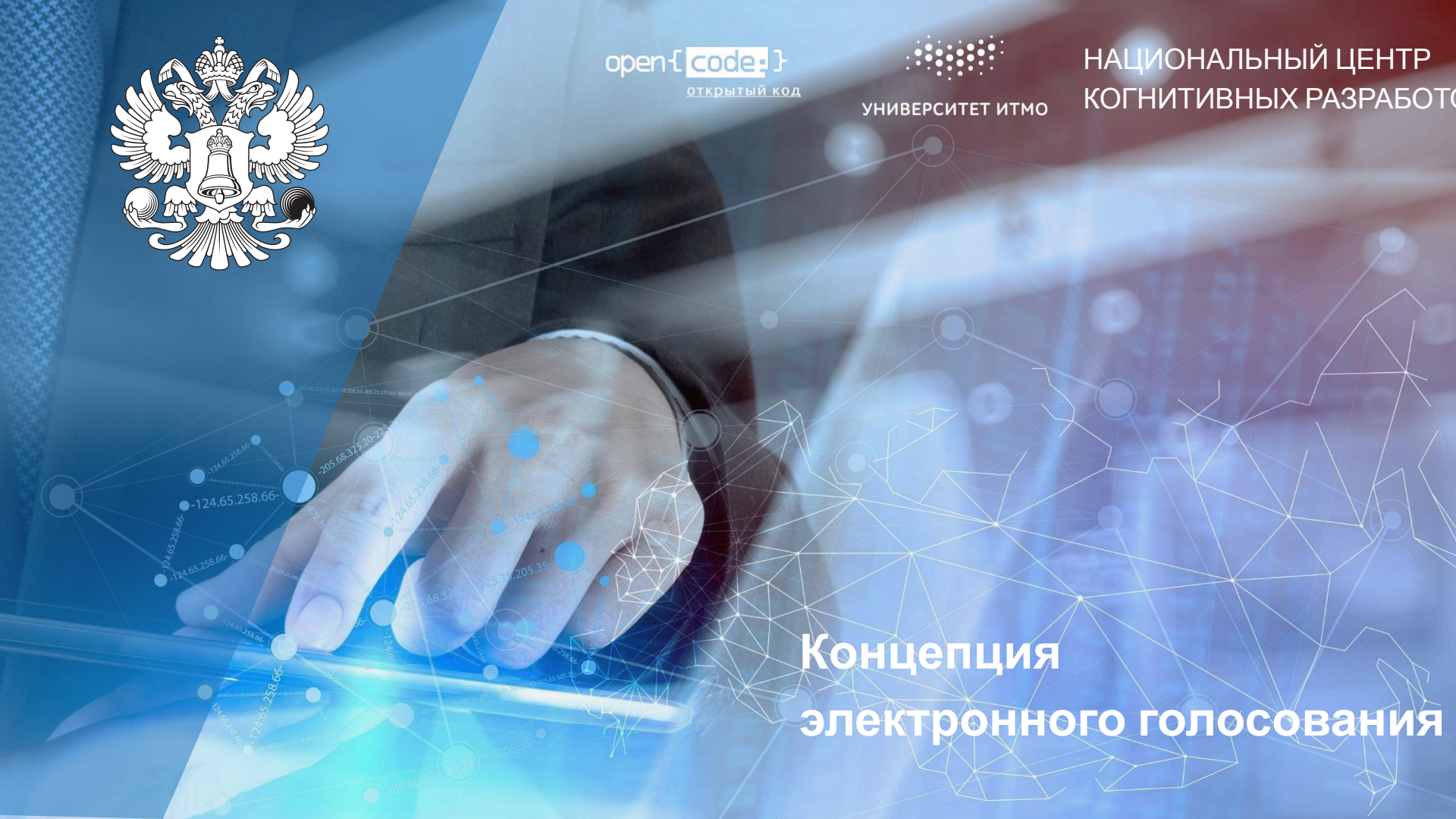


Концепция электронного голосования

Концепция – результат совместной работы

НАЦИОНАЛЬНЫЙ ЦЕНТР КОГНИТИВНЫХ РАЗРАБОТОК

УНИВЕРСИТЕТ ИТМО

open{ code: }
открытый код

Основные элементы концепции

Центральное понятие – электронное голосование, стратегической целью которого является обеспечение избирательных прав граждан без необходимости обращения на избирательные участки

Условия ее реализации – доступ гражданина в момент голосования к сети Интернет и подтвержденная учетная запись на портале государственных услуг

Составные части предлагаемой системы:

- Электронные средства голосования
- Электронные средства подсчета голосов

Основополагающие принципы концепции

- Обеспечение всеобщего и прямого избирательного права
- Гарантия тайны голосования
- Поддержка свободного и добровольного участия граждан
- Доступность сервиса
- Устранение рисков вмешательства в процесс
- Безопасность персональных данных
- Прозрачность всех технических процессов

Схема реализации идеи электронного голосования №1 (без возможности присутствия избирателей на ИУ)

Верхний уровень

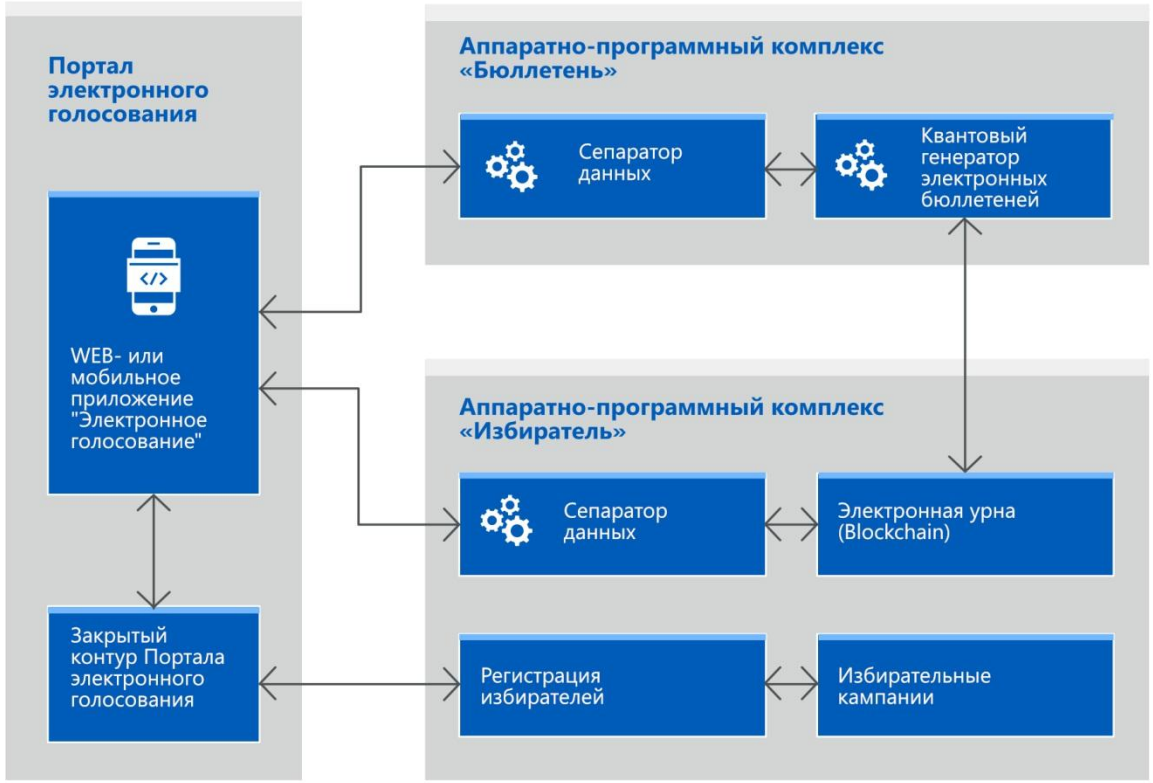
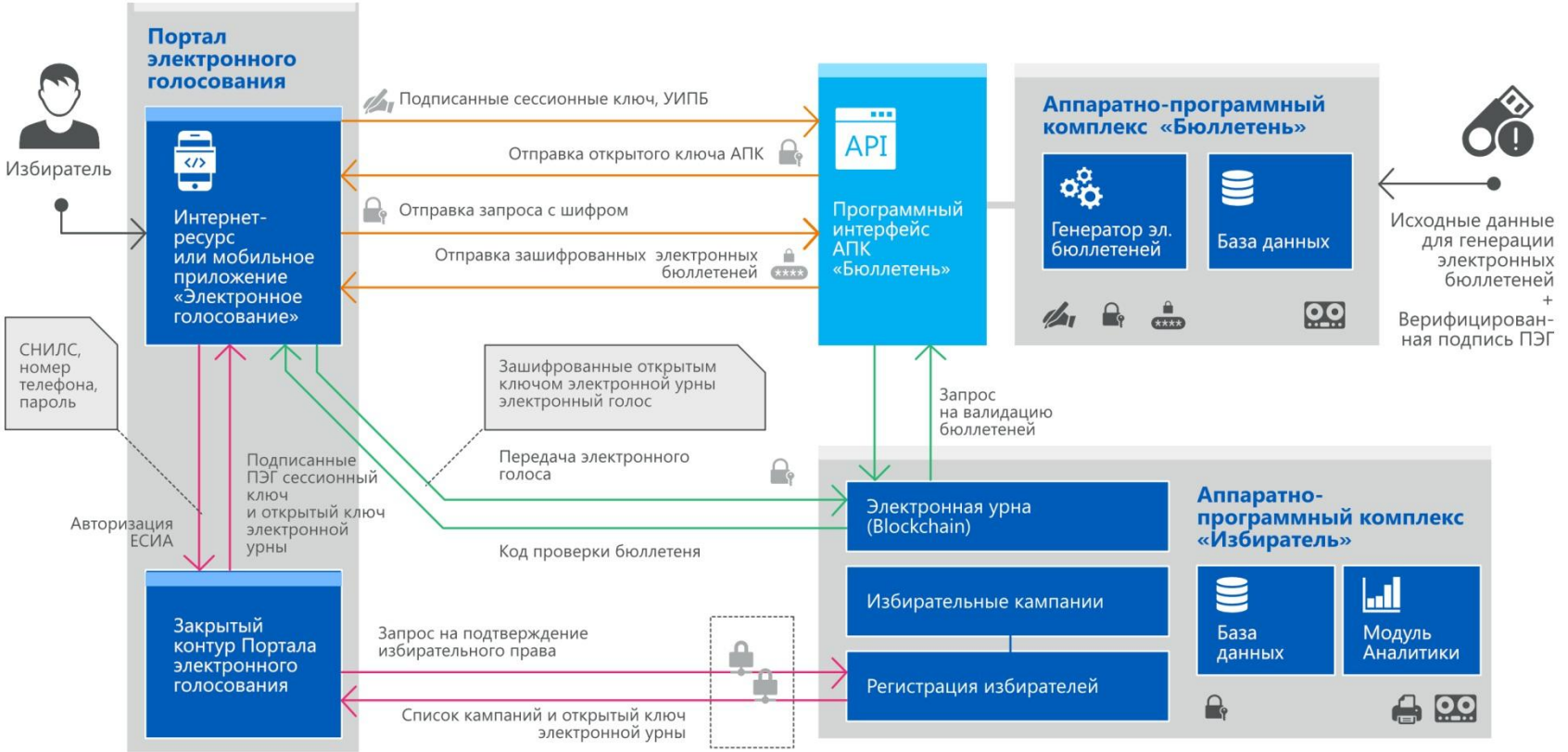


Схема реализации идеи электронного голосования №1 (без возможности присутствия избирателей на ИУ)



Сценарий электронного голосования для избирателя по схеме №1

- Авторизация пользователя после прохождения автоматически генерируемого теста-проверки
- Создание индивидуального пароля доступа к электронным бюллетеням
- Создание криптографического ключа (шифра) на основе биологического датчика случайных чисел (или сканера отпечатка пальца, сетчатки глаза)
- Голосование:
  - Получение электронных бюллетеней
  - Выбор избирательной кампании
  - Выбор и передача голоса
  - Сохранение результата
- Получение кода проверки учета голоса

Состав Портала электронного голосования (ПЭГ)

Закрытый контур ПЭГ обеспечивает взаимодействие с АПК «Избиратель»:

- для подтверждения избирательного права конкретного гражданина,
- для обеспечения работы менеджера распределенных транзакций.

Открытый контур ПЭГ – это web- или мобильное приложение «Электронное голосование», обеспечивающее непосредственно процесс голосования:

- получение электронного бюллетеня;
- осуществление обезличенного волеизъявления.

Задачи АПК «Избиратель»

- Агрегирование данных обо всех избирательных кампаниях.
- Обеспечение проверки на наличие активного избирательного права у конкретного гражданина.
- Прием и обработка электронных бюллетеней для голосования.
- Формирование аналитических и статистических срезов
- Формирование итоговых протоколов электронного голосования.
- Обеспечение защиты от попыток «вбросов» электронных бюллетеней для голосования.
- Ведение учета проведения электронного голосования, дублирующегося на физическом носителе информации.

Состав АПК «Избиратель». Программная часть

- ИС «Регистрация избирателей» обеспечивает учет использования избирательного права гражданином, формирует аналитические и статистические данные по различным срезам.

- ИС «Избирательная кампания» обеспечивает хранение, обработку и передачу информации об избирательных кампаниях в разрезе избирательных участков.

- ИС «Электронная урна» обеспечивает прием, проверку и обработку поступающих электронных бюллетеней для голосования; ведет анонимный учет поступающих результатов электронного голосования, дублирующийся на физический носитель информации; формирует протоколы об итогах электронного голосования с применением технологии Blockchain.

Состав АПК «Избиратель». Аппаратная часть

Сепарация данных поступающих к АПК запросов:

- очистка цифрового сигнала от шумов при чтении,

- выделение данных для последующей их обработки в системе «Электронная урна».

Задачи АПК «Бюллетень»

- Формирование электронных бюллетеней на основе данных о кампании и избирательном участке.
- Адресная выдача электронного избирательного бюллетеня гражданину.
- Обеспечение анонимного учета выданных бюллетеней на программном и аппаратном уровнях.
- Обеспечение проверки на валидность данных, поступающих в процессе электронного голосования.
- Ведение учета выданных бюллетеней, дублирующегося на физическом носителе информации.

Состав АПК «Бюллетень». Программная часть

Программный интерфейс АПК «Бюллетень»

- отвечает за приём и обработку поступающих от избирателей запросов на выдачу электронных бюллетеней,
- поддерживает аутентификацию источника поступления запроса,
- участвует в организации симметричного и асимметричного шифрования,
- обеспечивает контроль выдачи повторных бюллетеней.

Состав АПК «Бюллетень». Аппаратная часть

- «Сепаратор данных» отвечает:
  - за очистку цифрового сигнала от шумов при чтении,
  - выделение данных для последующей их обработки в программной части АПК «Бюллетень».

- «Квантовый генератор электронных бюллетеней» обеспечивает генерацию случайных чисел на основе алгоритмов квантовой криптографии , используемых в качестве уникальных идентификаторов электронных бюллетеней.

Схема реализации идеи электронного голосования № 2 (с возможностью присутствия желающих голосовать на ИУ)

Верхний уровень

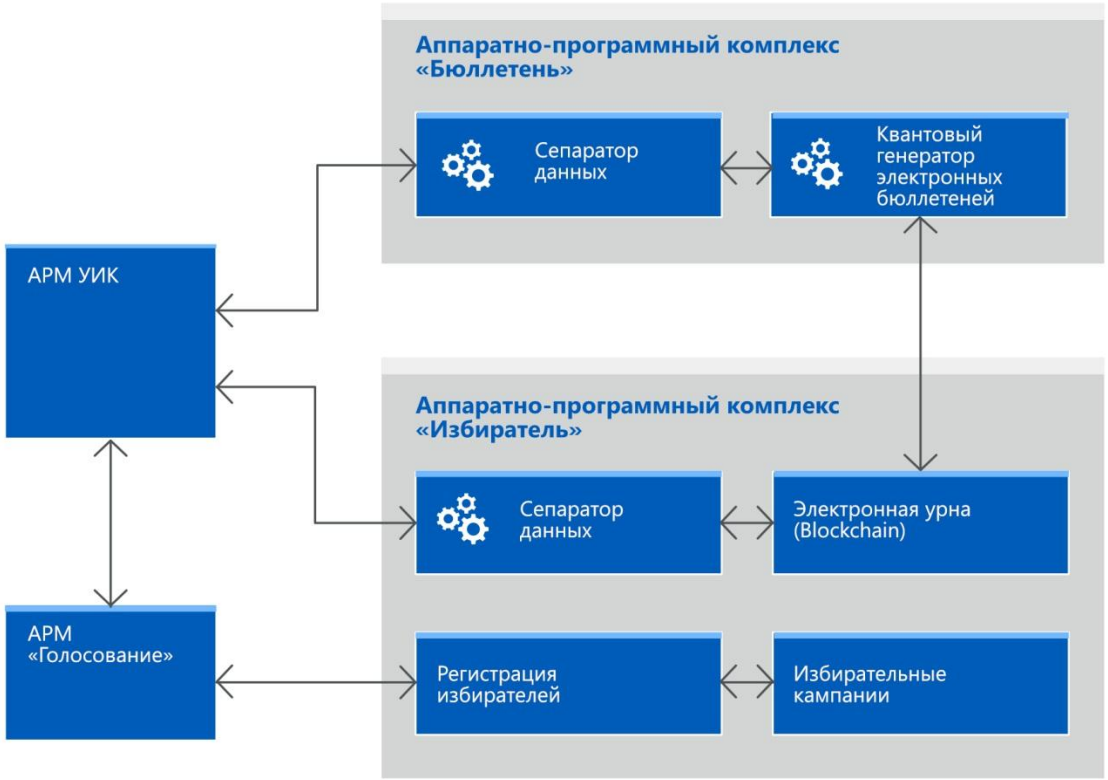
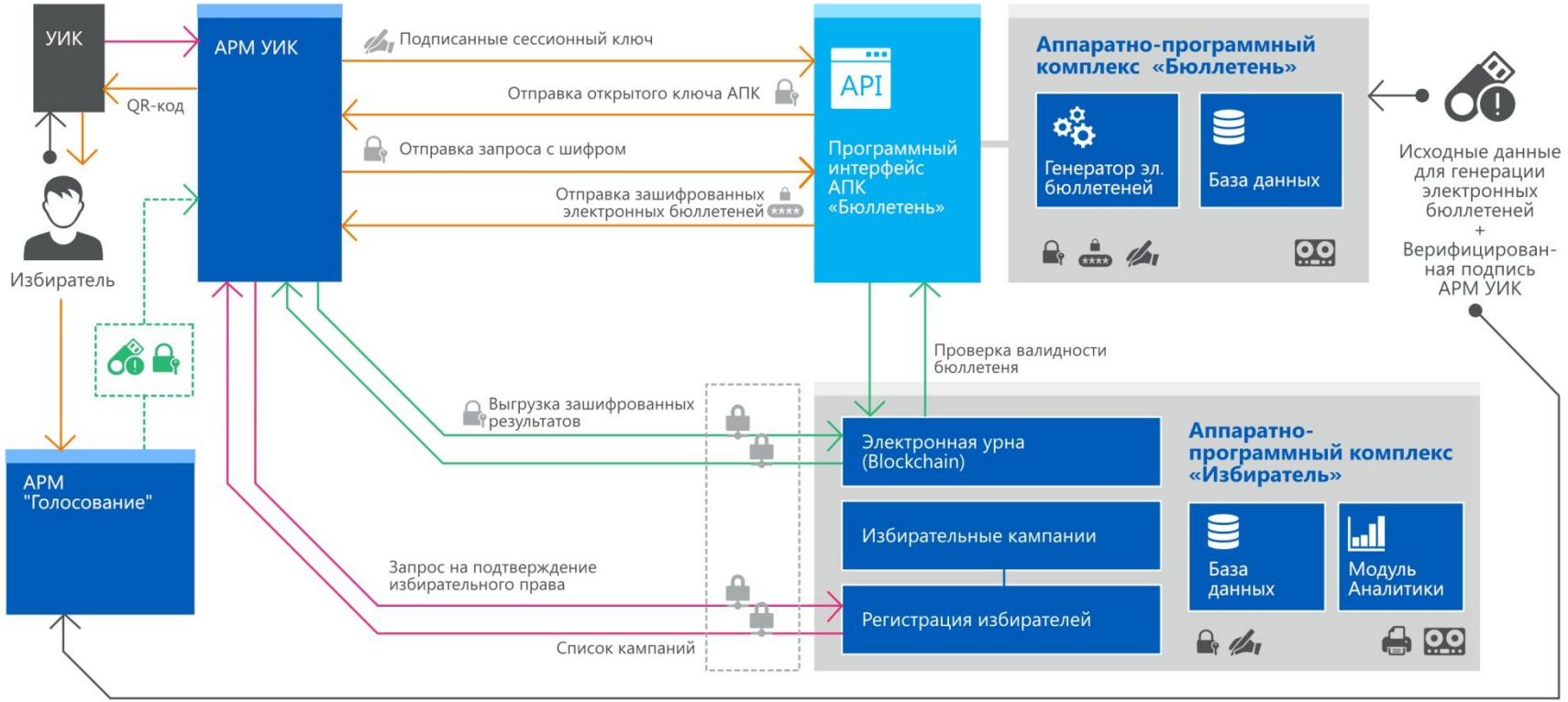


Схема реализации идеи электронного голосования № 2 (с возможностью присутствия желающих голосовать на ИУ)



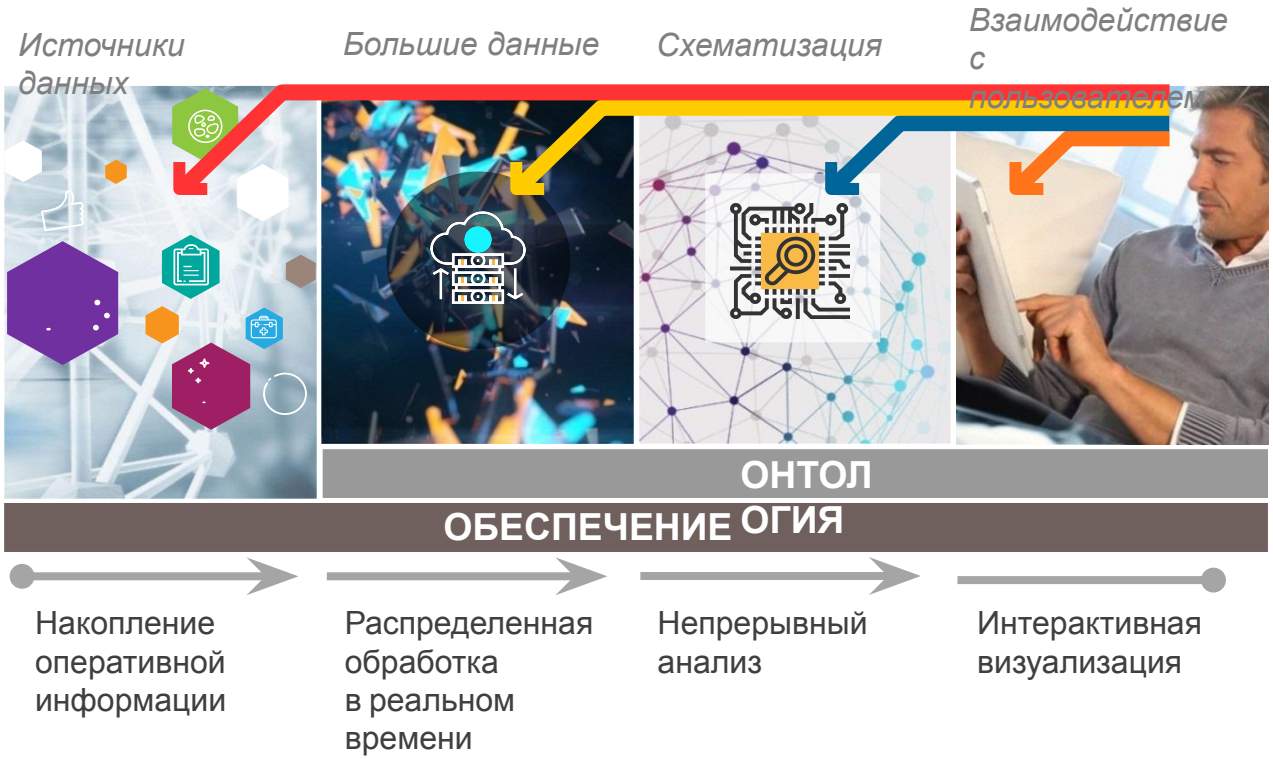
Сценарий электронного голосования для избирателя по схеме №2

- Обращение в УИК
- Создание криптографического ключа (шифра) на основе биологического датчика случайных чисел (или сканера отпечатка пальца, сетчатки глаза)
- Получение QR-кода с данными о доступных кампаниях
- Голосование:
  - Считывание QR-кода на АРМ «Голосование»
  - Выбор кампании
  - Выбор и передача голоса
  - Подтверждение сохранения
- Завершение сеанса голосования

Широкие аналитические возможности

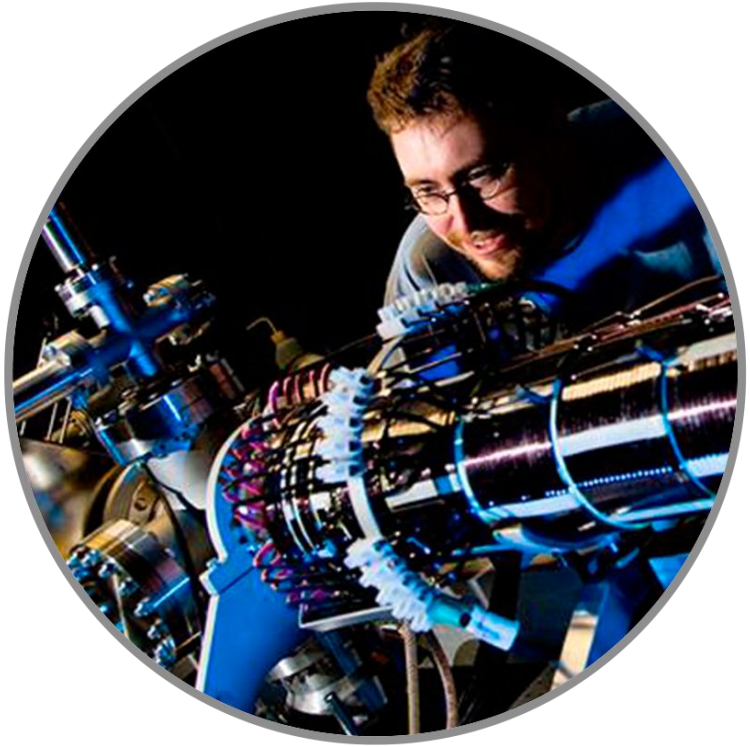
В основе – интеллектуальные технологии обработки больших данных.

Накопление и непрерывный анализ гарантированно обезличенных данных, поступающих из указанных выше систем. Результат – социальный срез участвующих в выборах граждан (пол, возраст, территория проживания), выводы по социальному срезу не участвующих и рекомендации по их привлечению в дальнейшем.



Близкая угроза

"Защитный потенциал большинства современных систем обеспечения безопасности информации находится под угрозой в связи с потенциально возможным появлением в ближайшей и среднесрочной перспективе квантовых компьютеров. Их вычислительный ресурс должен быть несравнимо выше, чем у классических", — констатировал начальник Главного управления развития информационных и телекоммуникационных технологий Минобороны генерал-майор Олег Масленников в ходе форума "Инфофорум-2018".



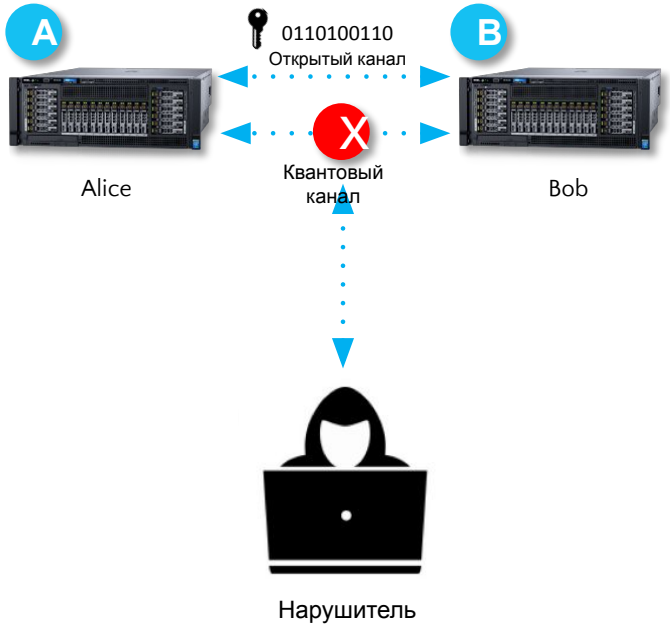
Квантовые инфраструктуры в мире

Крупнейшие многоузловые квантовые сети созданы в США (разработка Управления перспективных исследовательских проектов Министерства обороны США (DARPA)), Европе (SEQOQC), Японии (Сеть Токио, разработчик – компания Toshiba), Китае и Австралии.

1. Западно-Американский
2. Восточно-Американский
3. Европейский
4. Британский
5. Китайский
6. Японский
7. Австралийский

Принципы защищенной передачи данных на основе технологии квантовой коммуникации

- Для генерации ключей шифрования используются кванты света - фотоны;
- В силу физических свойств фотонов (разрушаются при измерении, невозможно разделить и скопировать неизвестное состояние) – отправитель и получатель в процессе передачи всегда будут знать, есть ли в канале связи «нарушитель», который пытается украсть данные;
- Путем измерения состояний фотонов получателем и сравнений их с данными отправителя, формируется закрытый ключ шифрования необходимой длины (равной длине



Невозможно «прослушать» или взломать в силу физических законов

Технические характеристики

- Скорость генерации квантового ключа: до 100 кбит/с
- Частота обновления ключа до 100 раз в секунду
- Скорость передачи данных 1 Гбит/с
- Поддержка протоколов TCP/IP, UDP
- Маршрутизация L2/L3
- Предельные потери в оптическом канале: 39 дБ (230 км)
- Спектральный диапазон C (1530 .. 1565 нм)
- Тип волокна: SMF-28e или аналогичное
- Интерфейс подключения: fc/apc
- Частота импульсов: 100 МГц
- Коэффициент квантовых ошибок (QBER): < 5 %

Системы для центров обработки данных

- Канал: оптика, OTN с форматом кадра OTU2 (10Gbit/s).
- Абонент: оптика 10Gbit Ethernet или 8x1Gbit Ethernet.
- Производительность шифрования 10Gbit/s.
- Алгоритм шифрования: ГОСТ Р34.12-2015 (Магма).
- Шифрование данных осуществляется в режиме гаммирования в соответствии с ГОСТ Р34.13-2015.
- Имитозащита данных осуществляется в соответствии с ГОСТ Р34.13-2015.
- Формирование и контроль имитовставки за каждый кадр OTU2.
- Ключи — парные.
- Коррекция ошибок FEC RS (255, 239).

Квантовый генератор случайных чисел

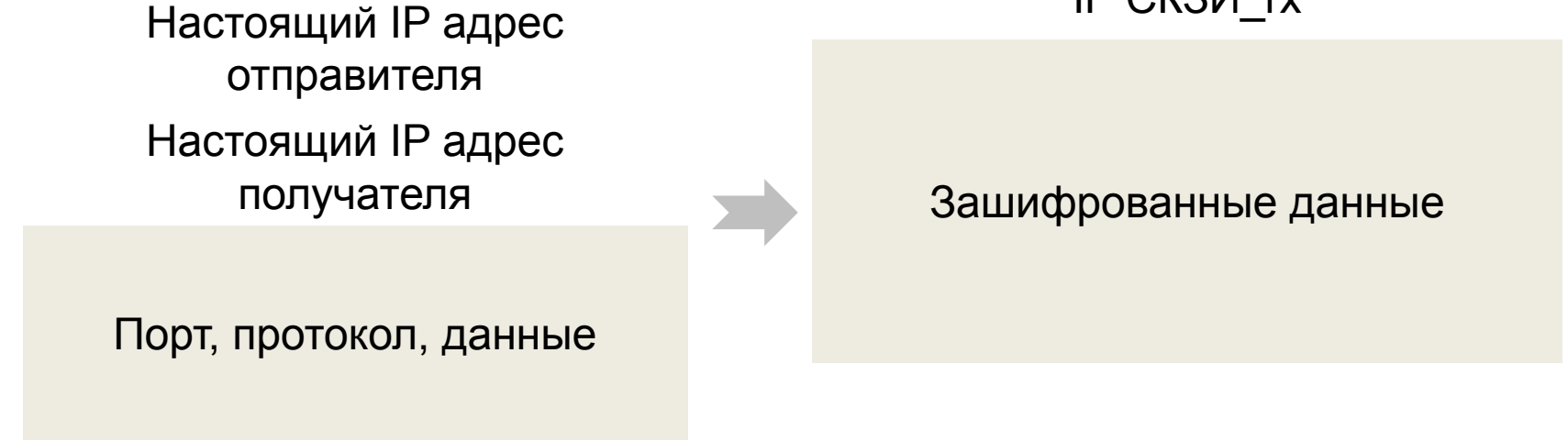
	КГСЧ, основанный на поляризационном шуме	КГСЧ, основанный на вакуумных флуктуациях
Источник энтропии	• Поляризационный шум в ВИЛ (вертикально излучающий лазер) • Экспериментально выравниваемое распределение шума • Стабилизированные параметры распределения	Шумы вакуумных флуктуаций, регистрируемые при гомодинном детектировании
Преимущества по сравнению с классическими ГСЧ	• Статистический анализ необработанных данных параллельно с извлечением случайности • Адаптивный статистический анализ, определяющийся сценарием работы устройства • Онлайн контроль сбоев в работе компонентов системы	• Доверенный источник энтропии • Соблюдение статистических параметров • Компактность
Скорость генерации	до 240 Мбит/с	до 500 Мбит/с
Смещение*	<0.000015	не более 10^{-3}
Тестирование	• батарея тестов NIST • батарея тестов Diehard	

*Смещение определяется как различие между измеренной вероятностью единиц и идеальной вероятностью: b=|p(1)-0.5|

Сепаратор данных
Подсистема сокрытия структуры данных

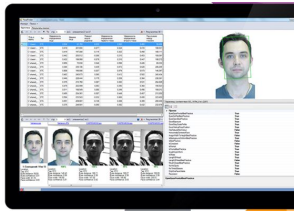
Для сокрытия архитектуры внутренней сети необходимо шифровать пакет целиком с заголовками, так как в них содержится ценная информация:
- настоящие адреса отправителя и получателя;
- тип протокола;
- номера портов, по которым можно определить тип сервиса.

Если зашифровать пакет целиком - в открытой сети будут фигурировать лишь адреса криптооборудования. Но полезные данные и информация о внутренней организации сети будут надёжно защищены.



Примеры внедрения: инжиниринговый центр

SafeNet



Квантовые коммуникации

КВАНТОВЫЕ КОММУНИКАЦИИ

УНИВЕРСИТЕТ ИТМО

Эльбрус

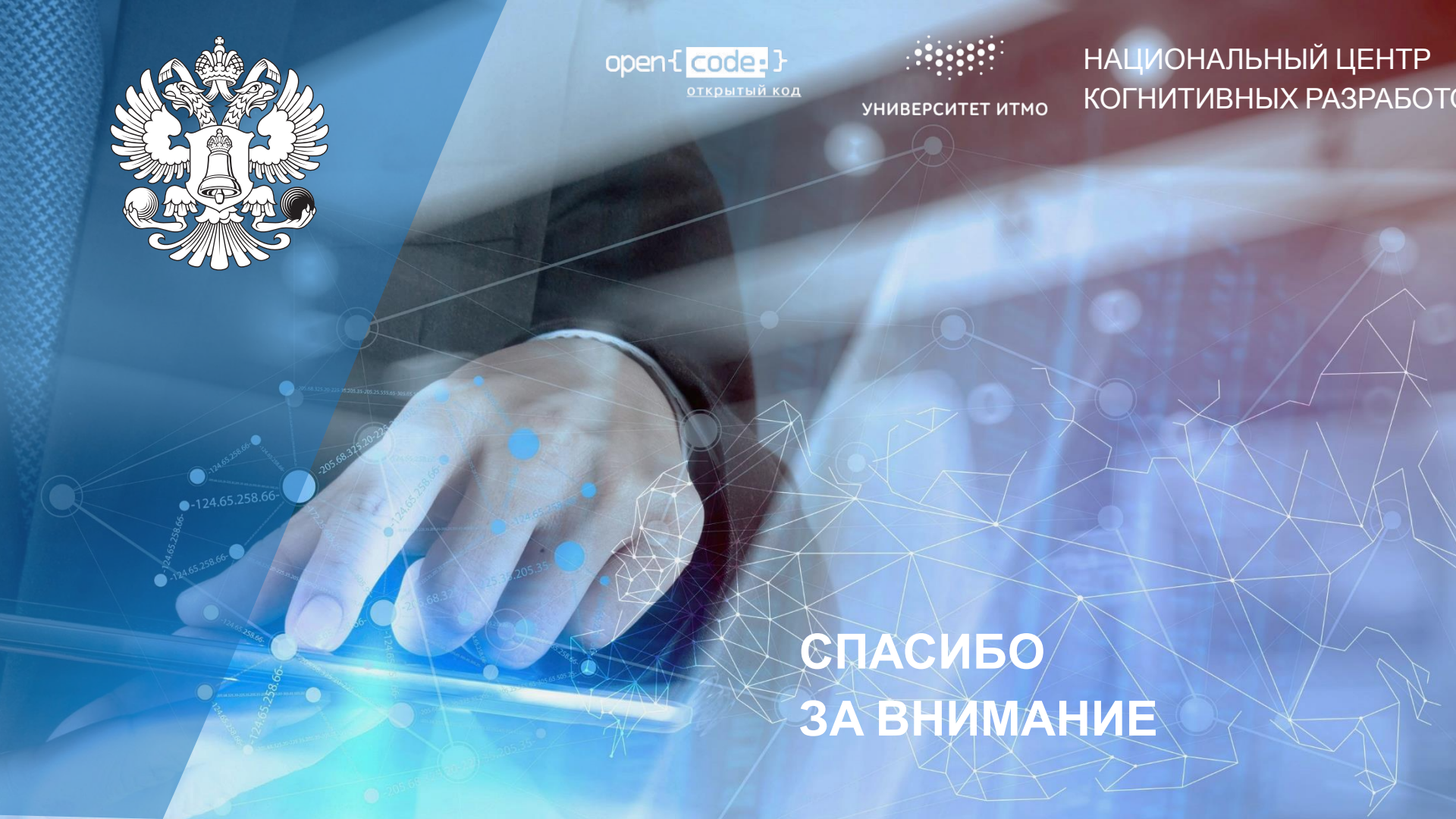
МЦСТ ЭЛЬБРУС

Системы хранения

RAIDIX

Биоидентификация

Центр Речевых Технологий


open{code:}
открытый код
УНИВЕРСИТЕТ ИТМО
НАЦИОНАЛЬНЫЙ ЦЕНТР
КОГНИТИВНЫХ РАЗРАБОТ
СПАСИБО
ЗА ВНИМАНИЕ