



**Федеральное агентство связи
(РОССВЯЗЬ)**

ЗАДАЧИ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ, УСТОЙЧИВОГО ФУНКЦИОНИРОВАНИЯ И БЕЗОПАСНОСТИ СЕТЕЙ СВЯЗИ ПЕРСПЕКТИВНЫХ ПОКОЛЕНИЙ

**Заместитель руководителя
Федерального агентства связи
Р.В. Шередин**

**Научно-практическая конференция
«Информационная безопасность в
современном обществе»
(Росинфоком -2016)**

Новосибирск, 2 сентября 2016 г.



Современный мир – информационное общество

Россвязь – активный участник построения информационного общества
явления, сопутствующие вхождению в информационную эпоху

Доминанта информационных процессов во всех сферах жизни и деятельности общества

Новые вызовы и угрозы

Развитие беспроводных технологий

Развитие технологий передачи больших объемов данных в масштабе времени, близком к реальному

Рост требований к оперативности и качеству информационного обеспечения жизнедеятельности общества

Осмысление путей разработки адекватных технических и сетевых решений



Промышленная революция 4.0 – киберфизические системы (соединение реальных объектов с информационными процессами или виртуальными объектами через информационные сети или Интернет)



Взаимодействие человека и государства: переход к электронному формату

***10. Расширение областей использования информационных технологий, являясь позитивным фактором для развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые вызовы и угрозы национальной безопасности. Это обусловлено усиливающейся тенденцией к использованию возможностей трансграничного оборота информации в информационном пространстве для достижения геополитических, военно-политических и иных целей в ущерб международной безопасности и стратегической стабильности, а также использованием информационных технологий в террористических, криминальных и иных противоправных целях.**

* - проект Доктрины информационной безопасности Российской Федерации, <http://www.scrf.gov.ru/documents/6/135.html>



Перспективные информационно-телекоммуникационные технологии

Мировые тенденции в условиях глобальной информатизации



Радикальное увеличение пропускной способности сетей и каналов связи

Повышение степени интеллектуальности систем связи

Обеспечение услугой передачи данных всех сфер жизни и деятельности людей

Перспективные информационно-телекоммуникационные технологии



Информация становится главной ценностью



Доктрина информационной безопасности России: национальные интересы РФ в информационной сфере и угрозы информационной безопасности

Доктрина информационной безопасности России

Основные составляющие национальных интересов РФ в информационной сфере

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею
2. Информационное обеспечение государственной политики Российской Федерации
3. Развитие современных информационных технологий, отечественной индустрии информации
4. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем

Угрозы информационной безопасности

- блокирование деятельности государственных СМИ;
- создание условий для усиления технологической зависимости России;
- закупка госорганами импортных средств связи и информатизации при наличии отечественных аналогов;
- вытеснение российских производителей;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности;
- противоправные сбор и использование информации;
- не декларированные возможности и вирусы;
- деструктивное воздействие на сети, включая радиоэлектронное подавление;
- жучки, закладки;
- перехват информации в сетях, дешифрование и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий и средств связи.

Проект новой Доктрины

Национальные интересы РФ в информационной сфере

- обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры Российской Федерации, включая критическую информационную инфраструктуру РФ и ЕСЭ РФ, в мирное время, в период непосредственной угрозы агрессии и в военное время;
- развитие отрасли информационных технологий в Российской Федерации, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказания услуг в области обеспечения информационной безопасности



Роль и место Россвязи в вопросах обеспечения информационной безопасности



Целостность



Устойчивость функционирования



Безопасность

Полномочия Россвязи

Угрозы

- блокирование деятельности государственных СМИ;
- создание условий для усиления технологической зависимости России;
- закупка госорганами импортных средств при наличии отечественных аналогов;
- вытеснение российских производителей;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности;
- противоправные сбор и использование информации;
 - не декларированные возможности и вирусы;
- деструктивное воздействие, включая радиоэлектронное подавление;
 - жучки, закладки;
 - перехват информации в сетях ПД и на ЛС, дешифрование и навязывание ложной информации;
 - использование несертифицированных отечественных и зарубежных информационных технологий.

- организует выполнение мероприятий по управлению и восстановлению единой сети электросвязи России при чрезвычайных ситуациях;
- организует систему сертификации в области связи, включающую в себя органы по сертификации, испытательные лаборатории (центры), независимо от их организационно-правовых форм и форм собственности;
- осуществляет функции государственного заказчика научно-технических и инвестиционных программ и проектов в установленной сфере деятельности;
- обеспечивает защиту сведений, составляющих государственную тайну, в процессе деятельности Агентства, а также контроль и координацию деятельности подведомственных учреждений и иных организаций в указанной области.

Роль и место Россвязи в вопросах обеспечения информационной безопасности

Подготовка платформы и условий обеспечения безопасности сетей связи различного назначения, построенных с использованием перспективных технологий (с задействованием потенциала подведомственных НИИ и ВУЗов).

Цель: обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи РФ



Формирование тематики «Росинфоком-2016»

2015 год: создание НТС Россвязи

«Росинфоком-2015»
октябрь 2015
Санкт-Петербург

Вопросы истории развития и состояния сетей связи

Определение основных направлений и задач обеспечения эффективного применения созданных сетей

Проработка нормативно-правовой сферы

Панельная дискуссия
май 2016
Москва

Перспективы развития сетей, систем и технологий связи

Определение концептуальных направлений развития отрасли в период интенсивного перехода к информационному обществу

Возникновение широкого спектра угроз, влияющих на сохранность, достоверность информации, скорость и своевременность ее передачи

«Росинфоком-2016»
сентябрь 2016
Новосибирск

Обеспечение целостности, устойчивости и безопасности перспективных сетей связи

Разработка мер и мероприятий по обеспечению информационной безопасности на сетях связи

Информационная безопасность в среде Интернет



Сферы инновационного развития телекоммуникаций и информационная безопасность

Интернет-ориентированная
связь

Связь Мобильного мира

Когнитивная связь

Квантовая связь

Угрозы
информационной
безопасности

Аппаратные
средства

Программное
обеспечение

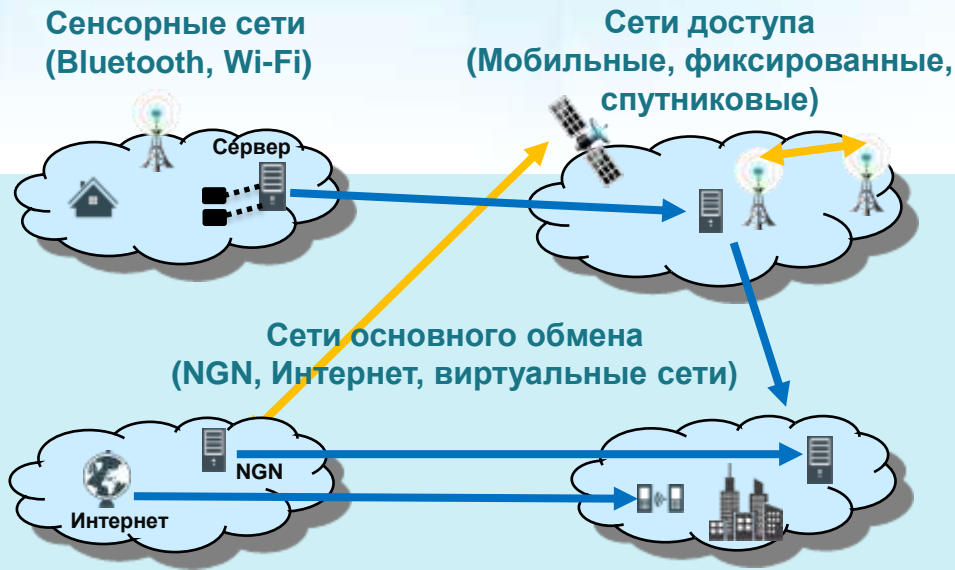
Система
связи

Традиционные точки приложения
процесса обеспечения
безопасности



Интернет-сфера в информационном обществе

Типы сетей телекоммуникационного уровня



Угрозы информационной безопасности в интернет-сфере

Особенности построения российского сегмента Интернет и его существенная зависимость от состояния взаимодействия и отношений с зарубежными партнерами

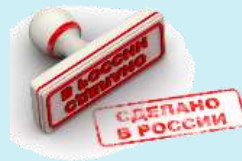
Формирование модели угроз интересам стран в ИКТ сфере в части создания и применения Интернет-ориентированных технологий связи

Разрушение контента и ПО
Дезинформация
Внешнее управление системами и процессами

Международный уровень



Защита интересов РФ в области ИКТ на международном уровне



Импортозамещение

- Развитие отечественных технологий, техники и информационных продуктов, в том числе разработка отечественных аппаратно-программных средств;
- Повышение устойчивости и защищённости отечественных сетей связи, в первую очередь тех, которые используются государственными структурами.

Интернет-ориентированная связь

Связь Мобильного мира

Когнитивная связь

Квантовая связь



Мобильный мир как часть Глобального информационного пространства

Основа Мобильного мира – сети подвижной связи и широкополосного беспроводного доступа



Мобильный мир вышел за пределы отрасли телекоммуникаций

22 млрд устройств M2M и Интернета вещей

5 млрд человек

Всемирный прогноз

2016

2018

Будущее Мобильного мира – переход от контентных моделей к бизнес-моделям



Интернет-ориентированная связь

Связь Мобильного мира

Когнитивная связь

Квантовая связь

9



Угрозы информационной безопасности в сфере Мобильного мира

Основные угрозы информационной безопасности

Перехват информации

Технологическая слежка за пользователем

Утечки персональных данных

Контент – угрозы

Основной пригодный к практическому использованию способ секретной связи – организация защищенного канала поверх стандартных открытых каналов



- «Прозрачно» задействуется существующая сетевая инфраструктура
- Дополнения, обеспечивающие секретность, реализуются «на уровне приложений»

Технологии защиты от информационных утечек основаны на использовании криптографии



- SSL (Secure Sockets Layer)
- TLS (Transport Layer Security).



Когнитивная связь - технологии искусственного интеллекта. Перспективы и вызовы

Тенденция использования в информационно-телекоммуникационных сетях агентоориентированного искусственного интеллекта (когнитивных элементов)

Технология построения когнитивного радио

Технология построения когнитивных сетей

Технология построения когнитивных инфокоммуникационных систем

Перспективный сценарий преодоления возрастающей сложности окружающего мира – передача части интеллектуальных функций в экономике, политике и производстве когнитивным системам

С развитием концепций «умного города», Интернета вещей, сетей транспортных средств предполагается развитие интеллектуальноподобных всепроникающих сетей (SUN – Smart Ubiquitous Networks), решения по управлению которыми реализуются на программном уровне при помощи специальных приложений и в которых уровень управления сетью отделён от устройств передачи данных и реализуется программно.



Россвязь будет активно поддерживать научные исследования и разработки в области создания экспертных систем, мультиагентных систем, обеспечивающих интеллектуализацию и автоматизацию процессов управления комплексными сетями связи и вещания.

Интернет-ориентированная связь

Связь Мобильного мира

Когнитивная связь

Квантовая связь

11



Угрозы безопасности когнитивных систем связи



Нарушение конфиденциальности данных и программ

Разрушение целостности данных, программ и аппаратуры

Ограничение доступности данных

Срыв управления объектами и процессами



В силу большого удельного веса программных средств в обеспечении построения и эффективного применения интеллектуальных когнитивных сетей связи парирование названных угроз в значительной мере обеспечивается импортозамещением в аппаратно-программной сфере.

Однако это предполагает и использование способов обеспечения целостности, устойчивости и безопасности сетей связи, которые связаны с инфраструктурной живучестью сетей, криптографической защищенностью информации, обеспечением целостности контента и т.п.



Квантовая связь. Будущее инфокоммуникационных технологий

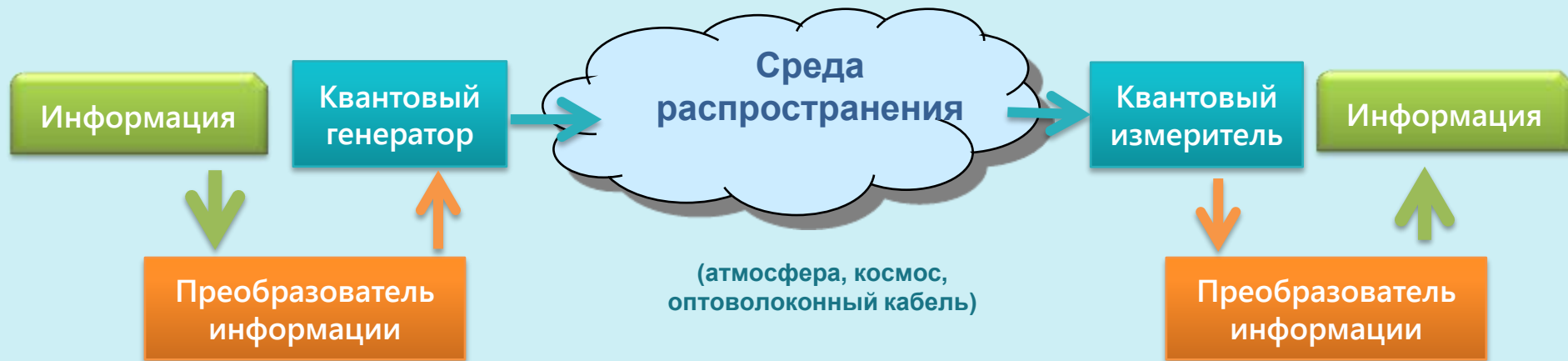
Квантовая связь – результат поиска инженерной мысли в направлении повышения защищенности информации в каналах связи с использованием достижений квантовой обработки и передачи данных



При решении задач синтеза и сетевой оптимизации современных и перспективных систем связи, обеспечения высокой защищенности информации в каналах связи современные компьютеры не способны решать ряд важных задач (криптография, поиск рациональных маршрутов в сетевых структурах и ряд других задач).



Использование квантовой теории идет по двум направлениям: создание квантовых компьютеров и разработка основ квантовой связи.





Квантовая связь – перспективы и угрозы

Квантовая связь представляет собой передачу кубитов на расстояние с использованием фотонов, что приводит к возникновению своего рода квантового Интернета

Перспективы

- Существенное ускорение производительности в некоторых видах вычислений
- Создание квантовых каналов связи – сверхзащищенных и высокопроизводительных сетей передачи информации, квантовая криптография

Угрозы

- Новые методы и средства криптоанализа – угроза традиционным инфокоммуникационным технологиям
- Проблемы защиты финансового сектора, ОПК и других защищаемых секторов.
- Перестают работать традиционные методы ЭЦП и удостоверения личности в цифровом пространстве





Задачи обеспечения целостности, устойчивого функционирования и безопасности при разработке технологий и строительстве сетей связи

Появление и развитие новых технологий связи обуславливает новые подходы к задачам обеспечения устойчивости, целостности и безопасности

Традиционные задачи

Совершенствование средств криптографии

Развитие систем контроля целостности контента

Развитие систем защиты от несанкционированного доступа

Модернизация антивирусной защиты

Совершенствование нормативно-правовой и нормативно-технической базы безопасности на сетях связи

Современные задачи

Создание и внедрение систем выявления атак

Разработка и внедрение протоколов связи, работающих с любыми криптонадстройками

Обеспечение конвергентной совместимости различных сетей связи

Импортозамещение в аппаратно-программной сфере сетевого ядра систем связи



Подтверждение соответствия как способ обеспечения информационной безопасности

Принятие технических решений по созданию перспективных систем связи, адекватных угрозам информационной безопасности, является необходимым, но не достаточным условием реальной защищенности

Одним из эффективных методов ее достижения является подтверждение соответствия заданным требованиям серийных образцов техники связи. В системе подтверждения соответствия в области связи 5 органов по сертификации и 19 испытательных лабораторий (центров), 5 из них в подведомственных Россвязи организациях



Оценка параметров ЭМС

В отрасли имеется уникальная организация, выполняющая задачи оценки соответствия параметров техники связи различного назначения - филиал ФГУП НИИР Испытательный центр «Омега» (г. Севастополь).

ИЦ «Омега», наряду с функциональными испытаниями, проводит испытания по таким параметрам, существенно влияющим на информационную безопасность, как параметры электромагнитной совместимости.



Испытания средств Эра-ГЛОНАСС



Функциональные испытания, в т.ч. средств КОСПАС-САРСАТ



Испытательный центр «Омега»

Механико-климатические испытания





Подготовка квалифицированных кадров – залог обеспечения информационной безопасности и безопасности ЕСЭ РФ

Кадры - основная движущая сила отрасли «Связь»

Отрасли необходимы специалисты, способные воспринять задачи развития инфокоммуникационного и телекоммуникационного рынков и обеспечить их решение в ближайшей перспективе

Подготовка кадров для телеинфокоммуникационной отрасли осуществляется в 4-х вузах, подведомственных Россвязи. В 2016 г. наши подведомственные учебные заведения обучили 35,5 тысячи студентов по 11 направлениям и 24 специальностям высшего образования и по 14 специальностям среднего профессионального образования.

Подготовка кадров ведется с учетом тенденций сегодняшнего дня. В рамках направлений «Информатика и вычислительная техника» и «Инфокоммуникационные технологии и системы связи» выделены специальности высшего образования в сфере безопасности телекоммуникационных систем, среди них: **Программная защита информации и Безопасность и программная защита инфокоммуникаций.**





**Федеральное агентство связи
(РОССВЯЗЬ)**

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

www.rossvyaz.ru