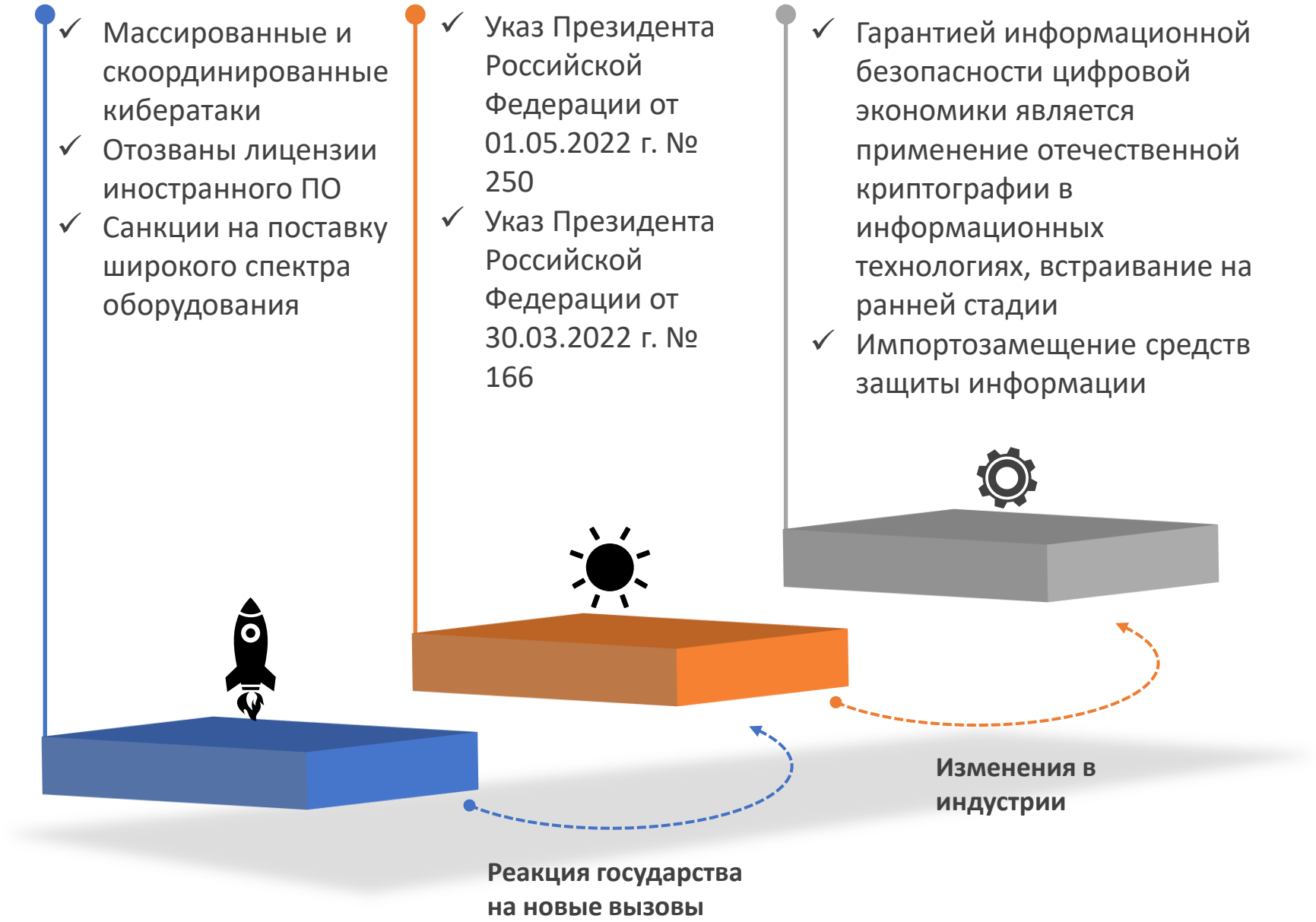
# Криптография и технологическая независимость

А.М. Шойтов
Заместитель министра Минцифры России
Президент Академии криптографии
Российской Федерации

Март 2023

# Основные вызовы и события по ИБ за 2022



# Криптография по итогам 2021

В рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» Академией Криптографии завершено 16 НИР в области криптографии.

Исследование криптографических механизмов идентификации и аутентификации

Сформирован комплексный подход к обеспечению ИБ в облачных платформах

Исследование криптографических алгоритмов защиты информации платежных систем

Исследование криптографических механизмов и протоколов, применяемых в системах беспроводной связи

Исследование криптографических механизмов и протоколов, применяемых в системах, использующих технологии искусственного интеллекта

Исследование криптографических методов защиты информации квантовых вычислительных систем

# Предпосылки к созданию АНО НТЦ ЦК: необходимость эффективных решений в области разработки и внедрения защищенных информационных технологий

## Недостаток компетенций

Отсутствие у функциональных заказчиков компетенций для формулировки требований по информационной безопасности

## Длительные сроки сертификации

Длительный процесс сертификации средств защиты информации и аттестации автоматизированных систем в защищенном исполнении (в том числе при обновлении программного обеспечения или доработки)

## Нехватка обеспечения

Неоднородность компетенций лицензиатов и их недостаточная аппаратная и инструментальная обеспеченность

## Отсутствие совместимости

Несовместимость реализации одинаковых криптографических механизмов, выполненных различными разработчиками

# Эскиз экосистемы АНО НТЦ ЦК

**Сервис разработки технологий**
- Совместная разработка технологий
- Распоряжение правами на интеллектуальную собственность

**Техническая инфраструктура**
- Тестирование разработок
- Независимое тестирование
- Сравнительный анализ на основании передовых методик

**Коммуникационные сервисы**
- Взаимодействия между разработчиками
- Взаимодействия между разработчиками и потребителями
- Проведение консультаций с независимыми экспертами

**Банк программного и аппаратного обеспечения**
- Функциональное тестирование на различных программно- аппаратных платформах.
- Встречное тестирование с участием поставщиков

**Витрина разработок**
- Поиск актуальных разработок
- Результаты независимого тестирования
- Анонсы предстоящих релизов
- Сервис пробной эксплуатации

**Сервис управления развитием**
- Размещение запросов по характеристикам перспективных разработок.
- Доведение запросов до разработчиков.

# Учредители АНО «Национальный технологический центр цифровой криптографии» и стратегические цели организации

Организация создается в целях предоставления услуг в сферах исследования безопасности информационных технологий, в том числе с применением криптографических алгоритмов и механизмов, проектирования, создания, доведения до практической реализации, распространения и гармонизации отечественных решений по обеспечению информационной безопасности информационных технологий, в том числе с применением криптографических алгоритмов и механизмов

**Российская Федерация,**
**Полномочия учредителя осуществляет:**

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

infotecs

КРИПТОПРО

КОД безопасности

## Стратегические цели

- Исследование безопасности информационных технологий
- Проведение фундаментальных, поисковых и прикладных исследований в области разработки доверенных информационных технологий
- Разработка криптографических алгоритмов и механизмов
- Проектирование и создание отечественных решений по обеспечению информационной безопасности информационных технологий
- Распространение и гармонизация отечественных решений по обеспечению информационной безопасности информационных технологий

# Наблюдательный совет АНО «Национальный технологический центр цифровой криптографии»

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Минцифры России

МИНПРОМТОРГ РОССИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Банк России

Российская Академия Наук

Московский государственный университет имени М. В. Ломоносова

ЦЕНТР КОМПЕТЕНЦИЙ ПО ИМПОРТОЗАМЕЩЕНИЮ В СФЕРЕ ИКТ

infotecs

КРИПТОПРО

КОД безопасности

# Задачи Федерального проекта Информационная безопасность Национальной программы Цифровая экономика Российской Федерации решаемые в АНО НТЦ ЦК

## Разработанные решения криптографической защиты

Количество разработанных решений с внедренными механизмами криптографической защиты для использования в ключевых отраслях экономики (2023 г. - 3 шт, 2024 г. - 3 шт)

## Научно-техническая база

- созданы лаборатории по научно-практическим направлениям перспективных исследований и внедрения механизмов криптографической защиты информации, инфраструктура для взаимодействия научного сообщества и разработчиков цифровых технологий с государственными регуляторами в области защиты информации;
- введены в эксплуатацию технические средства, предназначенные для моделирования информационных систем, макетирования безопасного исполнения цифровых технологий, в том числе с применением методов и средств криптографической защиты информации, хранения репозитория криптографических примитивов.

## Разработки решений информационной безопасности

Разработаны отечественные решения в области информационной безопасности информационных технологий, в том числе с применением криптографических алгоритмов и механизмов.

## НИР и ОКР

Проведены научно-исследовательские и опытно-конструкторские работы, направленные на решение научно-практических задач внедрения методов современной криптографии в цифровых технологиях.

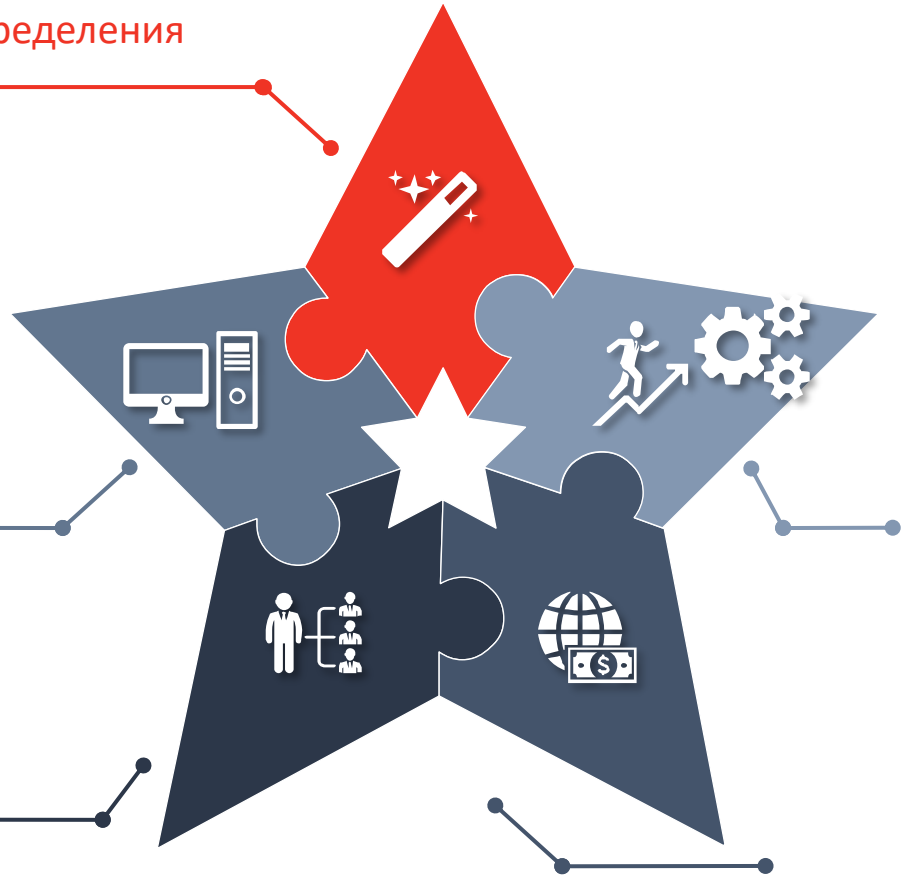
## Координация деятельности

Обеспечена координация деятельности научного сообщества и разработчиков цифровых технологий в области защиты информации в целях обеспечения внедрения методов современной криптографии в цифровых технологиях.

# Планируемая инфраструктура АНО НТЦ ЦК

Лабораторный комплекс по исследованию заявленных свойств систем квантового распределения ключа

Лабораторный комплекс по исследованию, разработке, изготовлению, сопровождению и сертификации специализированных микропроцессоров, реализующих в своем составе аппаратные средства защиты



Центр по унификации программно-аппаратных комплексов, телекоммуникационного оборудования и его программного обеспечения, разрабатываемых с использованием технологии квантового распределения ключей и лаборатория - структурное подразделение организации содействия развитию отечественной криптографии:

- УЦ для TLS-сертификатов
- УЦ для подписи кода ПО
- УЦ для выдачи сертификатов абонентских устройств
- Центр эмиссии абонентских устройств
- ПАК для тестирования отечественных СКЗИ

Спецвычислитель на базе НИВЦ МГУ (защищенная инфраструктура для проведения удаленными пользователями открытых экспериментальных исследований в области информационной безопасности)

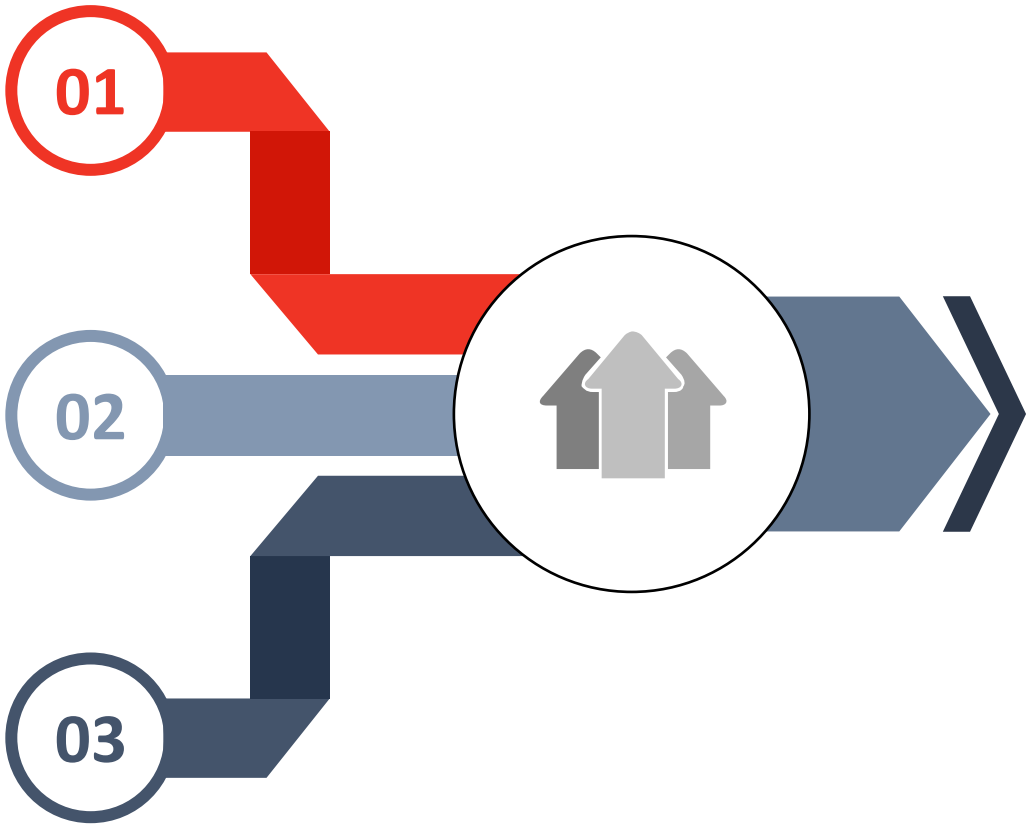
Проектирование, внедрение, аттестация ИС Национальный мультисканнер, включая построение инфраструктуры и разработку прикладного программного обеспечения

# Механизмы работы инфраструктуры

**Формирование спроса на отечественные СКЗИ**

**Формирования технологических условий для внедрения и распространения отечественной криптографии**

**Содействие внедрению технологий, созданных научными коллективами, в промышленность**




- ✓ Поиск стратегических заказчиков
- ✓ Выбор классов продуктов для внедрения отечественных криптографических механизмов
- ✓ Формирование стимулирующих условий для заказчиков, производителей и потребителей
- • Реестр криптографических решений готовых для внедрения в отечественные ИКТ
- • Постанова задач разработкам криптографических решений
- ▪ Постановка актуальных научных задач
- ▪ Подбор научных коллективов для решения актуальных научных задач
- ▪ Информационные поддержка, включая издание периодического специализированного журнала
- ▪ Внедрение научных разработок в производство
- ▪ Содействие с участием институтов развития и венчурных фондов коммерциализации результатов научных коллективов и полученных на их основе продуктов

# Первоочередные направления работ АНО «Национальный технологический центр цифровой криптографии»

## 1 Электронная подпись

Технологии обеспечения общедоступности для граждан Российской Федерации применения усиленной квалифицированной электронной подписи

## 2 Криптографическая защита

Технологии обеспечения взаимозаменяемости и совместимости средств криптографической защиты информации, используемых в информационных системах цифровой экономики

## 3 Квантовая криптография

Технологии анализа безопасности и сертификации средств квантовой криптографии в целях их внедрения в государственные и частные информационные системы и телекоммуникационные сети

## 4 Обезличивание массивов

Математически обоснованные безопасные технологии обезличивания массивов персональных данных с использованием технологий искусственного интеллекта

## 5 Безопасная микроэлектронника

Технологии безопасного использования микроэлектронных изделий в средствах защиты информации

## 6 Безопасное сопряжение

Законченные общедоступные технологические решения для безопасного подключения/сопряжения различных информационных систем (адаптеры подключения к ЕСИА, НСУД и т.д.)

## 7 Безопасные библиотеки

Технологии создания библиотек (SDK) для применения в мобильных и WEB-приложениях с целью поддержки отечественных криптографических алгоритмов (TLS с ГОСТ, OpenID Connect и т.п.)

# Что будет результатом работы АНО НТЦ ЦК?

**Наш продукт: Решения для Цифровой экономики**

Позитивное изменение IT ландшафта


Стабильный интенсивный рост ИБ индустрии

# Каналы внешних коммуникаций АНО НТЦ ЦК

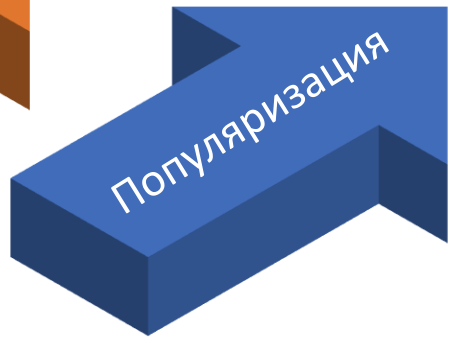
# Перспективные области для сотрудничества АНО НТЦ ЦК на 2023


Аналитика мировых тенденций развития науки и техники, а также рынка информационно-коммуникационных технологий. Разработка прогнозов в области информационной безопасности и ИТ.


Предоставление научно-технической и экспериментальной инфраструктуры разработчикам ИТ и СЗИ для проведения вычислений и моделирования работы объектов информатизации.


Проведение фундаментальных, поисковых и прикладных исследований в области разработки доверенных информационных технологий.

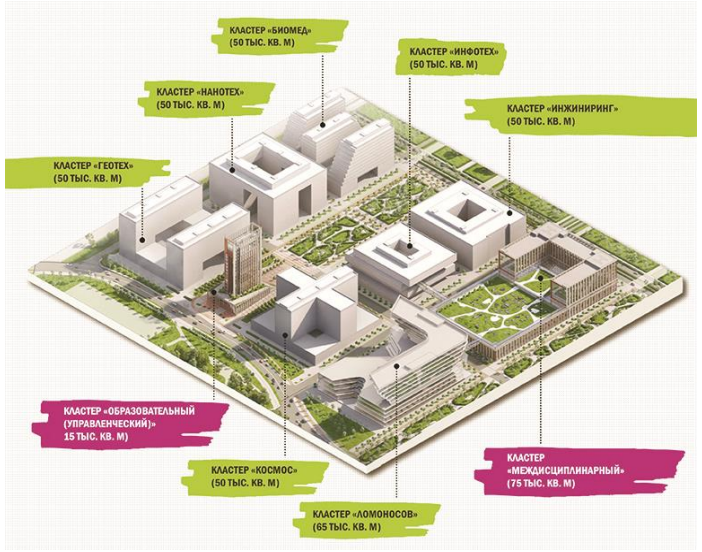

Тестирование СЗИ, в том числе на соответствие заявленным характеристикам, а также на их совместимость друг с другом.




Популяризация достижений отечественной цифровой криптографии для ИТ и ИБ отраслей, учащихся и широкого круга потребителей электроники.

# АНО НТЦ ЦК как участник проекта ИНТЦ МГУ «Воробьевы горы»

Информационные технологии и математическое моделирование: локализация в ИНТЦ МГУ «Воробьевы горы»




**Форум «Цифровая экономика: технологии доверенного искусственного интеллекта»**

*Москва, Кластер «Ломоносов», 25 мая 2023 г.*

Инфраструктура и оборудование для пилотирования научных решений на базе ИНТЦ

Налоговые льготы, предоставляющие дополнительные возможности для инвестирования в новые разработки и технологии

Комплекс лабораторий МГУ имени М.В.Ломоносова, доступных для резидентов

Научная экспертиза от профессорского состава университета