Музей криптографии

Что посмотреть в Музее криптографии за 1 час

В сентябре 2021 года откроется первый в России Музей криптографии.

Проект разрабатывается АО «НПК «Криптонит» при поддержке профессионального и научного сообщества.

Результаты проектирования

Разработана концепция экспозиции на **1200 м²**

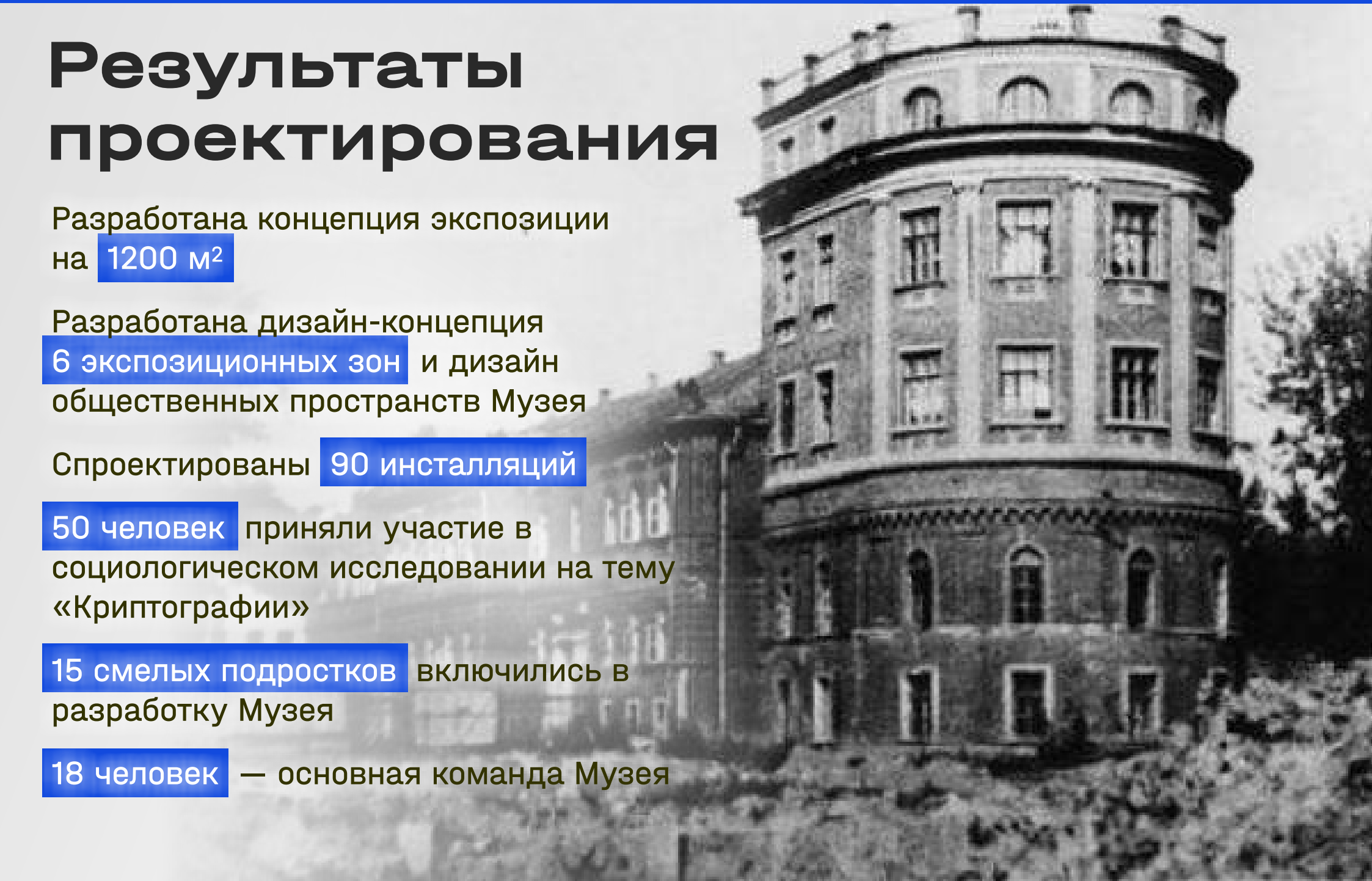
Разработана дизайн-концепция **6 экспозиционных зон** и дизайн общественных пространств Музея

Спроектированы **90 инсталляций**

50 человек приняли участие в социологическом исследовании на тему «Криптографии»

15 смелых подростков включились в разработку Музея

18 человек — основная команда Музея



Предпроектное исследование аудитории

Подростки (13 - 17 лет) из общеобразовательных и специализированных школ, из государственных и частных школ. Разного возраста и бэкграунда.

Учителя из общеобразовательных и специализированных школ, из государственных и частных школ, часть из районных школ. Учителя математики, информатики, истории, начальных классов.

Родители (детей 12-17 лет) живут в Москве или ближайшем Подмосковье. В каждой семье разное количество детей.

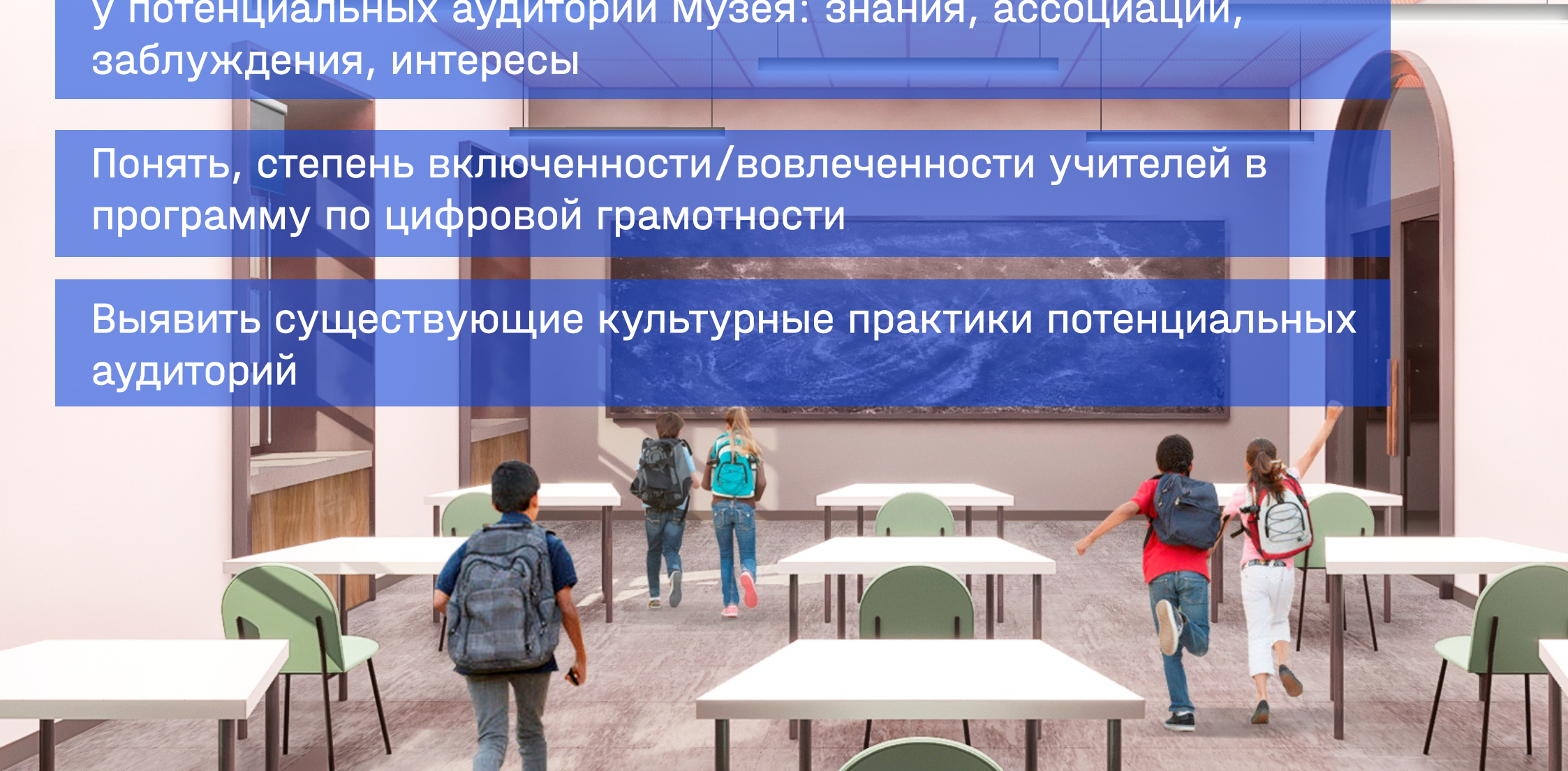
"Молодые люди» (24 - 35 лет) работают в Москве, не специалисты в области современных технологий (не имеют профильного образования и не работают в сфере IT).

Задачи исследования:

Понять, какие представления о криптографии существуют у потенциальных аудиторий Музея: знания, ассоциации, заблуждения, интересы

Понять, степень включенности/вовлеченности учителей в программу по цифровой грамотности

Выявить существующие культурные практики потенциальных аудиторий



Результаты исследований

Представления о криптографии: респонденты имеют очень смутное представление о том, что такое криптография, или не имеют вовсеПодростки лучше ориентируются в цифровом мире, более открыты к теме криптографии, хоть и не имеют особых знаний.

Представления родителей о теме различаются от «а я знаю все про криптовалюты, я вам все расскажу» до «я ничего не понимаю».

Респонденты в возрасте 24-35 лет имеют меньше всего знаний о криптографии. При слове «криптография» респонденты вспомнили криптовалюты и комиксы Марвел.

Экспозиция

История развития криптографии от зарождения письменности до постквантовых технологий

Содержательная часть экспозиции

сформирована по двум «направлениям»:

1. Криптография как наука
2. Криптография в истории

Экспозиция построена по принципу обратной хронологии

«Домашинная» криптография
XV–XIX вв.

Криптография в цифровую эпоху
1990е гг. — 2050е гг.

Научная криптография
Конец XIX cent. — 1990е гг.

Цифровая криптография

Вторая половина XX века — XXI век

«Цифровой» период развития криптографии, связанный с применением компьютерных и IT технологий. «Будущее» криптографии.

Мир без криптографии

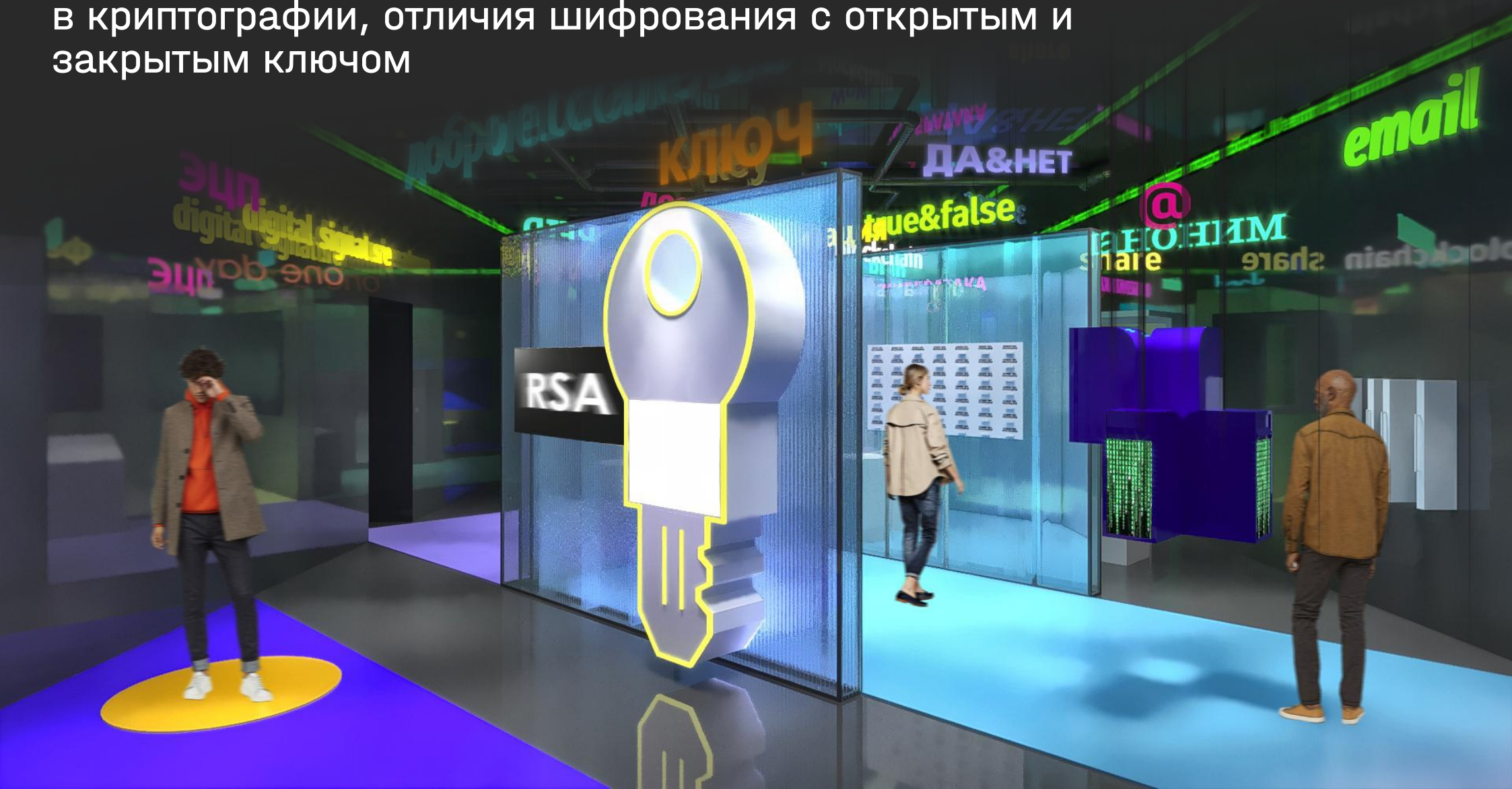
Криптография необходима для устойчивого функционирования всех систем современного мира и защищает стабильность нашей жизни на всех уровнях — на личном и государственном.

Сюжеты:

1. Самолет
2. Умный дом
3. ГЭС
4. Мессенджеры
5. Сайты
6. Супермаркет
7. Банкомат
8. Компьютерные игры
9. Видеозвонки
10. Угон машины

Ключ

С помощью наглядных образов вводится понятие «Ключ» в криптографии, отличия шифрования с открытым и закрытым ключом

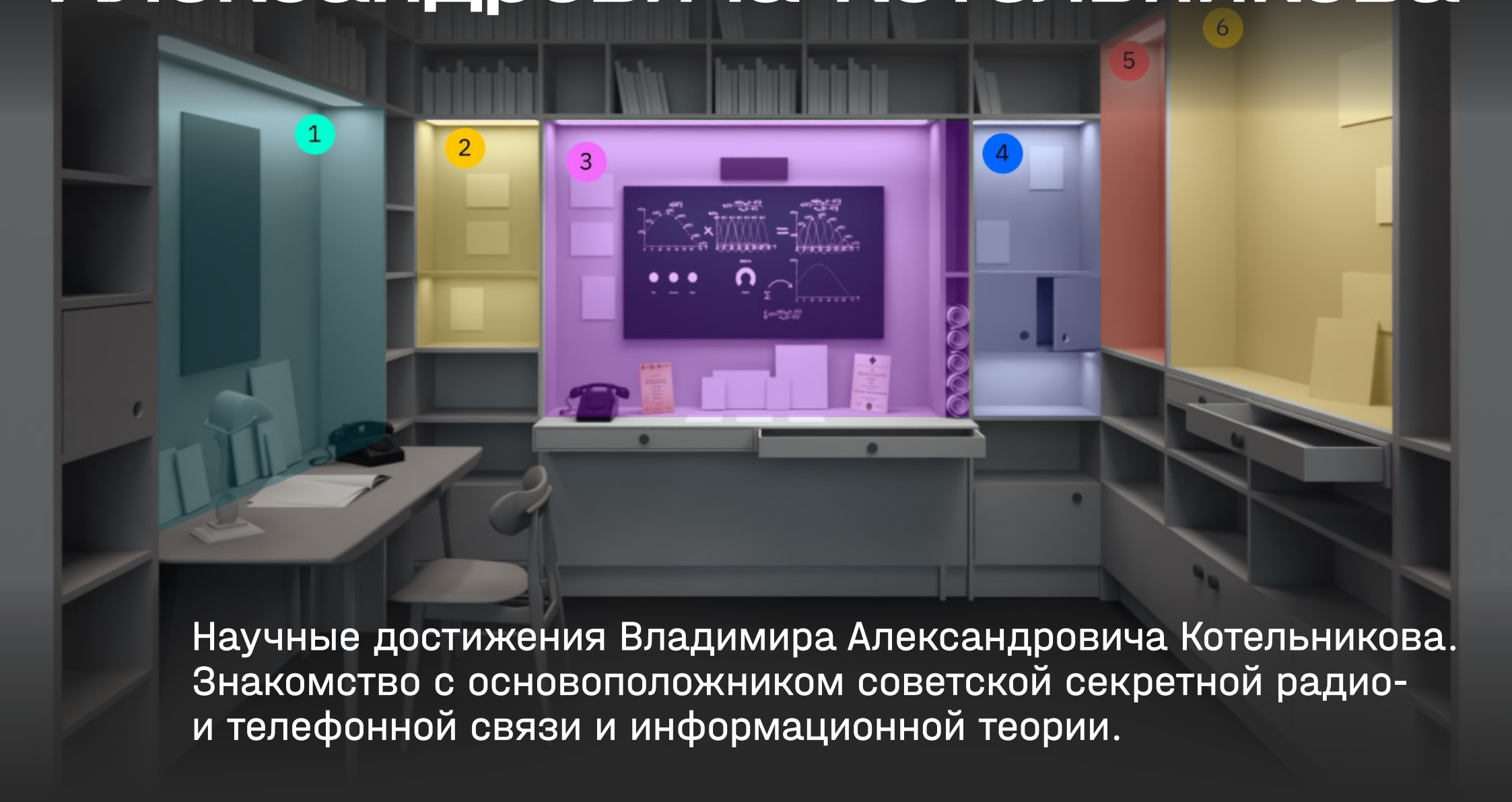


Научная криптография

Конец XIX века — 1990-е гг.

Основные прорывы и открытия криптографической мысли. Электромеханические и электрические каналы коммуникации.

Кабинет Владимира Александровича Котельникова



Научные достижения Владимира Александровича Котельникова. Знакомство с основоположником советской секретной радио- и телефонной связи и информационной теории.

Кабинет Владимира Александровича Котельникова

Технический проект аппаратуры лаборатории Котельникова 1941 года

Атлас поверхности Венеры

«Механическое сердце»

Главные экспонаты зоны — шифромашины Фиалка и Энигма

Эволюция технических средств шифрования текстов — электромеханических, роторных и электрических шифровальных машин Советского Союза и других стран.

Механическое сердце криптографии — Фиалка

Главная шифромашина СССР и стран Варшавского договора.
История создания, применения и принципы работы.

Уникальные экспонаты

- М-105
- М-205
- М-153
- М-401, М-401 ПД
- М-161
- М-204М
- М-154-4М

Уникальные экспонаты

Дельта-М, М-467. Предназначена для шифрования информации, передаваемой по стандартным ТЧ, спутниковым и по УВК каналам связи на скоростях 2.4, 4.8, 9.6 кбит\сек

Прерия, Т-819. Для автоматического шифрования с гарантированной стойкостью симплексных радиотелефонных переговоров, ведущихся по УКВ каналам связи между самолетами

Эльбрус. Т-217, 1960-е гг. Аппаратура временной стойкости для шифрования речевой информации

Яхта. Т-219, 1960-е гг. Аппаратура временной стойкости для шифрования речевой информации

Интерьер. Т-230-03, 1980-е гг. Аппаратура гарантированной стойкости для шифрования аналоговой телефонной, а также импульсной телефонной, телеграфной, фототелеграфной и телекодовой информации

Историк-1. Т-240С+Т-240Д, 1980-е гг. Аппаратура гарантированной стойкости для шифрования телефонной информации, передаваемой в симплексном режиме по УКВ-радио и проводным каналам связи между самолетами ВВС

Трамплин М-480. Аппаратура гарантированной стойкости для шифрования речевой и документальной информации, передаваемой по телефонным сетям общего пользования

ТС-25, использовался с СТ-35 (стартстопный телеграфный аппарат)

Весна, Т-206-3М1 (1970-е). Телеграфная аппаратура шифрования для автоматического засекречивания и рассекречивания телекодовых и телеграфных сообщений

Угломер (Т-230-06), 1970-е гг. Телеграфная аппаратура шифрования для автоматического засекречивания и рассекречивания телекодовых и телеграфных сообщений, предназначенная для совместного использования аппаратурой Т-230-1А(М) и Т-230-03 (Интерьер)

От пишущей машинки до электронных шифромашин

От пишущей машинки как архетипа шифровальной машины к роторам, ламповой панели, перфоридеру и транзисторной схеме

«Домашинная» криптография

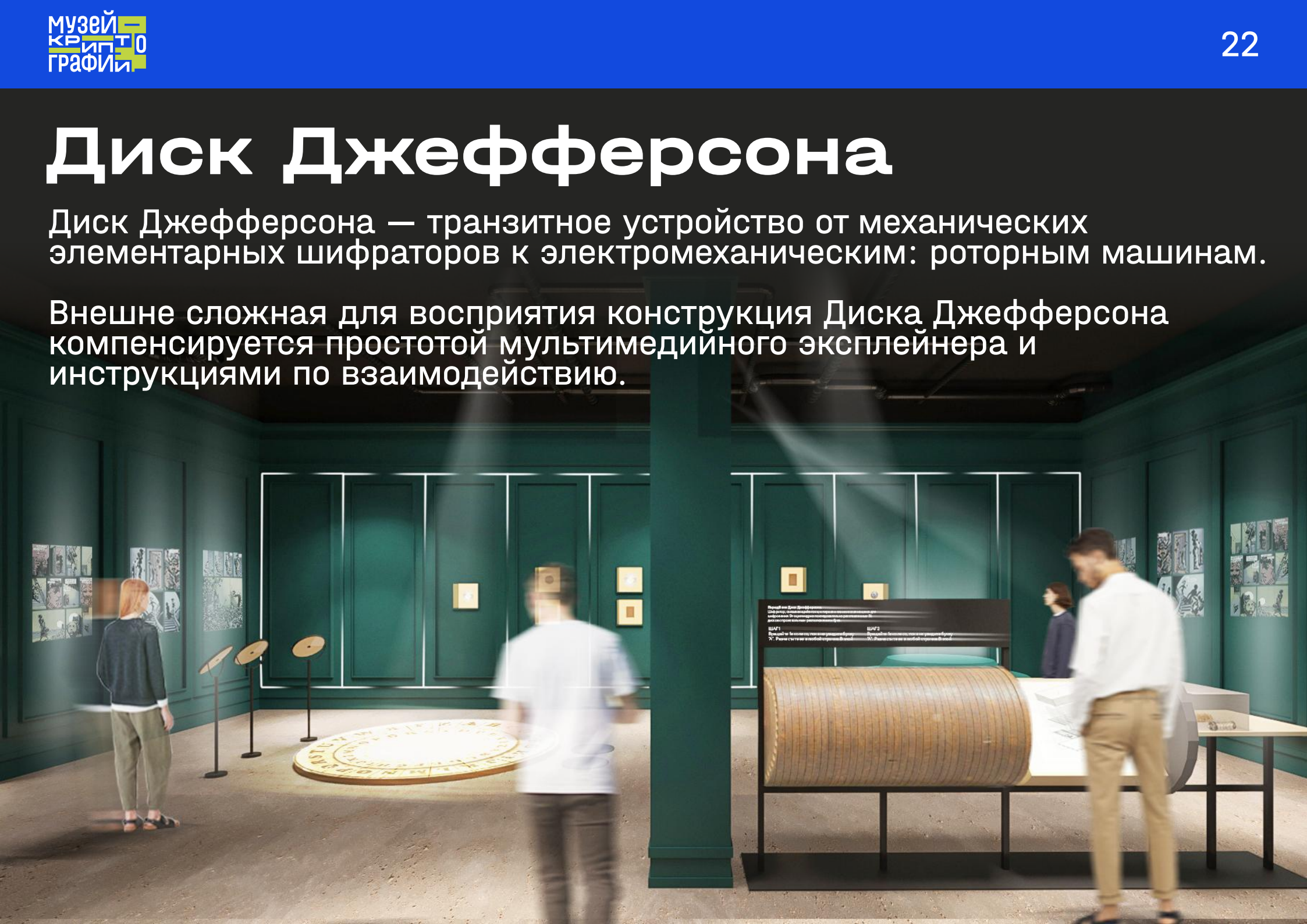
XV век — начало XX века

Шифрование и дешифровка письма. Почтовые отделения как каналы передачи информации и «службы национальной безопасности».

Диск Джефферсона

Диск Джефферсона — транзитное устройство от механических элементарных шифраторов к электромеханическим: роторным машинам.

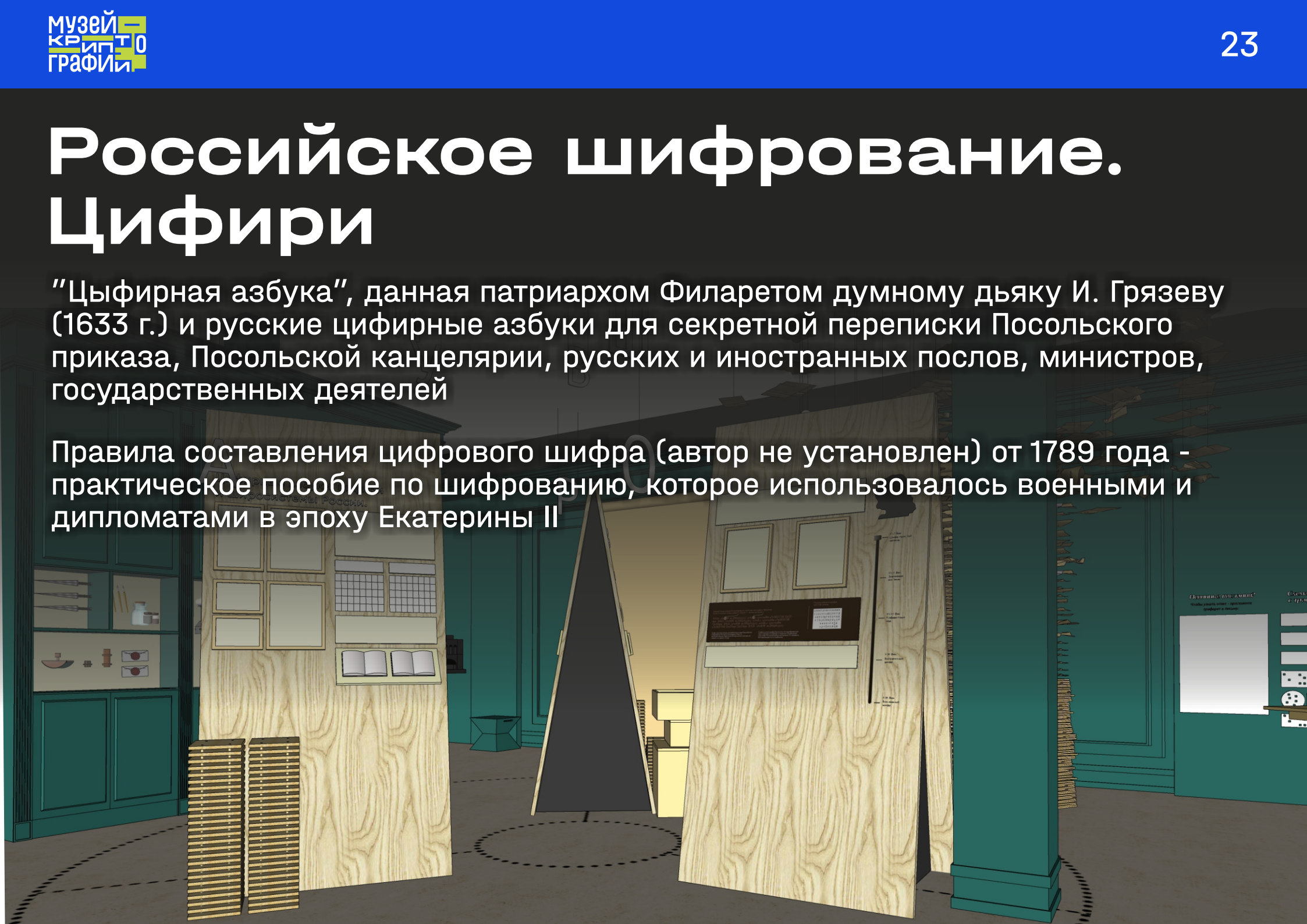
Внешне сложная для восприятия конструкция Диска Джефферсона компенсируется простотой мультимедийного эксплейнера и инструкциями по взаимодействию.



Российское шифрование. Цифири

"Цыфирная азбука", данная патриархом Филаретом думному дьяку И. Грязеву (1633 г.) и русские цифирные азбуки для секретной переписки Посольского приказа, Посольской канцелярии, русских и иностранных послов, министров, государственных деятелей

Правила составления цифрового шифра (автор не установлен) от 1789 года - практическое пособие по шифрованию, которое использовалось военными и дипломатами в эпоху Екатерины II



«Протокриптография»

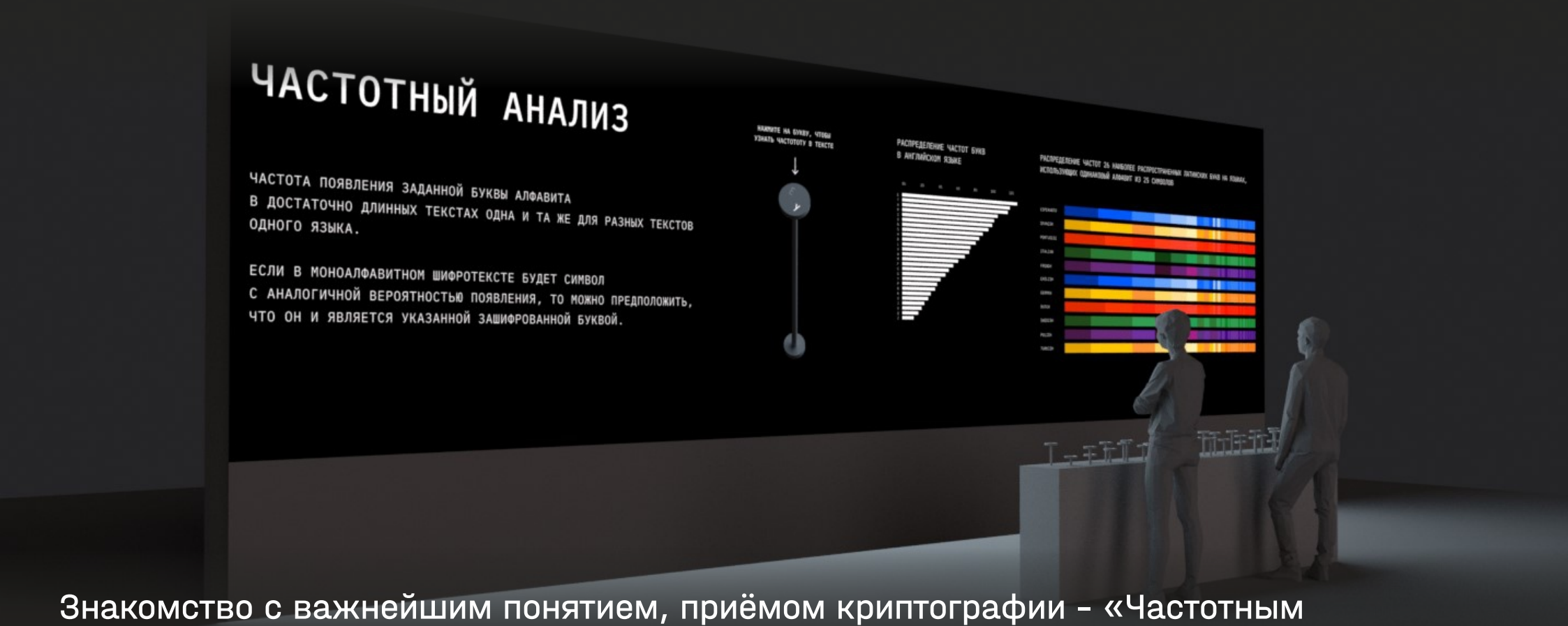
1900-й г. до н. э. — середина XV века

Языковые системы и криптографические «головоломки» как первые попытки шифрования информации.

Шифр Цезаря

Особую роль в криптографии сыграл способ шифрования, предложенный Юлием Цезарем и изложенный им в “Записках о галльской войне”. Цезарь заменял буквы в соответствии с подстановкой, нижняя строка которой представляет собой алфавит открытого текста, сдвинутый циклически на три буквы влево.

Частотный анализ



Знакомство с важнейшим понятием, приёмом криптографии - «Частотным анализом»

Что такое частотный анализ? Как часто повторяются буквы в английских и русских текстах?

Как изобретение этого метода повлияло на криптоанализ?

«Память здания»

История здания через воспоминания людей и шифровальную технику.

135 лет истории здания, где в разные годы располагались приют, детская колония, спецтюрьма и закрытая лаборатория

«Память здания»

Представлены рассекреченные фотографии и документы разных периодов

«Память здания»

Музей криптографии

До встречи в Музее!