Федеральное агентство связи
(РОССВЯЗЬ)

IX Уральский форум
«Информационная безопасность финансовой сферы»

Устойчивое функционирование Единой сети электросвязи Российской Федерации - залог обеспечения безопасности информационной инфраструктуры финансового рынка. Предложения по противодействию угрозам.

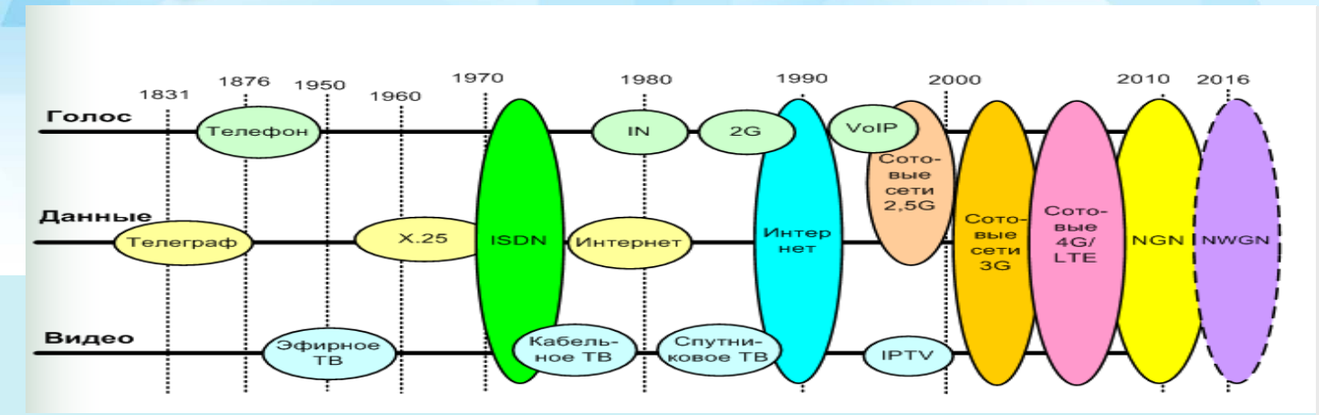
Презентация подготовлена совместно со специалистами ФГУП ЦНИИС

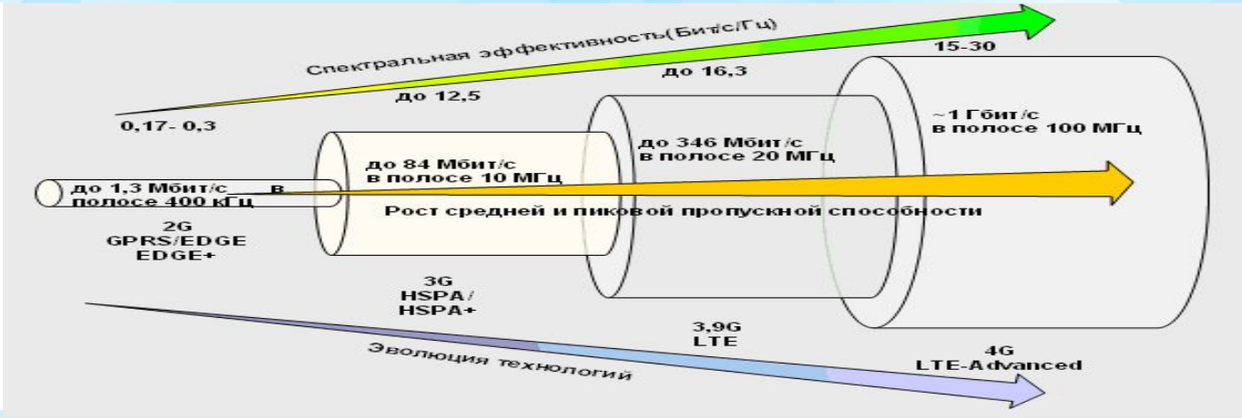
ЦНИИС

Заместитель руководителя
Федерального агентства связи
Шередин Роман Валериевич

Республика Башкортостан
14 февраля 2017 г.

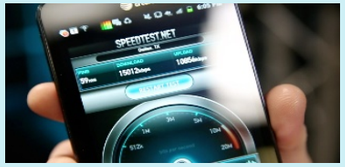
Эволюция сетей и технологий связи





От сторожевых постов и башен,
оптического семафорного телеграфа –
к современным технологиям и средствам связи

Технологии ближайшего будущего



- Широкополосный беспроводной доступ
- Интернет вещей
- Оптические технологии
- Технологии SUN и NFV

Современное общество = Информационное общество

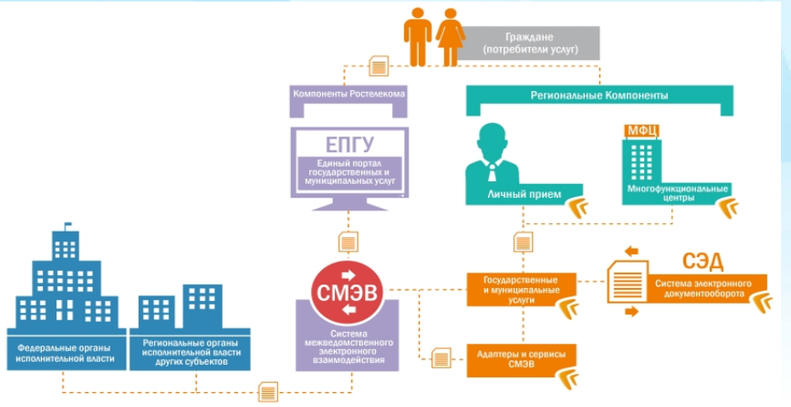
Сопутствующие явления

Доминанта информационных процессов во всех сферах жизни и деятельности общества

Рост требований к оперативности и качеству информационного обеспечения жизнедеятельности человека, общества, бизнеса и государства

Развитие технологий, в том числе беспроводных, передачи больших объемов данных в масштабе времени, близком к реальному.

Повышение степени интеллектуальности сетей связи, конвергенция сетей и услуг. Виртуализация и облачные технологии.



гражданин, бизнес и государство:
переход к электронному формату взаимодействия

«Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.
Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.
При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.»*

* - п. 10 Доктрины информационной безопасности Российской Федерации, Указ Президента РФ от 05.12.2016 № 646

Новые вызовы и угрозы

разработка адекватных технических и сетевых решений для их нейтрализации

Стратегия национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.

Указом Президента Российской Федерации от 31.12.2015 утверждена **Стратегия национальной безопасности РФ**. В Стратегии указано, что при ее реализации ***особое внимание уделяется обеспечению информационной безопасности с учетом стратегических национальных приоритетов***.

- В Стратегии, среди основных угроз государственной и общественной безопасности, отмечена деятельность террористических и экстремистских организаций, связанная с ***нарушением безопасности и устойчивости функционирования критической информационной инфраструктуры*** Российской Федерации.
- В соответствии со Стратегией для противодействия угрозам качеству жизни наших граждан органы власти во взаимодействии с институтами гражданского общества обеспечивают ***развитие информационной инфраструктуры***, ***доступность информации*** по различным вопросам социально-политической, экономической и духовной жизни общества, ***равный доступ к государственным услугам*** на всей территории Российской Федерации, в том числе ***с использованием информационных и коммуникационных технологий***.

Указом Президента Российской Федерации от 05.12.2016 утверждена **Доктрина информационной безопасности**

- Доктриной обозначены стратегические цели и основные направления обеспечения информационной безопасности с учётом стратегических национальных приоритетов Российской Федерации.
- Введено понятие «***информационная инфраструктура Российской Федерации***», под которой понимается совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации и под ее юрисдикцией.
- В числе национальных интересов в информационной сфере указано ***обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры, и Единой сети электросвязи Российской Федерации***, в мирное время, в период непосредственной угрозы агрессии и в военное время.

Решение задач обеспечения информационной безопасности в целом и ***обеспечения устойчивого и бесперебойного функционирования информационной инфраструктуры в частности, неразрывно связано с развитием науки и образования в сфере информационных технологий, а также постепенным импортозамещением инфраструктурного оборудования.***

Указанные задачи Россвязи понятны и их решением Агентство занимается в повседневной деятельности.

Полномочия Федерального агентства связи

В соответствии с постановлением Правительства РФ от 30.06.2004 № 320
«Об утверждении положения о Федеральном агентстве связи» и иными НПА
Федеральное агентство связи (Россвязь):

является федеральным органом исполнительной власти, осуществляющим функции по управлению государственным имуществом и оказанию государственных услуг в сфере электросвязи и почтовой связи, в том числе в области создания, развития и использования сетей связи, спутниковых систем связи, систем телевизионного вещания и радиовещания;

организует выполнение мероприятий по управлению и восстановлению единой сети электросвязи Российской Федерации при чрезвычайных ситуациях;

организует систему сертификации в области связи;

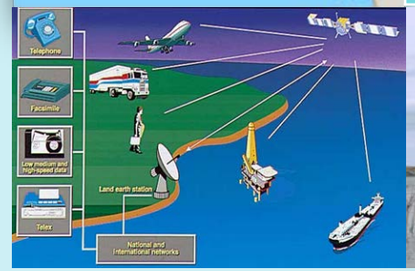
ведет регистрацию деклараций о соответствии средств связи и реестр сертификатов соответствия системы сертификации в области связи;

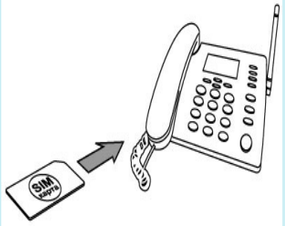
рассматривает заявления и принимает решения о выделении ресурса нумерации;

осуществляет обеспечение работ по учету, изъятию, передаче и переоформлению ресурса нумерации, а также по формированию и ведению реестра нумерации российской системы и плана нумерации;

осуществляет функции государственного заказчика научно-технических и инвестиционных программ и проектов в установленной сфере деятельности.

является учредителем 4 высших учебных заведений, осуществляющих подготовку кадров с высшим и средним профессиональным образованием для отрасли инфотелекоммуникационной отрасли





Россвязь & Силы обеспечения ИБ

Информационная безопасность

Целостность

Конфиденциальность

Доступность

Безопасность информационной инфраструктуры – среды распространения информации

=

Безопасность ЕСЭ РФ

Информация – главная ценность

Информационная инфраструктура финансовой сферы - составная часть информационной инфраструктуры Российской Федерации

Целостность

управление государственным имуществом и оказание государственных услуг **в сфере электросвязи и почтовой связи, в том числе** ***в области создания, развития и использования сетей связи*****, спутниковых систем связи, систем телевизионного вещания и радиовещания**

Устойчивость функционирования

организация системы сертификации в области связи**, включающей в себя органы по сертификации, испытательные лаборатории (центры)**

Безопасность

выполнение мероприятий по управлению и восстановлению Е**диной сети электросвязи Российской Федерации** ***при чрезвычайных ситуациях***

силы обеспечения ИБ - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством РФ задач по обеспечению ИБ

Участие Россвязи в IX Уральском форуме обусловлено тем, что задача обеспечения информационной безопасности – это комплексная задача, решение которой неразрывно связано с обеспечением целостности, устойчивости функционирования и безопасности Единой сети электросвязи Российской Федерации

НТС Россвязи

Научно-технический совет Россвязи

- Научно-техническое и научно-методическое обеспечение Россвязи
- Повышение эффективности деятельности подведомственных организаций

задачи

задачи

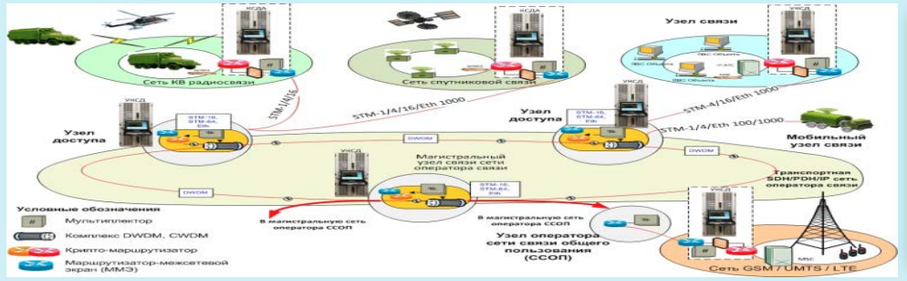
- Выработка единой технической политики в сфере деятельности Россвязи и подведомственных организаций
- Определение приоритетных направлений НИР и ОКР
- Организация проведения и всесторонний анализ результатов НИР и итогов выполнения ФЦП

Секция развития телефонных сетей связи и сетей передачи данных

Секция развития радиосвязи, спутниковой связи, радио– и телевещания

Секция организации подтверждения соответствия и обеспечения СОРМ

Секция развития стандартизации и добровольной сертификации



Секция развития универсальных услуг связи

Секция почтовой связи

Секция «Образование»

Секция сетей связи нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка

64 заседания секций и Президиума по 109 вопросам

http://www.rossvyaz.ru/about/Comission/HTS

Россвязь & ФГУП ЦНИИС vs Угрозы ИБ (для финансовой сферы)

ЦНИИС

ВЗЛОМ

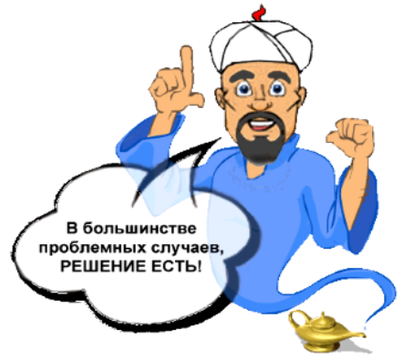
ФРОД

Подмена номера

ВРЕДОНОСНОЕ ПО

DDoS

СПАМ



Россвязь & подведомственные НИИ и ВУЗы

ЦНИИС

С 1918

Включен в перечни: стратегических предприятий; предприятий ОПК.

100% Государственная компания

Научная организация 1-ой категории

Центр внедрения СОРМ на ССОП

Оператор БДПН
ППРФ от 9.10.2013 №1832-р

Подключено более 150 банков

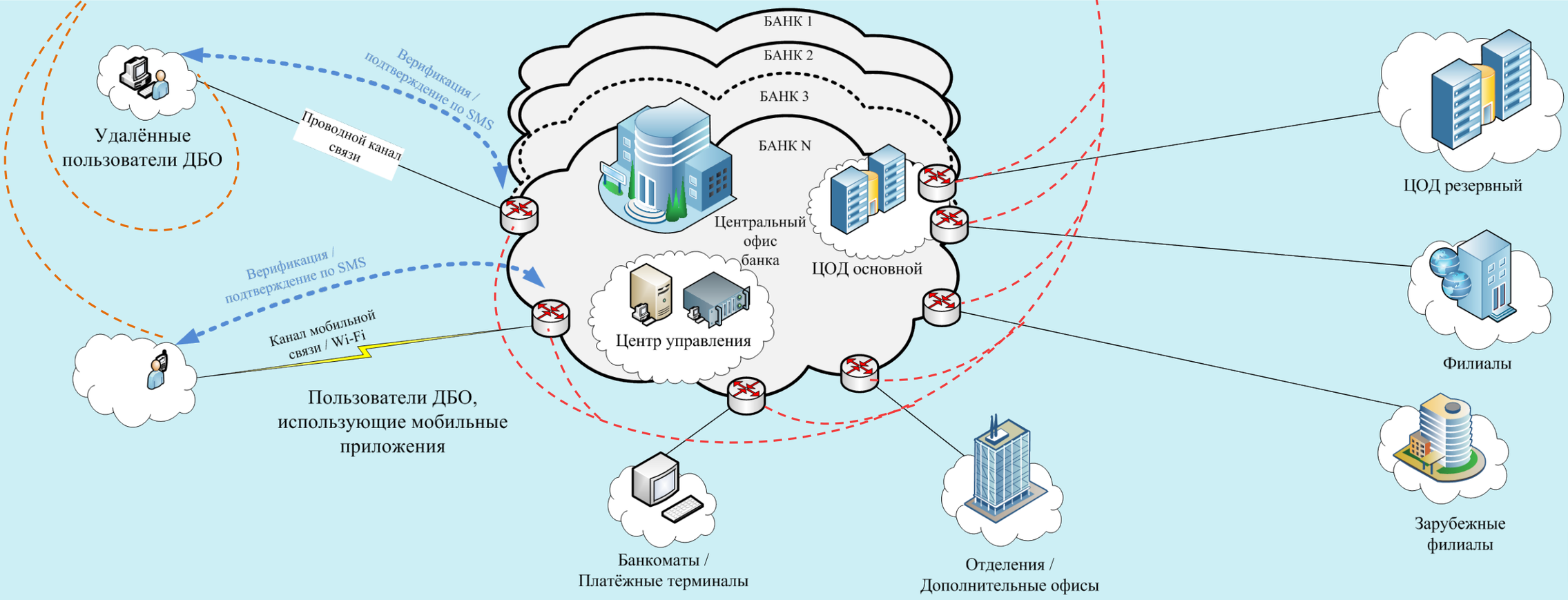
Подключено 100% операторов ПРТС

открытие БАНК | СБЕРБАНК | ВТБ | РоссельхозБанк | TELE2

Предложения ФГУП ЦНИИС для финансовой сферы. Угрозы для информационной инфраструктуры

ГРУППА УГРОЗ ТИПА «А»
Фрод (мошеннические платежи) из-за:
- Подмены номера
- Вредоносного ПО или атаки

ГРУППА УГРОЗ ТИПА «В»
Dos/DDoS атаки



Предложения по противодействию угрозам типа «А»

Основные функции и задачи

- ✓ Организационно-техническое взаимодействие со всеми действующими операторами подвижной радиотелефонной связи Российской Федерации в режиме реального времени
- ✓ Предоставление кредитным и иным организациям информации:
  - о подтверждении корректности связки IMSI-IMEI при проведении банковских операций с использованием сервисов ДБО

  В дальнейшем:
  - о дате заключения договора, о дате выдачи или замены SIM-карты
  - история архивов IMEI-кодов
  - данные об операционной системе

Результат для финансового рынка

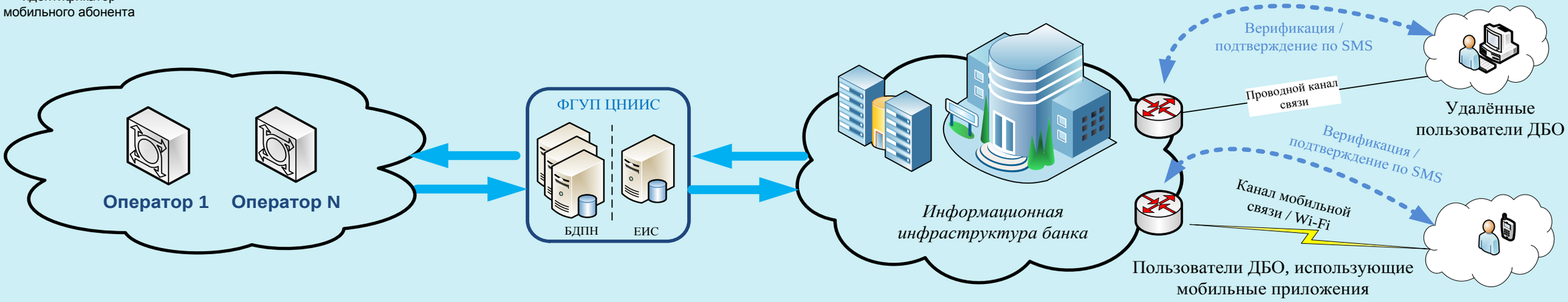
- ✓ Единый сервис (принцип «одного окна») для получения информации от ЦНИИС (по всем действующим операторам подвижной радиотелефонной связи Российской Федерации (в том числе и региональным))
- ✓ Дополнительная верификация абонентов
- ✓ Отслеживание абонентских устройств, с которых отсылается спам или вредоносное программное обеспечение
- ✓ Повышение уровня безопасности переводов денежных средств с использованием мобильного телефона
- ✓ Повышение уровня защищенности граждан

повышение защищенности банковских операций, проводимых клиентами, и предотвращение мошеннических действий.

IMSI
Международный идентификатор мобильного абонента

Единая информационная система (ЕИС)

IMEI
Международный идентификатор мобильного оборудования



Предложение по противодействию угрозам типа «В»

Вариант № 1 – постоянное взаимодействие инфраструктуры банка с ССОП через МЦА в режиме 24/7

Основные функции и задачи

- ✓ Обеспечение необходимого уровня защиты инфраструктуры банков:
  - анализа поведения сети в реальном времени, создание критериев нормального поведения сети, приложений и действий пользователей
  - распознавания уже известных сигнатур, периодическое их обновление в случае обнаружения новых видов атак с повышенным риском применения
  - анализа безопасности используемых приложений и вычисление потенциальных угроз в приложениях
- ✓ Служба технической поддержки
  - круглосуточное экспертное обслуживание заказчиков по противодействию DDoS атакам для восстановления работы сети и услуг

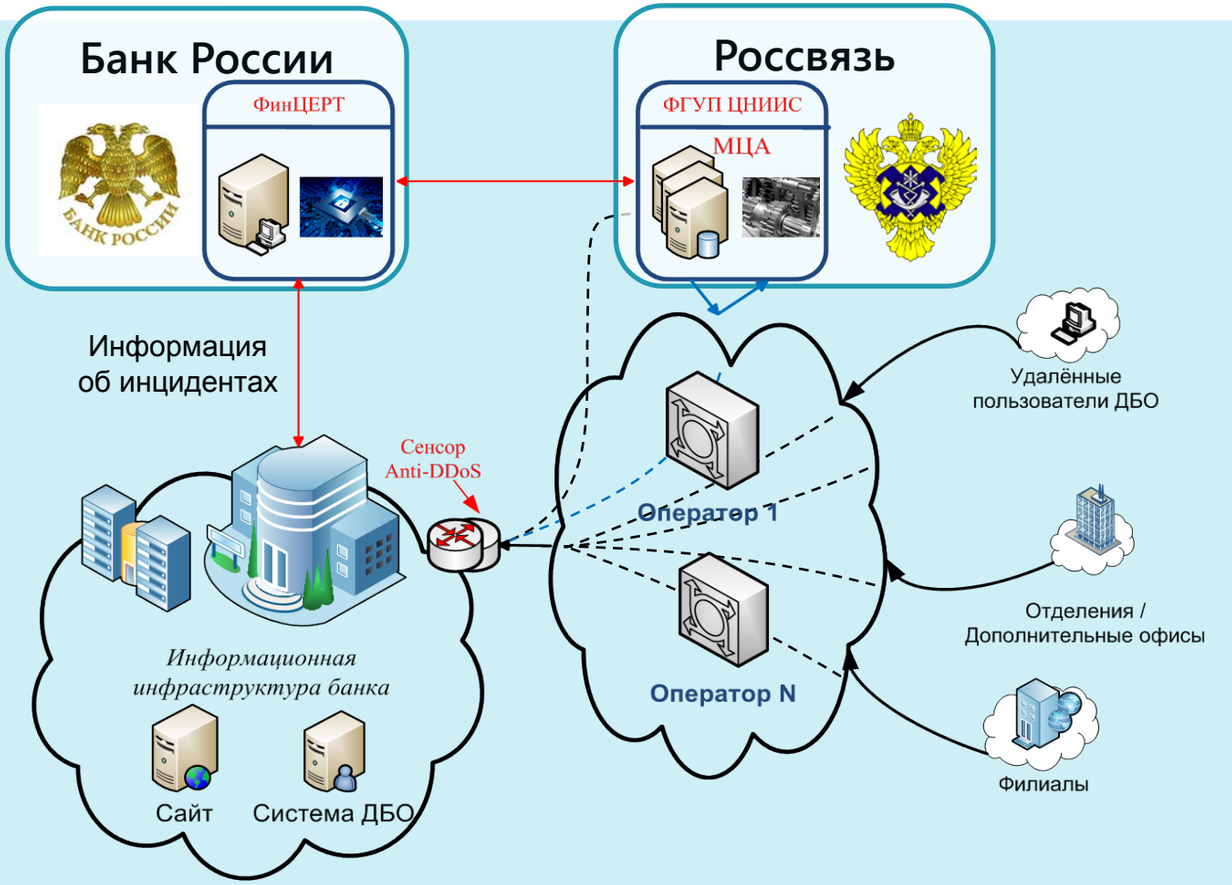
Результат для финансового рынка

- ✓ Проактивная защита от DDoS атак
- ✓ Повышение стабильности функционирования информационной инфраструктуры банка
- ✓ Повышение доступности и качества оказываемых услуг

Предложения по противодействию угрозам типа «В»

Вариант № 2 – фильтрация паразитного трафика по запросам

Штатный режим работы –
мониторинг угроз, анализ трафика
(в банк поступает «прямой» трафик)



При обнаружении DDoS атаки –
фильтрация трафика через МЦА
(в банк поступает «очищенный» трафик)

Вузы Россвязи как площадка для реализации различного уровня образовательных программ инженерно-технической направленности для представителей финансово-кредитных организаций

Россвязь – учредитель 4 вузов. Университеты находятся в Москве, Санкт-Петербурге, Самаре и Новосибирске. В их составе: 8 филиалов и 4 колледжа, от Хабаровска до Смоленска и от Ростова до Архангельска. Ежегодно обучается около 35 тысяч студентов по 32 направлениям подготовки и специальностям высшего образования и 15 направлениям среднего профессионального образования.

Учебные заведения обеспечивают подготовку высококвалифицированных кадров для страны в областях телекоммуникаций, информатики, радиотехники, управления и экономики. Подведомственные университеты имеют современную материально-техническую базу, позволяющую теоретические знания проверять на практике.

Среди направлений подготовки есть непосредственно связанные с информационной безопасностью и они востребованы абитуриентами.

Федеральное агентство связи
(РОССВЯЗЬ)

Благодарю за внимание!

www.rossvyaz.ru