОВАНИЕ АТАКИ НА СЕГМЕНТ ИНТЕРНЕТА ВЕЩЕЙ

Hype Cycle 2014