



доклад на тему

«Доверенная информационная среда- в обеспечении технологической независимости и информационной безопасности Российской Федерации

МВТ Форум « Армия 2019»

Заседание Комитета по информационно-коммуникационным технологиям
Ассоциации «Лига содействия оборонным предприятиям»
на тему: «Вопросы создания защищенной информационной среды системы управления жизненным
циклом изделия на основе отечественного доверенного программного обеспечения»



Москва, 27 06 2019г.

Докладчик: Заместитель генерального директора АО НПО Молния Морозова А.А. ,
помощник депутата ГД ФС РФ Комитет по обороне Хохлова А.А



«АКТУАЛЬНОСТЬ»



Москва, 27 06 2019г.



УГРОЗЫ

Национальному суверенитету России

Стратегия США
национальной безопасности
военная доктрина стран НАТО

представленные

Ведущими производителями вооружений
(**Boeing, Lockheed-Martin, General Dynamics, Northrop Grumman, Sikorsky, Bell, BAe, Airbus, Eurocopter и пр**)

достижение глобального цивилизационного и
военного превосходства над
МИРОМ



УГРОЗЫ



Национальному суверенитету России

Стратегия национальной
безопасности США и военная
доктрина стран НАТО

- Технологии, не являющиеся объектом коммерческого оборота

➤ Комплекс базовых технологий и стандартов для ведения боевых действий с вероятным противником

- Технологии, являющиеся объектами коммерческого оборота

➤ Комплекс базовых технологий и стандартов для ведения боевых действий с вероятным противником



УГРОЗЫ



Национальному суверенитету России

Стратегия национальной
безопасности США и военная
доктрина стран НАТО

Ведущие страны – производители вооружений выделяют десятки миллиардов долларов ежегодно в развитие информационного пространства, в частности в создание

цифрового инжиниринга(ЦИ) на базе:

- физико-математических моделей
- инженерно-физических расчётов
- петафлопных вычислительных мощностей(СК)
- программного обеспечения(ПО)

**ЦЕЛЬ ЦИ - расчёт режимов управление ЖЦ ВВСТ
и объектами КИИ**



УГРОЗЫ

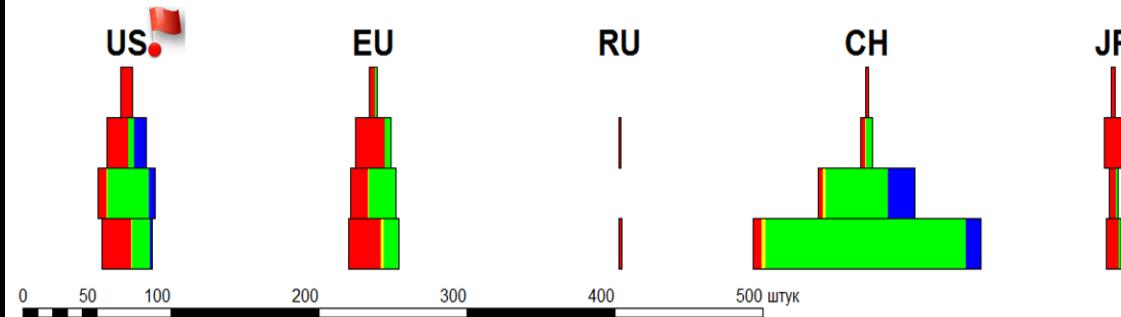


Национальному суверенитету России

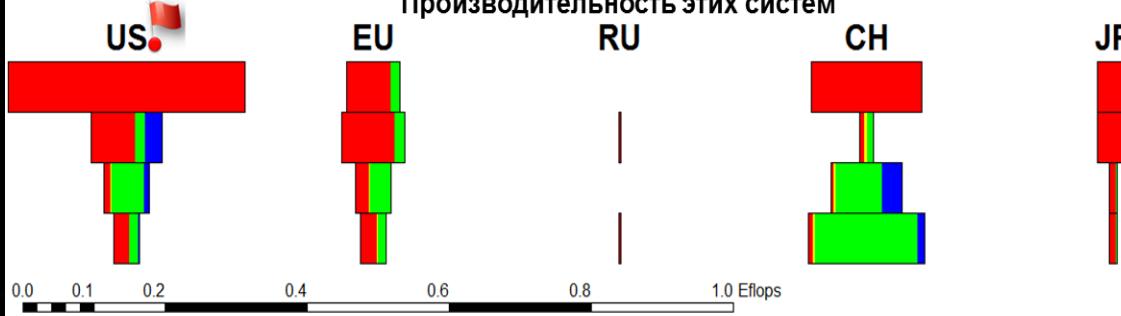
Стратегия национальной
безопасности США 2018г и военная
доктрина стран НАТО

Суперкомпьютерная киберинфраструктура США (US),
Евросоюза (EU), России (RU), Китая (CH) и Японии (JP), ноябрь 2018

Количество суперкомпьютерных систем высшего, высокого, среднего и младшего уровней



Производительность этих систем



ЦЕЛЬ СК - расчёт и управление ЖЦ ВВСТ и объектами КИИ

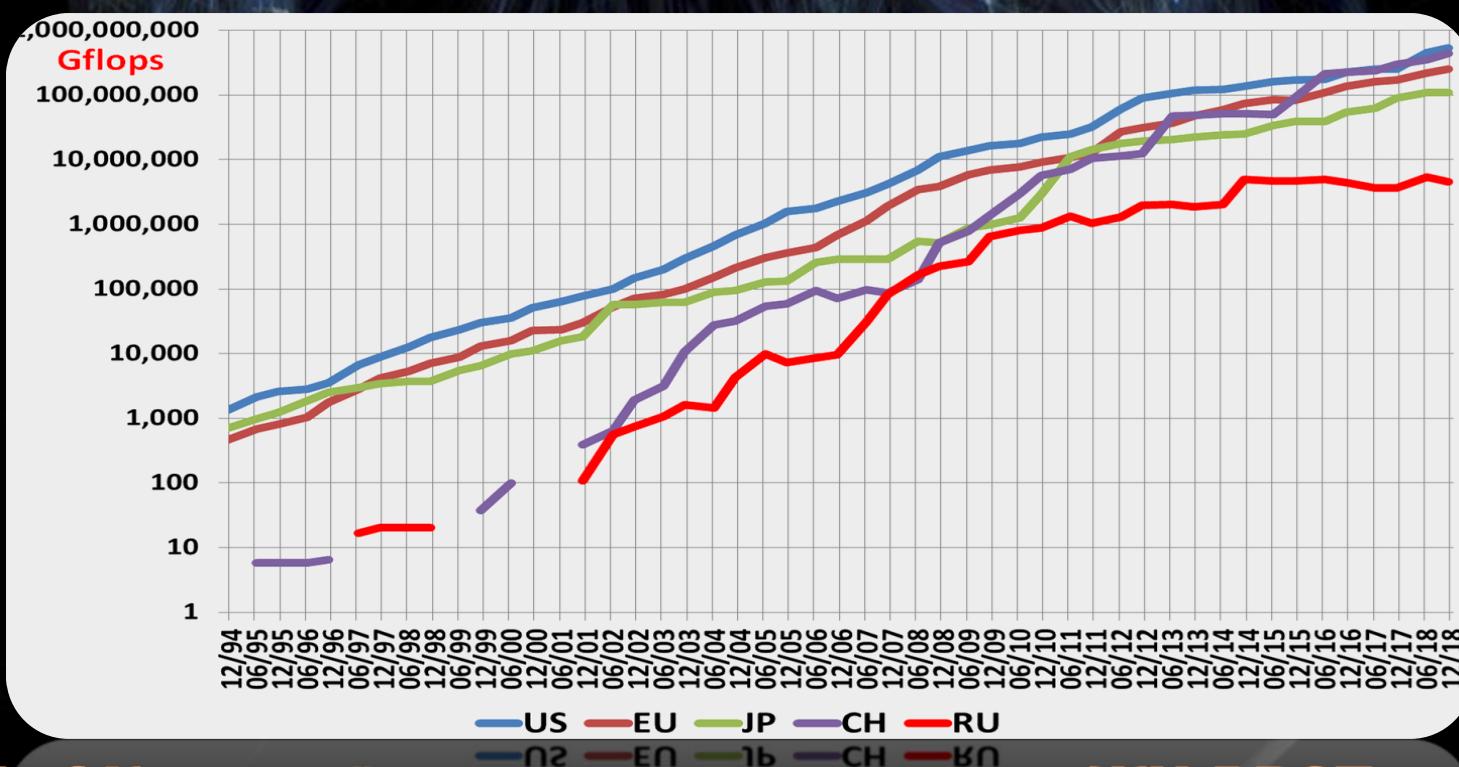


УГРОЗЫ



Национальному суверенитету России

Стратегия национальной
безопасности США 2018г и военная
доктрина стран НАТО



ЦЕЛЬ СК - расчёт режимов управления ЖЦ ВВСТ



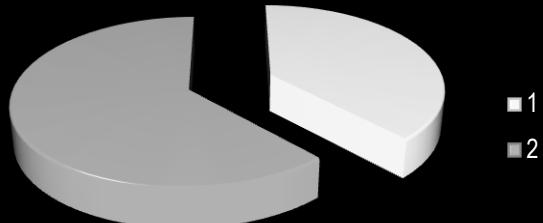
Национальному суверенитету России

**Текущее состояние проникновения зарубежных
цифровых технологий в российскую экономику в
разрезе происхождения**

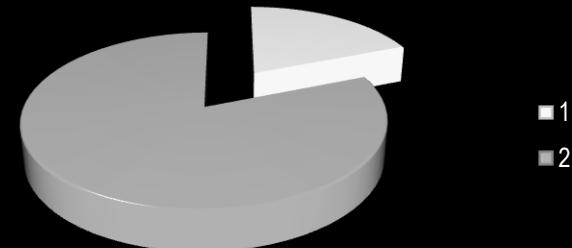
По числу закупок 2018г.
(555 един.)
Отечественные- 38 %
Зарубежные- 62%

По стоимости 2018г.
(всего 4, 5 млрд. един.)
Отечественные- 19 %
Зарубежные- 81%

кол-во закупок, ед.



кол-во закупок, руб.



ЦЕЛЬ ПО - расчёт режимов управления ЖЦ ВВСТ



УГРОЗЫ

Национальному суверенитету России

1. свыше 90% используемых информационно технологий принадлежат иностранным государствам, входящим в международное сообщество, осуществляющее экономические санкции против Российской Федерации;

2. зафиксирована зависимость на 100% от импортной электронной - компонентной базы, в том числе используемой, как при разработке ВВСТ, так и при создании объектов критической информационной инфраструктуры, обеспечивающей жизненный цикл вооружения , военной и специальной техники (далее ИКО ЖЦ ВВСТ).

**Стратегия национальной
безопасности США 2018г и военная
доктрина стран НАТО**

УГРОЗЫ

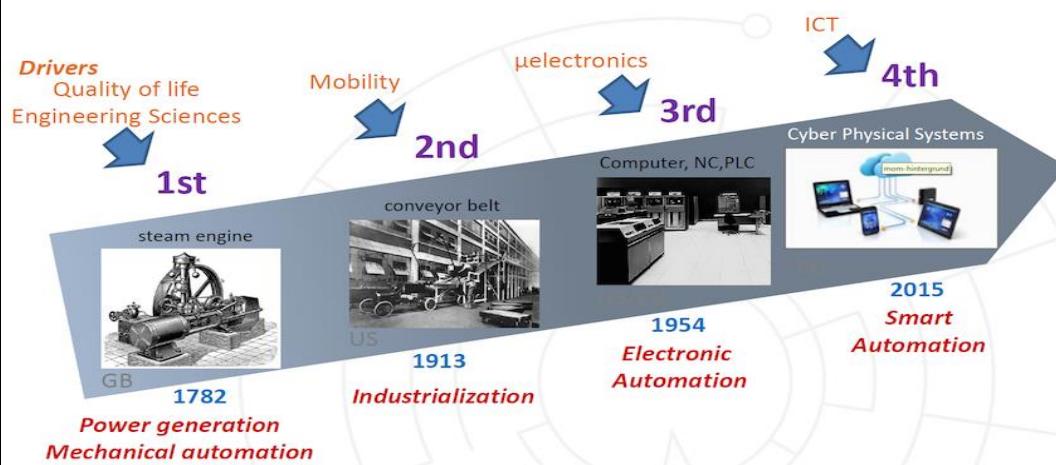
Национальному суверенитету России



- Технологии, являющиеся объектами коммерческого оборота

- Комплекс базовых технологий (в том числе ИКТ) и стандартов для ведения боевых действий на территории и руками вероятного противника (интернетизированная промышленность)

The 4th Industrial Revolution - „Industry 4.0“



(с 1954 г.) третья промышленная революция – цифровая революция, которая началась с использования электроники и информационных технологий для дальнейшей автоматизации производства.

(с 2015г.) четвертая промышленная революция – информационная революция , внедрение киберфизических систем и персонализированное производство (ИП).

Программа «Индустрии 4.0»
(Германия):

(с 1782г.) первая промышленная революция – механизация производства с использованием воды и мощности пара.

(с 1913г.) вторая промышленная революция – электрификация

а.

ЦЕЛЬ ИКО ЖЦ ВВСТ -управление ЖЦ ВВСТ

Стратегия национальной безопасности США 2018г и военная доктрина стран НАТО



УГРОЗЫ

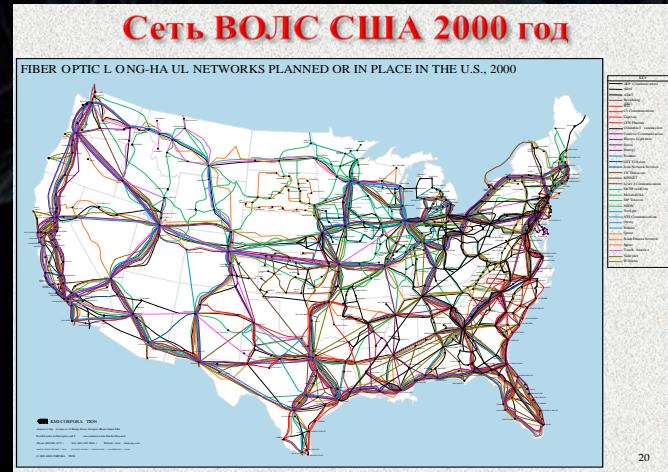
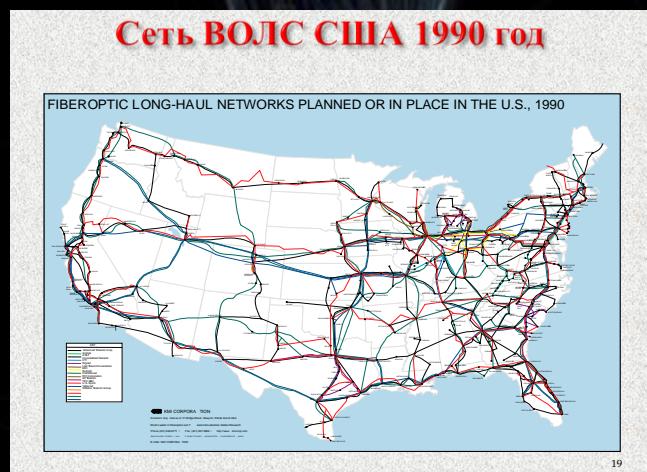
Национальному суверенитету России



Мировая тенденция в области индустриализации свидетельствует о том, что современные телекоммуникационные сети связывают между собою объекты ИКО, реализуя тем самым концепцию цифровизации экономики в целом и Интернета вещей (IoT) в частности.

Для этих сетей требуются Петабитные (10^{15}) компьютеры с Экзабитными (10^{18}) объемами памяти и линии передачи с Терабитными (10^{12}) скоростями передачи информации.

При этом фундаментом для реализации указанных тенденций является проводная сеть
волоконно - оптических кабелей (далее ВОЛС).



ЦЕЛЬ ИКО ЖЦ ВВСТ -управление ЖЦ ВВСТ



УГРОЗЫ



Национальному суверенитету России

**«... Серьезной угрозой безопасности России являются
возросшие возможности западных стран по ведению
наступательных операций в информационном пространстве и
готовность к их применению.**

**Сохраняется доминирование США и
ряда стран Европейского Союза**

в вопросах управления сетью интернет ...»

**Протокол заседания Совбез подписанный
Президента Российской Федерации
Владимиром Путиным от 5 ноября 2017г.**

«АКТУАЛЬНОСТЬ»



УГРОЗЫ



Национальному суверенитету России

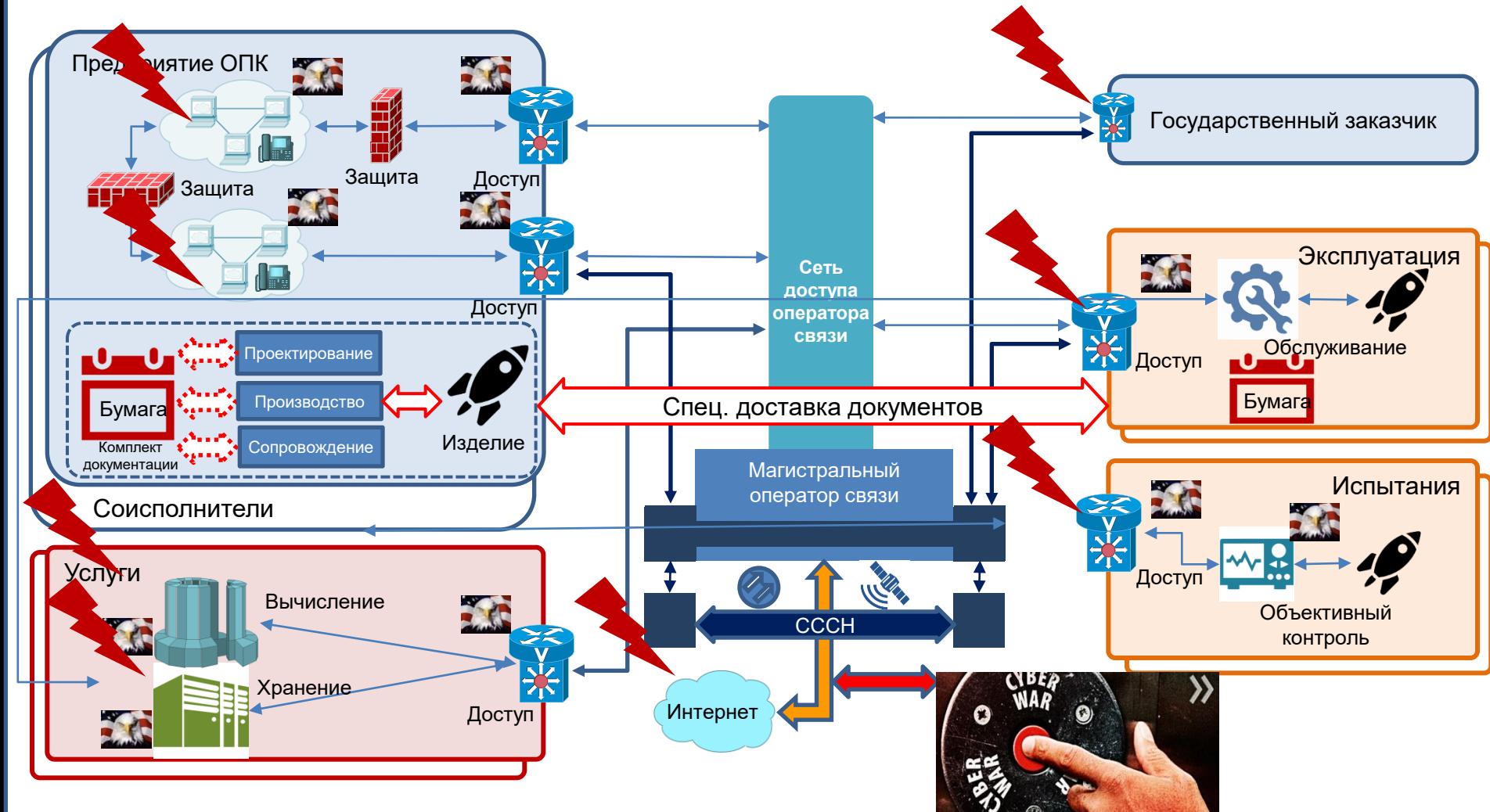
20 февраля 2019г
Президент России

Владимир Путин заявил на встрече с руководителями российских СМИ, что теоретически существует угроза отключения страны от мирового Интернета и нужно быть к этому готовым.



УГРОЗЫ

Национальному суверенитету РОССИИ





УГРОЗЫ

Утечка информации за счет побочных электромагнитных излучений и наводок на сети электропитания и заземления

Несанкционированный доступ к защищаемой информации, приводящий к нарушению ее конфиденциальности, целостности или доступности

Утечка информации за счет возможно внедренных в технические средства закладок, предназначенных для негласного получения информации

Нарушение требований организационно-распорядительной документации



УГРОЗЫ

Аппаратные:

- процессоры зарубежного производства содержат не декларируемые аппаратные команды управления и каналы доступа
- другие аппаратные компоненты, инж.- тех. системы иностранного производства имеют возможность несанкционированного отключения электропитания, не декларируемые возможности по управлению

Программные:

- искажение или удаление программных компонентов;
- внедрение и использование неучтенных программ;
- изменение и уничтожение программных компонентов;
- Заражение вредоносным программным обеспечением

Сетевые:

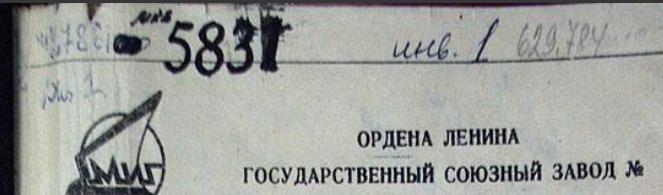
- прослушивание и подмена трафика;
- блокировка доступа;
- отказ в обслуживании;
- Изменение маршрутизации, системы доменных имен



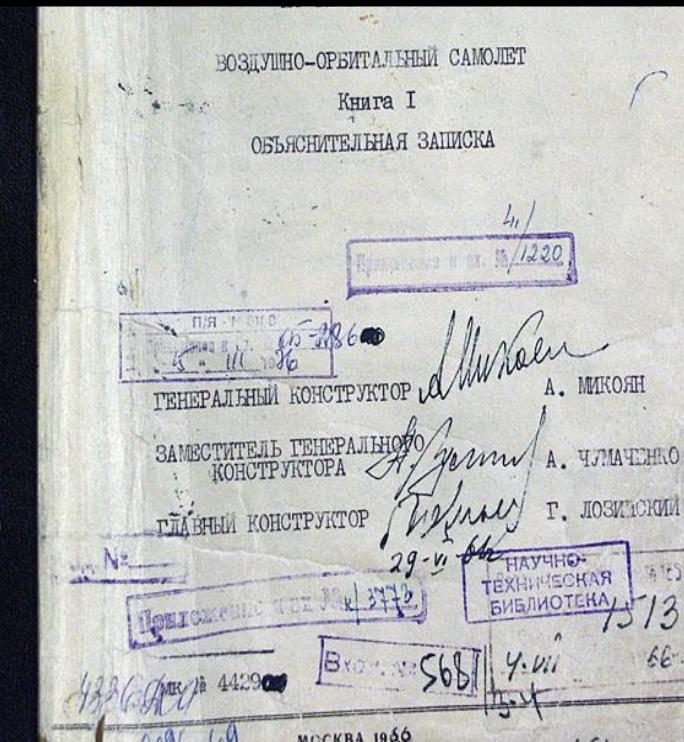
«СУЩЕСТВУЮЩИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЗАДЕЛ»



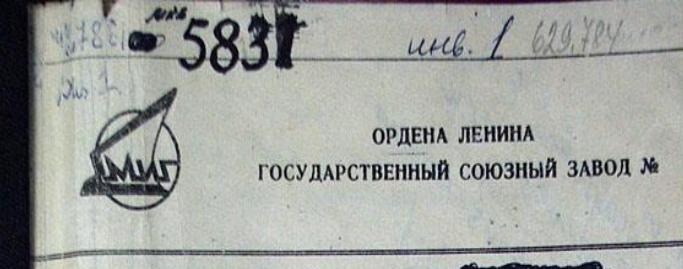
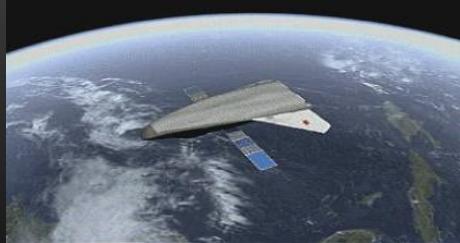
Москва, 24 04 2019г.



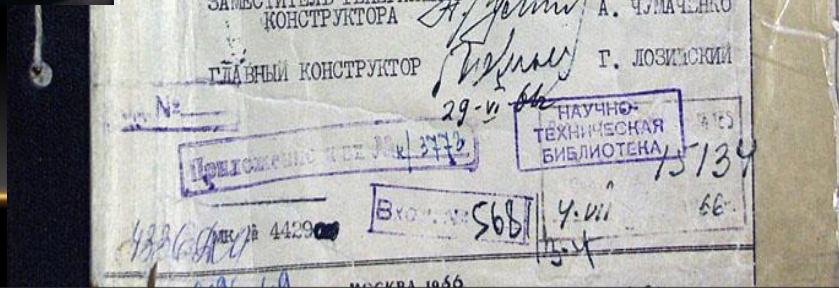
Наша промышленность и наука уже в 1988-м году успешно реализовала задачу, по масштабу подобную той, что содержится в послании Президента Федеральному Собранию РФ и в Национальной программе «Цифровая экономика Российской Федерации», развернув разработку транспортно-космической системы «Энергию-Буран» на более чем 1200 предприятиях по всему Советскому Союзу



«СУЩЕСТВУЮЩИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЗАДЕЛ»



Полёт КК «Буран» с последующим успешным приземлением в полностью автоматическом режиме 15 ноября 1988 г. явился высочайшей оценкой созданной системе взаимодействия участников проекта благодаря государственной политике в области науки и промышленности.



«СУЩЕСТВУЮЩИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЗАДЕЛ»



ролик



Москва, 24 04 2019г.



«ПУТИ РЕШЕНИЯ»



Москва, 24 04 2019г.



Национальный суверенитет России

**«...Сегодняшние решения определяют судьбу России
на десятилетия вперед.**

**Скорость технологических изменений
нарастает стремительно.**

**И тот, кто использует эту технологическую волну,
вырвется далеко вперед...»**

**послание Президента Российской Федерации
Владимира Путина Федеральному Собранию
от 1 марта 2018г.**

«ПУТИ РЕШЕНИЯ»



Национальный суверенитет России

«... Цифровая инфраструктура – это комплекс технологий и построенных на их основе продуктов, обеспечивающих вычислительные, телекоммуникационные и сетевые мощности, работающих на цифровой основе ...»

Программа « Цифровая экономика
Российской Федерации»
от 28 июля 2017г. №1632-р

«ПУТИ РЕШЕНИЯ»



Тесис



НПК «Сетецентрические платформы»



РЕМЕХ **ADEM**
CAD/CAM/CAPP/PDM
АСКОДА АПМ



**МЦСТ
ЭЛЬБРУС**



ИНЭУМ



ИТЦ НПО ПМ

РЕШЕТНЕВ
АО «ИСС»

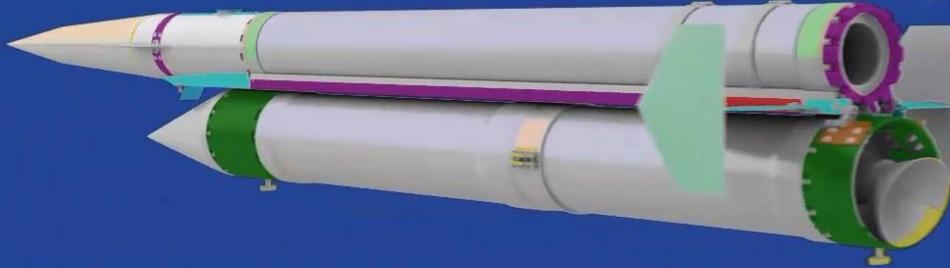


масштаб
научно-исследовательский институт

ЮРИОН
Научно-технический центр®



«ПУТИ РЕШЕНИЯ»



Ракета-мишень «Гвоздика»



Ваш ролик
«ПУТИ РЕШЕНИЯ»



Отечественные суперкомпьютеры в Топ500 Роль и место ИПС имени А.К.Айламазяна РАН

No	Дата	Tflops.	Суперкомпьютер	Разработчик
13	14 2014/11	170	PetaStream СПбГПУ	Имеется РКД, литер О    

Системы
специального назначения

Инженерное ПО

Системы электронного
документооборота

Системы поддержки
принятия решений (СППР)

Системы защиты
информации

Системы коммуникаций и
работы в Интернете и др.

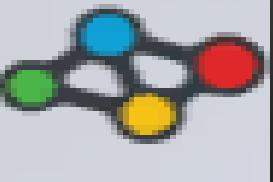
«ПУТИ РЕШЕНИЯ»



- наличие собственных, не зависящих от иностранных производителей, базовых репозиториев программных пакетов и исходных текстов программ;
- локализованный в пределах предприятий, находящихся в российской юрисдикции, жизненный цикл разработки ОС;
- уникальные разработки в области методики переноса дистрибутивов ОС на новые аппаратные платформы;
- многолетний опыт успешного участия в международных и отечественных сообществах разработчиков средств обеспечения безопасности ОС;
- многолетний успешный опыт эксплуатации ОС Альт в условиях повышенной нагрузки на средства защиты информации;
- политика открытого кода собственных разработок и непосредственного участия в проектах разработки базового открытого ПО;
- политика открытости по отношению к сторонним разработчикам, участвующим в развитии платформы;
- прозрачность и открытость в части публикации технической информации о дистрибутивах ОС Альт и базовых технологиях, на которых они построены.

ИСПОЛЬЗУЮТ ОС АЛЬТ И СУБД POSTGRES





НПК «Сетецентрические платформы»



Единая многоуровневая мультиагентная сетецентрическая платформа для управления в реальном времени



1

Актуальность

Мощное развитие цифровых технологий, рост данных о внутренних и внешних бизнес-факторах стремительно меняет клад традиционных производственных иерархий и парадигму управления:

- Требуется в режиме реального времени адаптивно поддерживать актуальность и достоверность планов как реакцию на возникающие новые события из задачи;
- Скорость и достоверность решения становятся ключевыми факторами победы;
- Сетецентризм ИТ-систем переходит в реальное организационное управление.

Раньше:
Дни и месяцы для
ручной разработки
планов и подготовки
решения

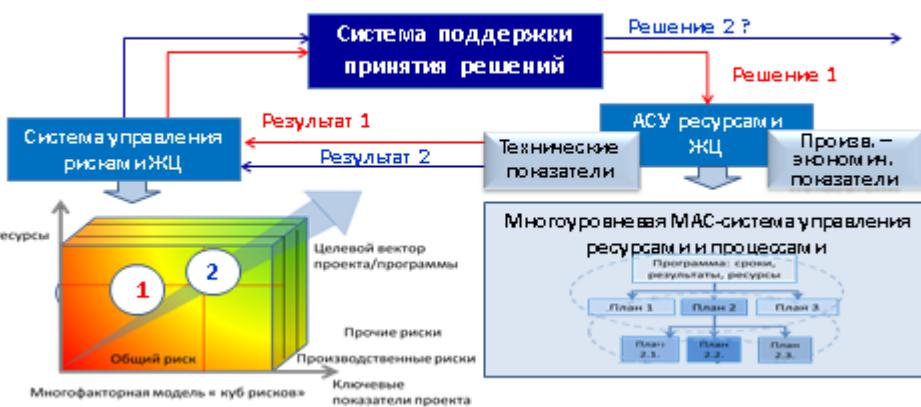
Вчера:
Десятки часов на расчет
планового решения.
SAP – лидер управления и
линейного программирования

Наступающее сегодня:
Минуты для
достоверного и
точного решения

Ключевая проблематика систем –
низкая достоверность и точность планов
во времени

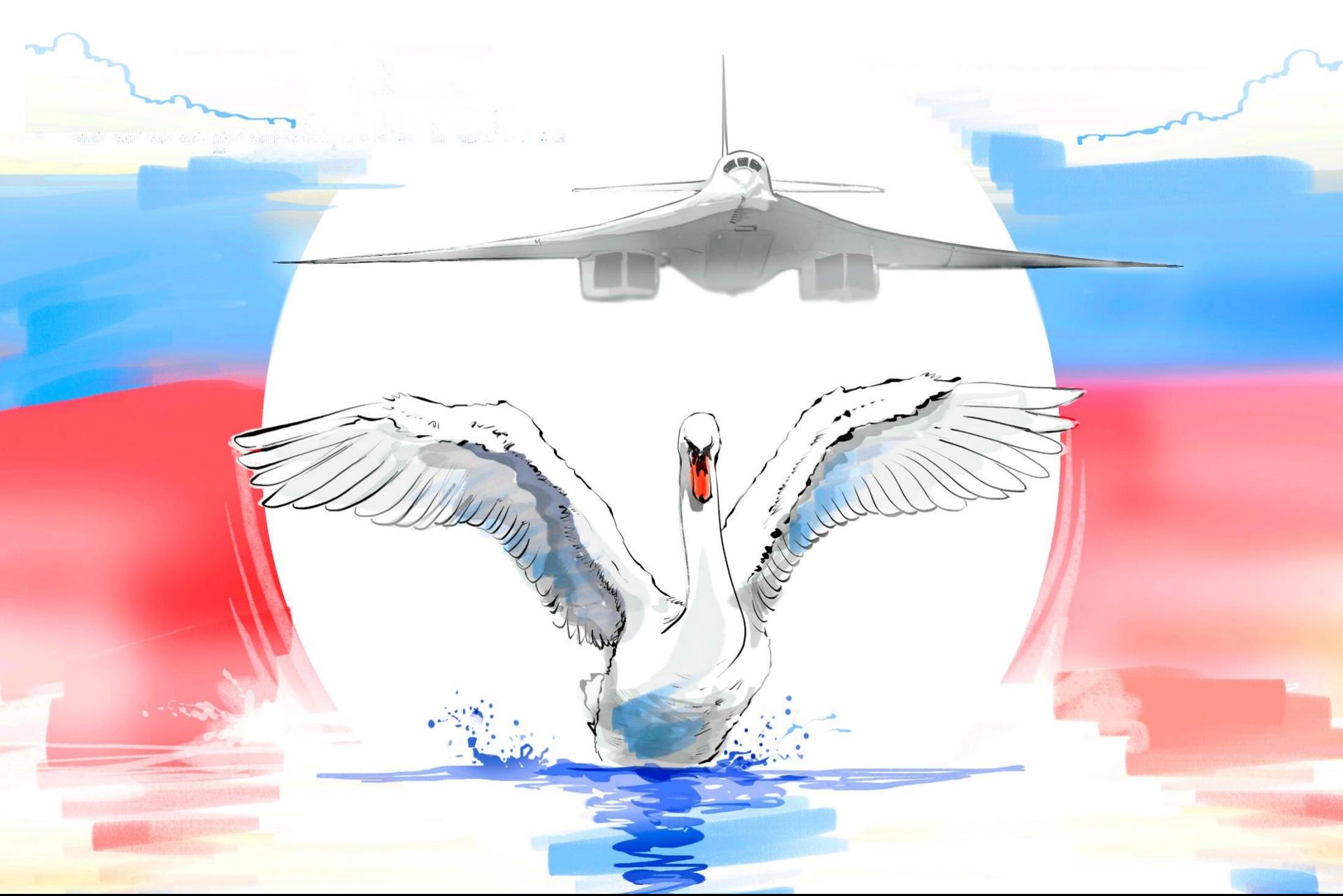


Переход к непрерывному управлению в реальном времени целями, рисками и результатами

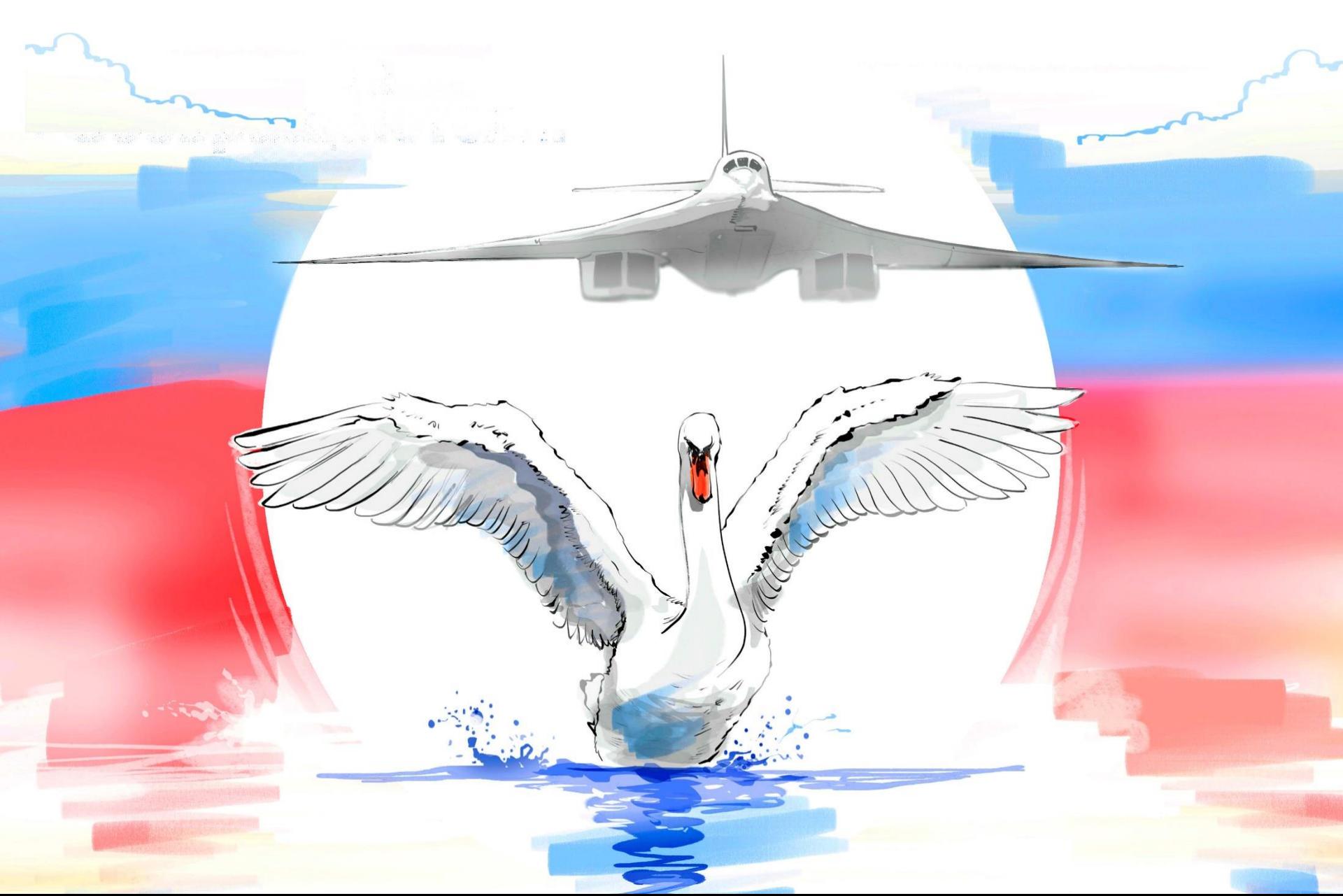


2

«ПУТИ РЕШЕНИЯ»



ролик



«ПУТИ РЕШЕНИЯ»



РЕШЕНИЕ К ОБСУЖДЕНИЮ

Москва, 24 04 2019г.

Модератор: Заместитель генерального директора АО НПО Молния Морозова А.А.