



Международная  
Олимпиада  
по финансовой  
безопасности

**Темная сторона**

**ИИ**

#Искусственный интеллект

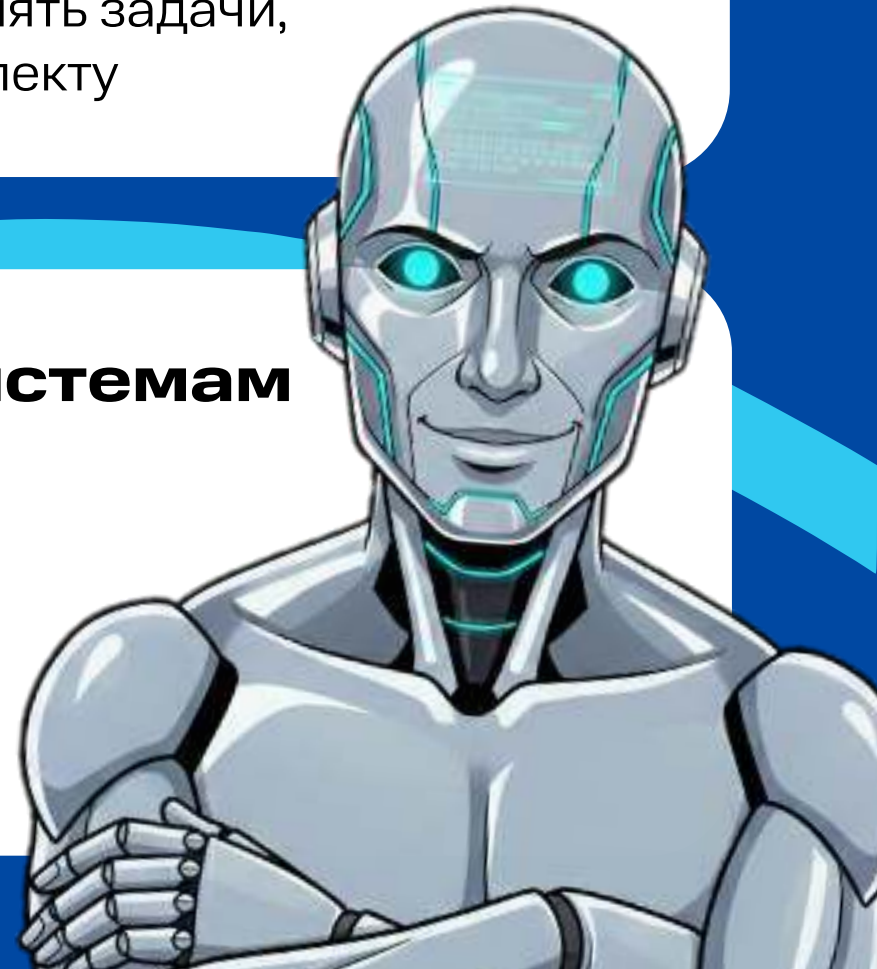


# ↔ Искусственный интеллект (ИИ) ✕ Artificial intelligence

компьютерные системы, способные выполнять задачи,  
свойственные человеческому интеллекту

## **ИИ — это технологии, позволяющие системам**

- понимать запросы, сформулированные естественным языком
- анализировать, обрабатывать и находить нужные данные
- распознавать образы, символы и закономерности
- обучаться на больших потоках данных
- принимать решения и адаптироваться к разным условиям





# Где применяется ИИ



## Медицина и здравоохранение

- Индивидуальные схемы лечения
- Разработка новых лекарств
- Анализ данных



## Банковская сфера

- Автоматические инвестиции
- Кредитный скоринг и оценка рисков
- Оперативное принятие решений



## Образование

- Адаптация материала под ученика
- Выявление пробелов в знаниях
- Составление дополнительных заданий



## Наука и исследования

- Быстрый поиск закономерностей
- Ускорение исследования
- Поиск решений на основе анализа





# Защита кибербезопасности



## Как ИИ противостоит мошенникам

- выявляет и перехватывает мошеннические схемы
- снижает нагрузку на реальные жертвы

КУДА НАЖАТЬ,  
МИЛОК?

## Пример: «Кибербабушка» — ИИ-модель сотового оператора

- общается с мошенниками от имени пожилого клиента
- отвлекает злоумышленников от реальных людей, тратит их время и ресурсы





# Обратная сторона ИИ



## Финансовые угрозы

- рост кибермошенничества с использованием ИИ
- кражи денежных средств и данных
- автоматизация преступных схем

## Особая зона риска

- рост числа пострадавших несовершеннолетних
- атаки через звонки и сообщения (школы, госорганы, операторы связи)
- мошенничество с игровыми аккаунтами и ГИА

## Операции без согласия клиентов

**27,5**  
млрд руб

2024 г

**21**  
млрд руб

9 мес. 2025 г

## Предотвращённые хищения

**222**  
млн руб

ноябрь 2025 г

## Противодействие

- Росфинмониторинг
- Финансовая разведка стран СНГ
- Евразийская группа по ПОД/ФТ



# Отмывание средств



**Кибермошенничество**

**Подставные  
банковские счета**

многократные переводы,  
смешивание средств

**Запутывание финансовых потоков**

**Криптоплатформы**

**Легализация / финансирование  
преступной деятельности**



Угроза носит транснациональный характер



# Кто такой дроппер?



## Дроппер

человек, который использует свои карты для обналичивания или транзита (дальнейшей отправки) похищенных денежных средств



# Вовлечение молодежи



## Кто вовлекается

- подростки от 14 лет
- студенты и школьники
- безработные



## Как вовлекают (психологические уловки):

- **срочность** — «только сегодня»
- **простота** — «справится любой»
- **мнимая легальность** — «все законно»
- **постепенность** — от малых сумм к большим
- **социальное доказательство** — «уже работают сотни»

## Более 1 млн дропперов

Масштаб проблемы в России

*данные Банка России*



# Ответственность



## Прямая уголовная ответственность

установлена за дропперские схемы в дополнении ст. 187 УК РФ

## Наказание

- до 3 лет лишения свободы — за передачу банковских реквизитов
- до 6 лет лишения свободы — для организаторов (дроповодов)

## Практика применения

- в 2025 г. возбуждено первое уголовное дело против дроповода
- сотрудничество с МВД — основание для освобождения от ответственности
- организатор выявлен по показаниям задержанного дроппера





# Дипфейки: новая угроза




## Дипфейк

(от англ. deepfake – «глубокий подлог»)

видео, аудио или фото, созданные ИИ, на которых человек делает или говорит то, чего никогда не было в реальности

## Как это работает

- звонки под видом опросов и запись голоса
- ИИ копирует лицо и голос человека
- создание голосовых дипфейков



**Достаточно нескольких секунд записи для создания голосового дипфейка**



# Первый громкий кейс



**2019 год, Великобритания**

мошенники с помощью ИИ скопировали голос CEO энергетической компании

**Схема атаки**

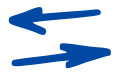
«Голос директора» звонит подчиненному со срочным распоряжением о переводе средств поставщику



**€220 000**

переведены на счет мошенников



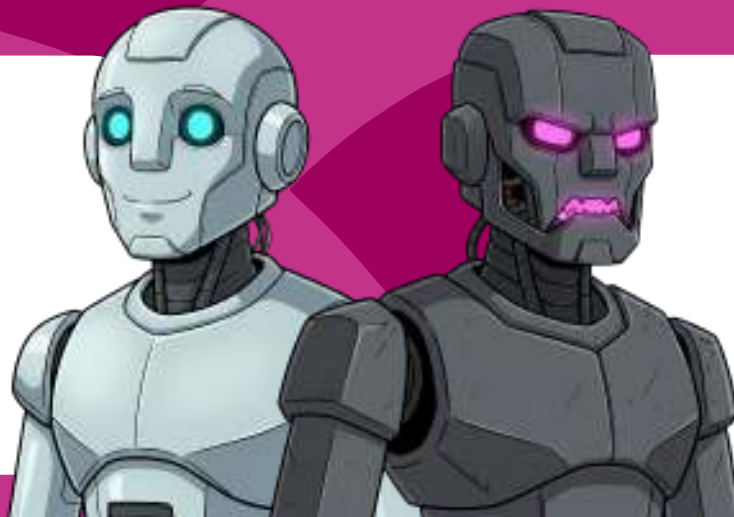


# «Злой близнец» (Evil Twin)



## Суть атаки

поддельная Wi-Fi-сеть,  
копирующая настоящую



## Что похищают

- логины и пароли
- данные банковских карт
- переписку и историю браузера

## Как работает схема

### Клонирование сети

тот же SSID, более  
сильный сигнал



### Подключение жертвы

кафе, аэропорты,  
торговые центры



### Man-in-the-Middle

перехват всего  
трафика

### Фишинг

фейковая  
страница входа



# «Злой близнец» в аэропорту



## Ситуация

- Школьница подключилась к Wi-Fi с названием аэропорта
- Сеть была первой в списке
- Код оказался одноразовым паролем

## Критические ошибки

- Проигнорированы предупреждения о незащищённой сети
- Введён номер телефона
- Введён код из мессенджера

## Результат

- Потеря доступа к мессенджеру
- Компрометация личных данных

## Важно!

Коды из мессенджеров никогда не вводятся при регистрации в Wi-Fi





# ИИ-фишинг



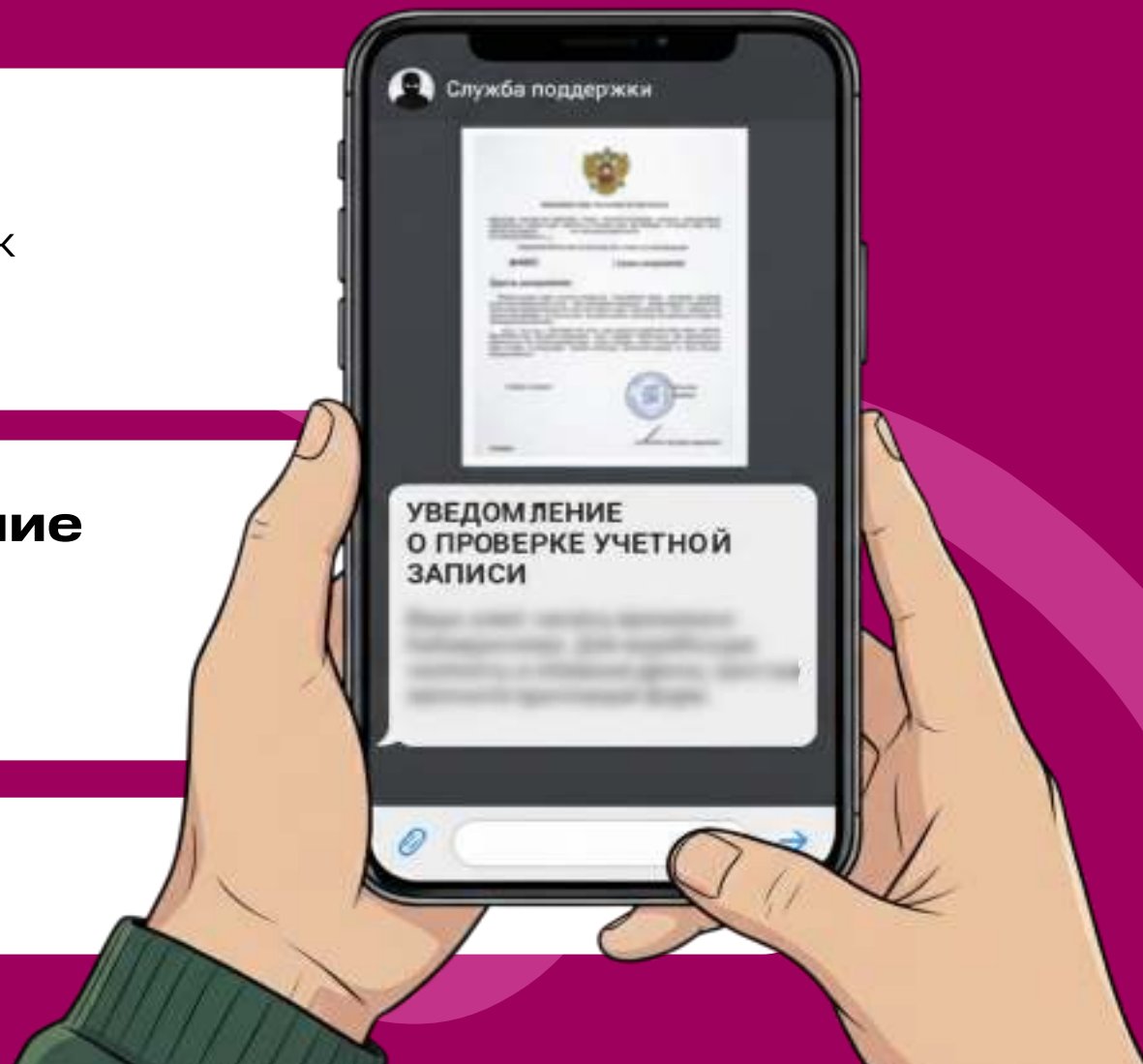
## Перед началом работы ИИ

- анализирует данные из соцсетей, сайтов, утечек
- генерирует «идеальные» письма и сообщения

## Отправляет персональное сообщение

- без ошибок и шаблонных фраз
- выглядит как реальное служебное общение

## Результат – потеря денег





# ИИ-ВИШИНГ



## ИИ-ВИШИНГ

(англ. vishing = voice + phishing): голосовой фишинг

- голосовая разновидность дипфейка
- ИИ копирует голос по нескольким секундам записи
- позволяет вести диалог с жертвой

**ИИ делает мошенничество максимально реалистичным**





# Романтический скам



## Суть атаки

- ИИ ведёт беседы с тысячами людей одновременно
- Создаёт иллюзию доверия, использует данные соцсетей для персонализации общения



## Как работает схема

**Переписка в чатах**  
личные вопросы,  
голосовые сообщения

**Предложение вложений**  
ставки, криптовалюта,  
финансовые пирамиды

**Демонстрация «успеха»**  
через фото, скриншоты,  
подарки

# ⇄ **Безопасность в публичном Wi-Fi** ✕

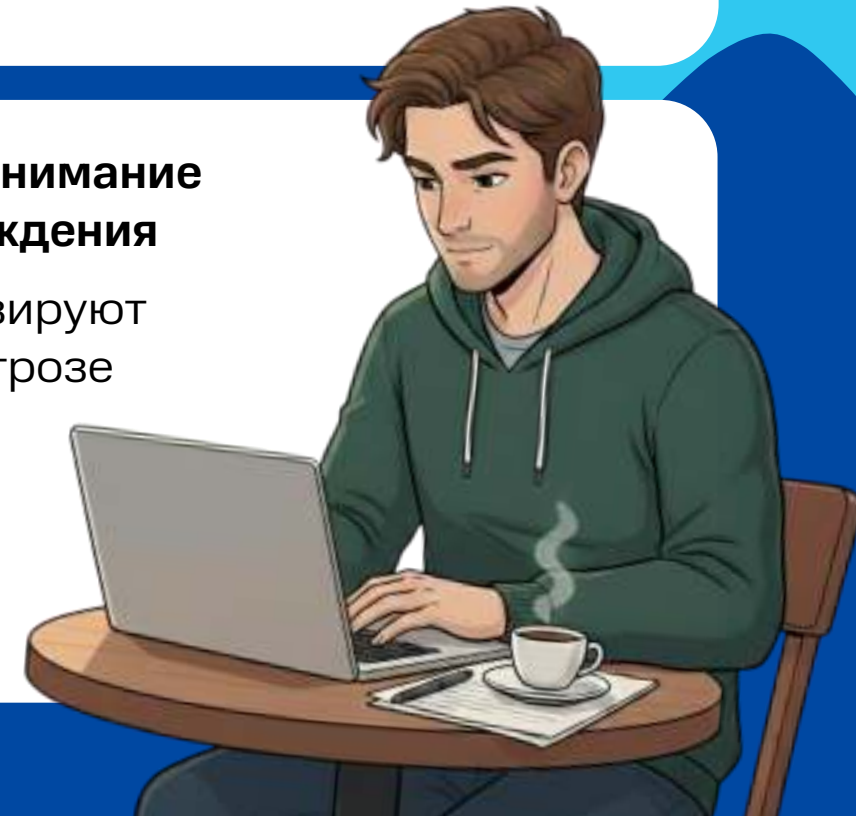
**Не пользуйтесь незащищёнными сетями**  
«Злые двойники» почти всегда открыты

**Используйте только HTTPS-сайты**  
Значок замка → соединение  
защищено сквозным шифрованием

**Подключайте многофакторную  
аутентификацию (MFA)**  
Пароль + одноразовый код

**Никогда не вводите пароли и данные карт**  
Публичный Wi-Fi перехватывает трафик

**Обращайте внимание  
на предупреждения**  
Они сигнализируют  
о реальной угрозе



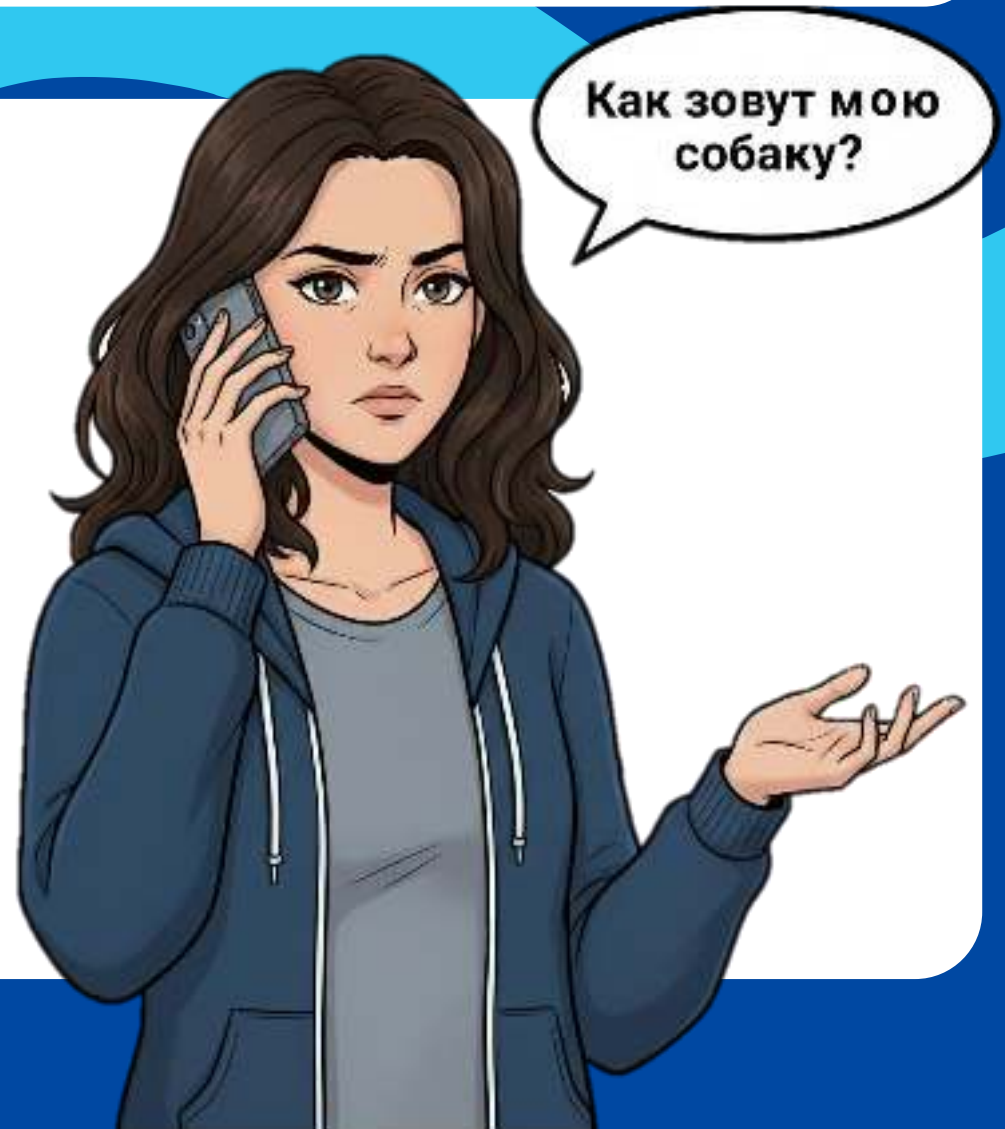


# Не поддавайтесь панике!



## Простой, но надёжный способ защититься от подделки голоса ИИ

1. Положите трубку при первых подозрениях
2. Перезвоните родственнику или другу из телефонной книги для проверки
3. Используйте семейное кодовое слово для подтверждения личности
4. Задавайте личные вопросы, известные только близким  
(например: «Как зовут нашу собаку?»)



# ⇌ Соблюдайте цифровую гигиену! ✕

## Как не дать ИИ клонировать ваш голос

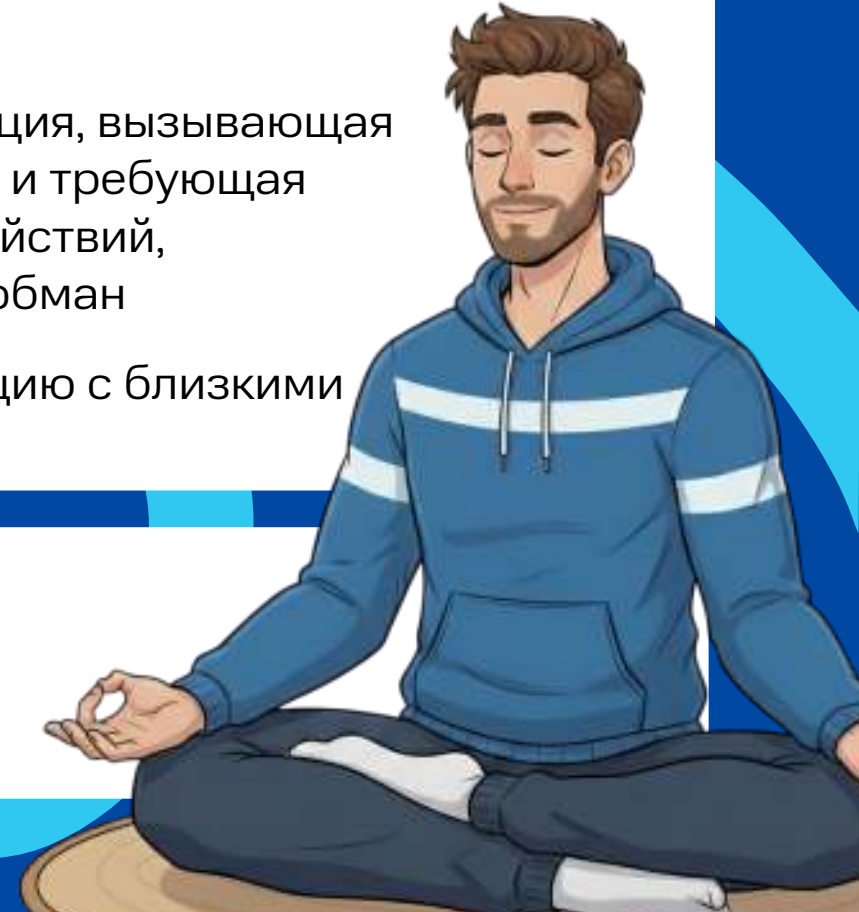
- **Закройте доступ к соцсетям**  
*(только для друзей)*
- **Не выкладывайте записи**  
голоса в открытый доступ  
*(статусы, стримы, мессенджеры)*

## Контролируйте эмоциональное состояние

- Любая информация, вызывающая сильные эмоции и требующая немедленных действий, скорее всего — обман
- Обсудите ситуацию с близкими

## Главное оружие – критическое мышление

Помните: государственные органы (ЦБ РФ, ФСБ, ФНС) не решают «важные вопросы» по телефону



# Отсекайте подозрительные контакты

## Как действовать, если столкнулись с мошенничеством

- **Прекратите разговор** при упоминании денег, ставок, криптовалют
- **Используйте критическое мышление**
- **Заблокируйте** мошенника
- **Не переводите никаких денег** человеку, которого не видели вживую
- **При необходимости** — сообщите в правоохранительные органы и администрацию платформы

**Романтический скам – это игра на доверии,**  
а финальной ставкой являются ваши деньги





# Дропперы — посредники в финансовых схемах мошенников



## Кто такие дропы

- Люди, принимающие похищенные деньги
- Переводят либо снимают деньги для кураторов
- Передают карту с доступом к онлайн-банку



## Дропы участвуют в уголовном преступлении

«Приобретение либо передача карты лицами, не являющимися клиентами банка» – за данное нарушение наказание: лишение свободы сроком до 6 лет с выплатой штрафа.

*Статья 187 УК РФ «Неправомерный оборот средств платежей»*



# Статистика дропов в РФ



**> 1 млн**

клиентов-дропперов  
в банках

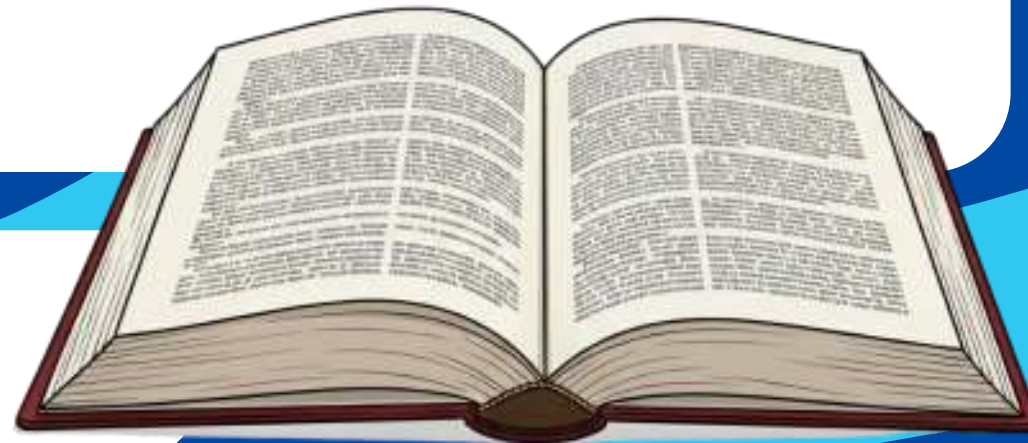
**~ 20%**

не осознающие  
последствий подростки

**Дропперы — важное звено  
в легализации украденных средств**

могут привлекаться к уголовной ответственности  
по ст. 174 УК РФ «Легализация (отмывание) денежных  
средств или иного имущества, приобретённых  
другими лицами преступным путём»

**Осведомлённость и осторожность  
критически важны**





# Виды дропперов по функциям



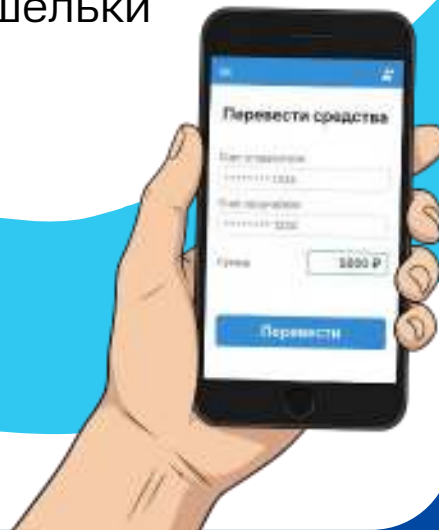
## Заливщики

- принимают наличные →
- зачисляют на счёт →
- переводят дальше



## Транзитники

- получают переводы →
- перенаправляют на другие счета или кошельки



## Обнальщики

- снимают деньги в банкоматах →
- передают организаторам



# Вербовка дропперов с помощью ИИ

## Как работает схема

### Нейросети и NLP

анализируют открытые источники  
(соцсети, форумы, маркетплейсы)

### Поиск уязвимых групп

студенты, безработные люди,  
ищущие «лёгкий доход»

### Оценка психологии жертвы

посты, стиль общения →  
внушаемость, алчность

### Первичный контакт

чат-боты, использование  
дипфейк-аватаров



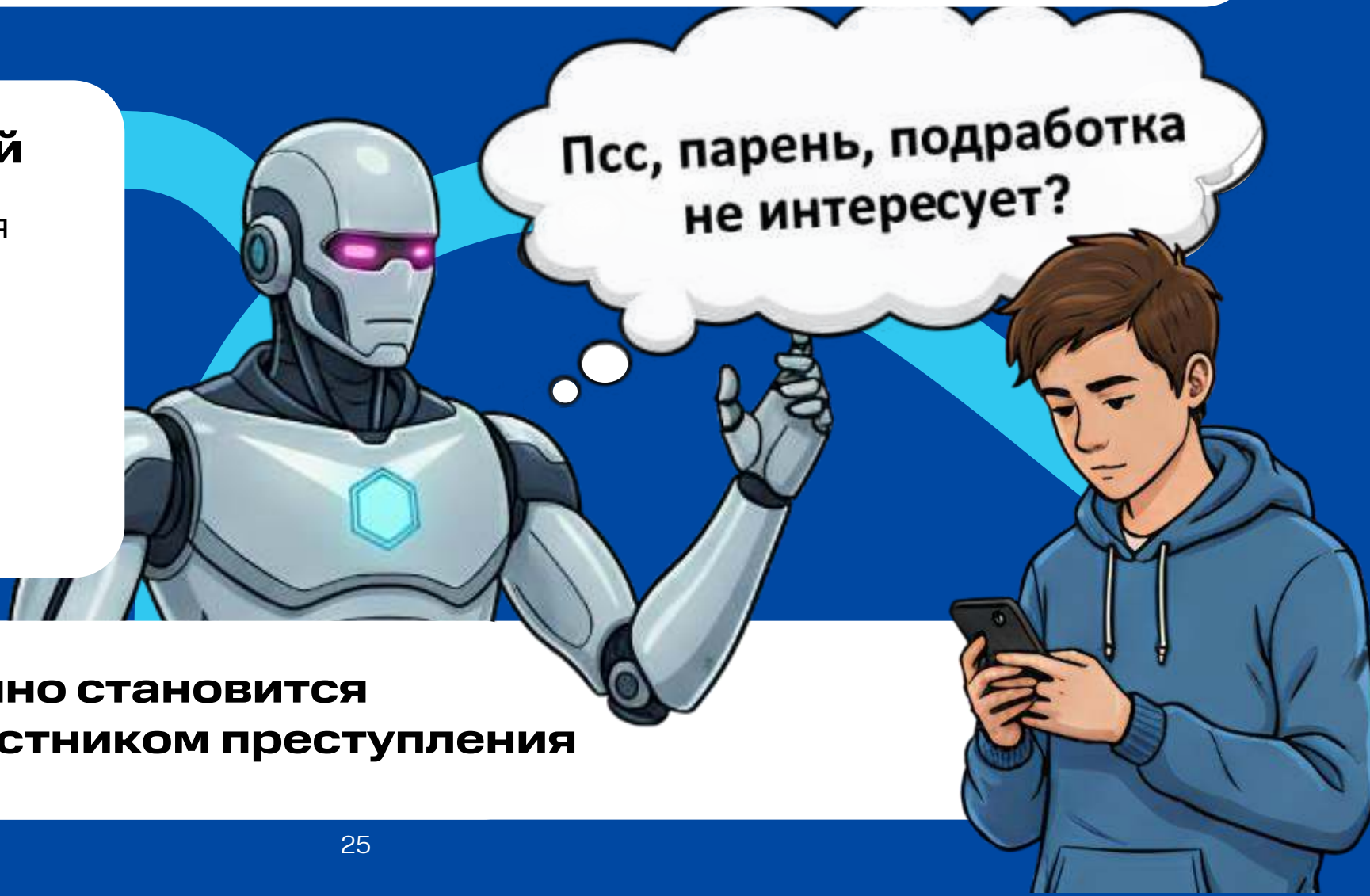


## «Простая подработка»



### Типичный сценарий

- без опыта и образования
- работа из дома, 2–3 часа в день
- обязательное условие — банковская карта или онлайн-банк



**Человек неосознанно становится дроппером и соучастником преступления**



# «Ошибочный перевод»



## Как работает схема

«Случайный»  
перевод  
поступает на счет

Звонок с просьбой  
срочно вернуть деньги  
на «правильный» счёт

Перевод денег  
по реквизитам  
злоумышленников

## Единственно верное решение

- Немедленно связаться с банком
- Действовать строго по его инструкциям

СМС от: Неизвестный абонент  
Сумма: 50 000 руб.

**СЛУЧАЙНО ОТПРАВИЛА,  
ПЕРЕШЛИТЕ ДЕНЬГИ  
ПО НОМЕРУ**



# «Администратор лотереи»



## Как выглядит вербовка

- Предлагают «техническую работу»
- Обязанность — распределять денежные призы «победителям»

## Что происходит на самом деле

- Нанятый человек становится дроппером
- Деньги на карте — похищенные средства у других жертв
- Переводы оформляются как «выигрыши», но уходят:
  - другим дропперам или подставным лицам
  - напрямую мошенникам



## Ключевая роль дроппера

- Дробит и «очищает» преступный денежный поток
- Существенно осложняет выявление схемы банками и правоохранительными органами



# Вербовка через соцсети



## Как находят жертву

- ИИ анализирует соцсети: посты о поиске работы, участие в розыгрышах
- Выбираются уязвимые люди

## Типичные легенды

- «Администратор донатов»
- Ассистент блогера или стримера
- Волонтер, принимающий пожертвования

## Как проходит вербовка:

- «Живой» аккаунт с украденными фото
- Сообщения с предложением подработки, помощи, «социального» проекта
- Убеждают в легальности схемы
- Просят переводить деньги через личную карту

**Ни одна легальная организация не использует карту случайного человека**



# ⇄ Уголовная ответственность в РФ ✕

## Статьи, предусматривающие наказание за дропперство

- **174 УК РФ** «Легализация (отмывание) денежных средств или иного имущества, приобретённых другими лицами преступным путём»
- **187 УК РФ** «Неправомерный оборот средств платежей»
- **159 УК РФ** «Мошенничество»

## Запомните главное:

- **Дропперство** — не «лёгкий заработок», а **уголовно наказуемое преступление**
- **Ответственность несут** как организаторы, так и **рядовые участники**





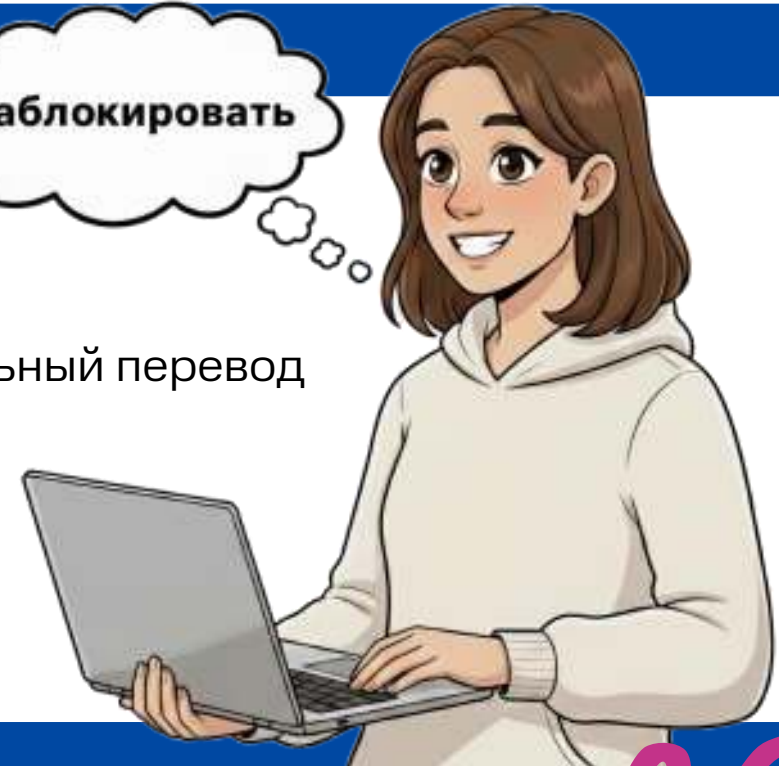
# Правила безопасности



## Если обнаружили признаки вербовки:

- Прекратите все контакты с мошенниками
- Ничего не переводите, даже если получили подозрительный перевод
- Заблокируйте карту и уведомите банк
- Сохраните переписку, реквизиты, номера мошенников
- Обратитесь в правоохранительные органы

Заблокировать



**Все предложения «лёгкого заработка» — подозрительны**

особенно если требуют персональные данные или доступ к банковским картам





# История и особенности



## Что такое криптовалюта:

- Цифровые деньги без участия госбанков
- Работает на блокчейне — децентрализованной таблице транзакций



**3 января 2009 г.**

сгенерирован первый блок Bitcoin

## Феноменальный рост стоимости

2009 г. | 1 цент

2025 г.  \$126 200

Доходность в прошлом ≠ доходность в будущем

## Основные криптоактивы

2026 г.



# Цифровой рубль vs Криптовалюта

## Цифровой рубль

- Дополняет наличные и безналичные средства
- Контролируется ЦБ РФ, доступ через мобильные приложения и интернет-банк
- Обязательная процедура КУС для защиты от мошенничества и отмывания денег

**Государственный  
и контролируемый актив**



## Криптовалюта

- Децентрализована — нет единого контроля государств или банков
- Используется как актив / имущество, не всегда законное средство платежа
- Псевдонимная: привязка к публичному адресу кошелька, риски безопасности

**Децентрализованный актив  
с высокой волатильностью**



# Криптовалюта и мошенничество X

## Доля преступных транзакций

2023 г.  0,61%

2024 г.  0,14%

## Субъекты с признаками нелегальной деятельности

Статистика ЦБ РФ

**3346**

январь–июнь 2024

**4183**

январь–июнь 2025

## Использование преступниками

- Наркотики, азартные игры, кража интеллектуальной собственности
- Отмывание денег, финансовые пирамиды
- Криптовалюта — способ привлечения средств и инвестиций с обещанием быстрого дохода

## Криптовалюта удобна молодежи,

но является инструментом мошенничества, особенно при использовании ИИ для массовости

# Мошеннический P2P-треугольник

## Как работает схема

### Фейковое объявление

Продажа товара по цене ниже рынка

### Подмена реквизитов

карта P2P-трейдера, а не продавца

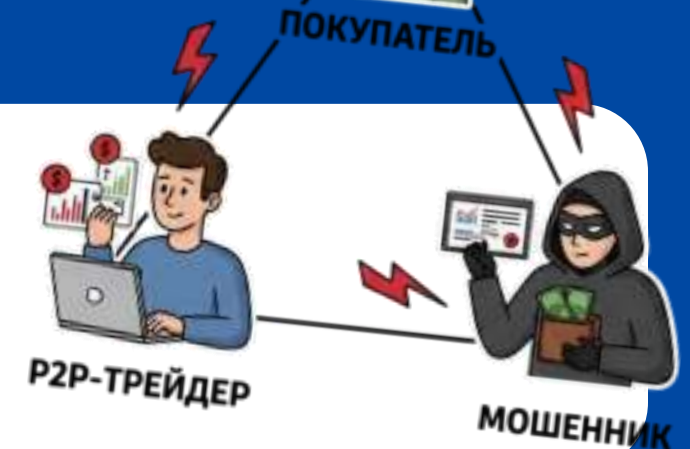
### Перевод денег P2P-трейдеру

покупка криптовалюты мошенникам



## Как снизить риски

- Проверять рейтинги и историю контрагентов
- Выбирать популярные и подтверждаемые способы оплаты
- Продавать товары только через проверенные торговые площадки





# Скам SQUID криптовалюта



## Что произошло

- Токен Squid обещали использовать в онлайн-игре по популярному сериалу
- **За 2 дня рост 44 000%, цена \$2860**
- Вскоре обесценился до 0
- **Мошенники вывели >3 млн \$,** пострадало 40 000+ инвесторов



## Сигналы опасности

- Невозможность продать токен
- Отсутствие листинга на известных биржах
- Ошибки на сайте

## Важно

- Перед инвестированием проверять создателей проекта и доступную информацию
- Осторожность и критическое мышление = защита от финансового мошенничества





# Пирамида Bitconnect



## Суть схемы

- **Маскировка** под криптоплатформу с ИИ для торговли
- **Обещание высокой прибыли** при минимальных рисках
- **Реферальная программа:** 7–15% от вкладов новых участников

## Последствия

- Пострадали инвесторы из **40+ стран**
- Убытки составили **>17 млн \$**

## Механизм обмана

- Деньги новых инвесторов → выплаты «прибыли» старым и бонусы → карманы организаторов
- Торгового робота не существовало

Гарантии высоких доходов  
+  
реферальные бонусы  
=  
явный сигнал  
финансового скама





# Финансовая пирамида Финико



## Суть схемы

- **Избавление от кредитов** через инвестиции
- Использование «математических моделей» и ИИ для «снижения рисков»
- Возможность купить квартиру или машину за **35% от стоимости**
- **Депозиты с доходностью 20–30% в месяц**

## Особенности

- Все операции проводились в биткоинах и Tether
- Пополнение счетов фиатными деньгами было запрещено
- Популярность схемы выросла за счет крупных «выгодных» предложений

**Высокие доходы + невозможность использовать обычные деньги = явный сигнал мошенничества**





# Правила безопасности



## Проверяйте легальность

- Все финансовые организации должны иметь лицензию ЦБ РФ
- Проверка через справочник:  
*cbr.ru/inside/warning-list*

## Главное правило

«Бесплатный сыр – только в мышеловке!»



## Признаки финансовых пирамид

- Нереалистичные обещания доходности, в разы выше рынка
- Реферальная программа
- Отсутствие лицензии и документов
- Агрессивная реклама и срочность («только сегодня!»)
- Непрозрачность: нет информации о руководстве или регистрации
- Прием наличных или криптовалюты без документов

# Главная цель злоумышленников

**Снизить бдительность  
и отключить критическое  
мышление жертвы**

Схемы меняются,  
суть остается прежней



# Фишинговые магазины и сайты



## Схема мошенников

Мошенники создают копии сайтов магазинов, авиакомпаний, банков и тп

Предлагают товары, билеты, путевки со скидкой, заманивая жертву

## Правила безопасности

Покупайте только через официальные приложения



Не переходите по ссылкам из писем



Проверяйте, что сайт использует **https**, а не **http**



Отдельная карта для онлайн-покупок



Проверьте ошибки в тексте и имени сайта



Используйте антивирусное ПО



# ⇄ Доставка цветов и «Госуслуги» ✕

## Схема мошенников

### Звонок

«службы доставки»

назвать из СМС код  
«подтверждения»

### Звонок

«Роскомнадзора»

сообщают о якобы  
небезопасной ситуации



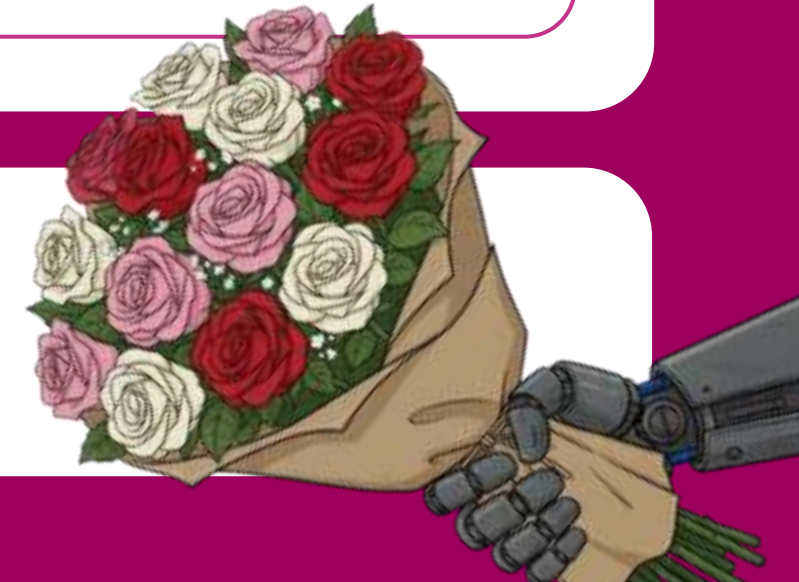
### Второй звонок

«службы безопасности»

помочь восстановить  
доступ к «Госуслугам»

## Правила безопасности

- Никогда не сообщайте SMS-коды – это коды для микрозаймов
- Спросите себя: ждали ли вы доставку? Если нет → аферисты



# ↔️ Блокировка карт с помощью ИИ ❌

## Схема мошенников

### Звонят в банк от «клиента»

Называют личные данные,  
с ИИ имитируют голос

### Блокируют карту

Причины: потеря,  
кража и прочее

### Угрожают жертве

Требуют деньги



## Правила безопасности

Звоните в банк только  
по официальному номеру

Ни при каких условиях  
не переводите деньги

Расскажите о схеме  
всем родственникам



# Глобальная проблема



## Взрослое население мира

**57%**

столкнулись  
с мошенничеством

**54%**

пострадали при  
онлайн-покупках

**48%**

от инвестиционного  
мошенничества



## Психологические последствия

**69%**

испытывают  
сильный стресс

**14%**

ухудшились  
отношения в семье

**17%**

теряют уверенность  
в себе



## Главный щит – критическое мышление и цифровая грамотность

- Почти каждый 4-й, считающий себя осторожным, всё равно теряет деньги
- Мошенники постоянно совершенствуют тактики и базовой бдительности уже недостаточно

# Международная олимпиада по финансовой безопасности



## Олимпиадные задания составлены на основе программ

### Школьники

- Математика
- Информатика
- Обществознание

### Студенты

- Международные отношения, зарубежное регионоведение
- Экономика, финансы, экономическая безопасность
- Математика, информационная безопасность
- Юриспруденция

## Призы и преимущества

- ✓ **Льготы при поступлении в вузы**  
Международного сетевого института  
(бакалавриат, магистратура, аспирантура)

- ✓ **Возможность стажироваться**  
в Росфинмониторинге  
и других организациях





rosfinolymp.ru

# Международная олимпиада по финансовой безопасности



sodrujestvo.org

Тематический урок  
«Финансовая  
безопасность»

*10 февраля —  
30 апреля*

**Отборочный  
этап**

**1 тур**      **2 тур**  
*14-17 марта    19-21 апреля*

**Квалификационный  
этап**

**Студенты**      **Школьники**  
*1-19 июня      2-3 сентября*

Зимняя школа  
по финансовой  
безопасности

*Ноябрь —  
декабрь*

**Пригласительный  
этап**

*02 февраля — 10 марта*

Летняя школа  
по финансовой  
безопасности

*Июль*

**Финальный  
этап**

*Сентябрь*



# Партнеры



ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ФИНАНСОВОМУ  
МОНИТОРИНГУ



МИНИСТЕРСТВО  
ПРОСВЕЩЕНИЯ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ



МИНИСТЕРСТВО  
ВНУТРЕННИХ ДЕЛ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ



РУДН



МИНИСТЕРСТВО НАУКИ  
И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ  
ФЕДЕРАЦИИ

**МУМЦБМ**

содружество



ЦЕНТР  
МЕЖОЛИМПИАДНОЙ  
ПОДГОТОВКИ