International Financial Security Olympiad

The Dark Side of AI

#Artificial intelligence

Artificial intelligence

Computer systems capable of performing tasks characteristic of human intelligence

AI — is technologies that allow systems to

- understand queries formulated in natural language
- analyze, process and find necessary data
- recognize images, symbols and patterns
- learn from large data streams
- make decisions and adapt to different conditions

Where AI is applied

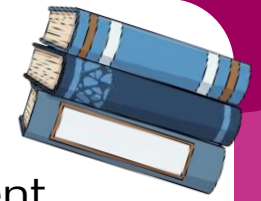
Medicine and Healthcare

- Individual treatment schemes
- Development of new drugs
- Data analysis

Banking Sector

- Automatic investments
- Credit scoring and risk assessment
- Operational decision-making

Education



- Adaptation of material to the student
- Identifying knowledge gaps
- Creating additional tasks

Science and Research

- Fast search for patterns
- Accelerating research
- Finding solutions based on analysis

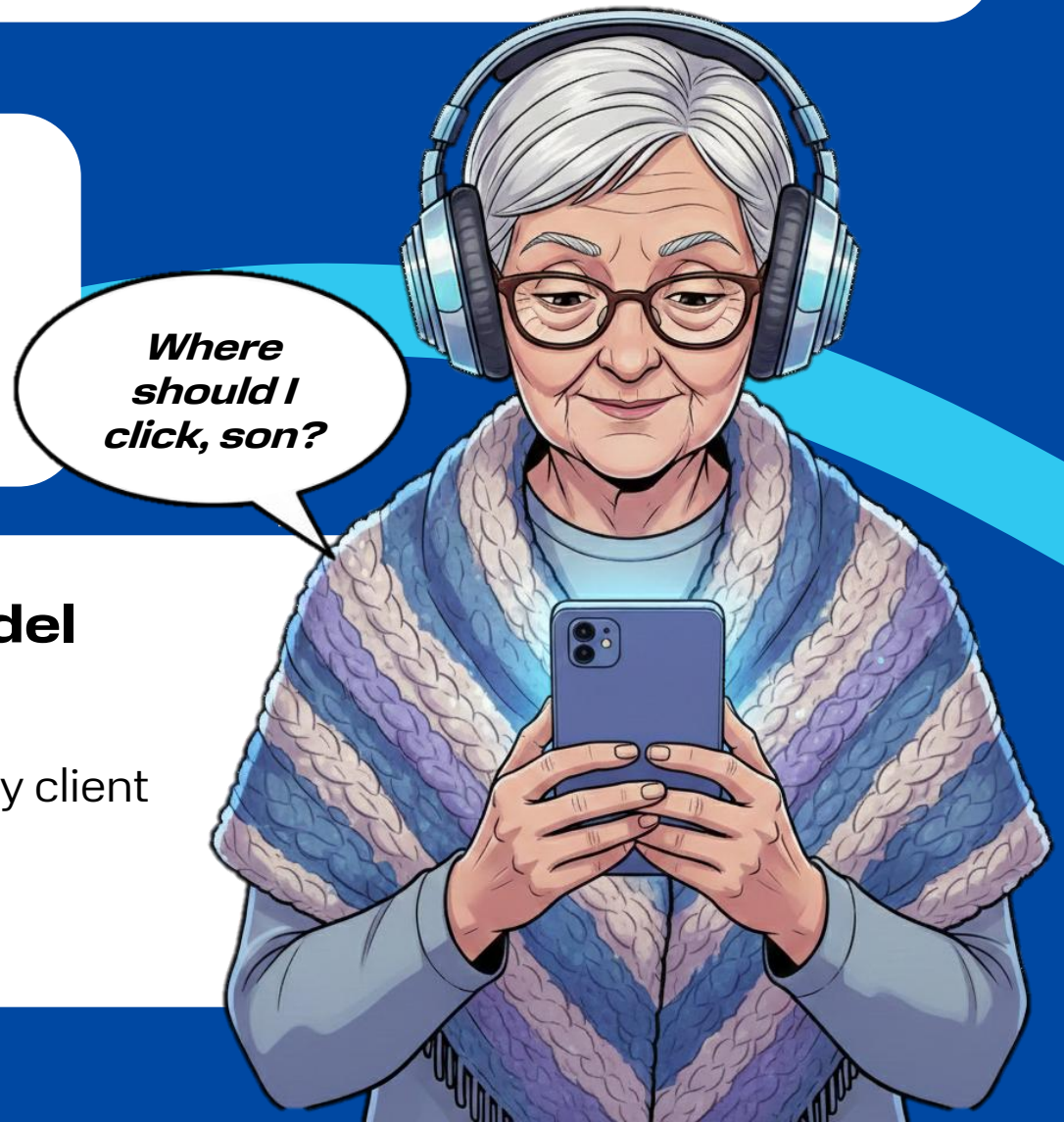
Cybersecurity protection

How AI counteracts scammers

- identifies and intercepts fraudulent schemes
- reduces the burden on real victims

Example: "Cyber Grandma" — an AI model from a mobile operator

- communicates with scammers on behalf of an elderly client
- distracts attackers from real people,
  wastes their time and resources



The Flip Side of AI

Financial Threats

- Growth of cyber fraud using AI
- Theft of funds and data
- Automation of criminal schemes

Special Risk Zone

- Increase in the number of minor victims
- Attacks via calls and messages (schools, government agencies, communication operators)
- Fraud with game accounts and state exams

Transactions without client consent

27,5 Bln Rbl — 2024

21 Bln Rbl — 9 month. 2025

Prevented Thefts

222 Mln Rbl

November 2025

Counteraction

- Rosfinmonitoring
- Financial intelligence of CIS countries
- Eurasian Group on AML/CFT

Money Laundering

Cyberfraud

Dummy bank accounts

Multiple transfers,
commingling of funds

Obfuscation of financial flows

Crypto platforms

Money laundering/financing of criminal activity

The threat is transnational in nature

Who is a dropper?

Dropper

a person who uses their cards
for cashing out or transiting (further sending) stolen funds

Involvement of youth

Who gets involved

- Teenagers from 14 years old students and schoolchildren unemployed

Over 1 million droppers

Scale of the problem in Russia

data from the Bank of Russia

How they get involved (psychological tricks):

- **urgency** — "only today“
- **simplicity** — "anyone can handle it“
- **imaginary legality** — "it's all legal“
- **gradualness** — from small amounts to large ones
- **social proof** — "hundreds are already working"

Responsibility

Direct criminal liability

established for dropper schemes in addition to Art. 187 of the Criminal Code of the Russian Federation

Repercussions

- **up to 3 years** imprisonment — for transferring bank details
- **up to 6 years** imprisonment — for organizers (drop guides)

Practice of application

- In 2025 the first criminal case against a drop guide was initiated
- Cooperation with the Ministry of Internal Affairs — grounds for exemption from liability
- Organizer identified from testimony of detained dropper

Deepfake

Deepfake

video, audio or photo created by AI,
in which a person does or says something
that never happened

How this works

- Calls disguised as surveys and voice recordings
- AI copies a person's face and voice
- Creation of voice deepfakes

A few seconds of recording is enough to create a voice deepfake.

The first high-profile case

2019, UK

Scammers used AI to copy the voice of an energy company CEO

Attack scheme

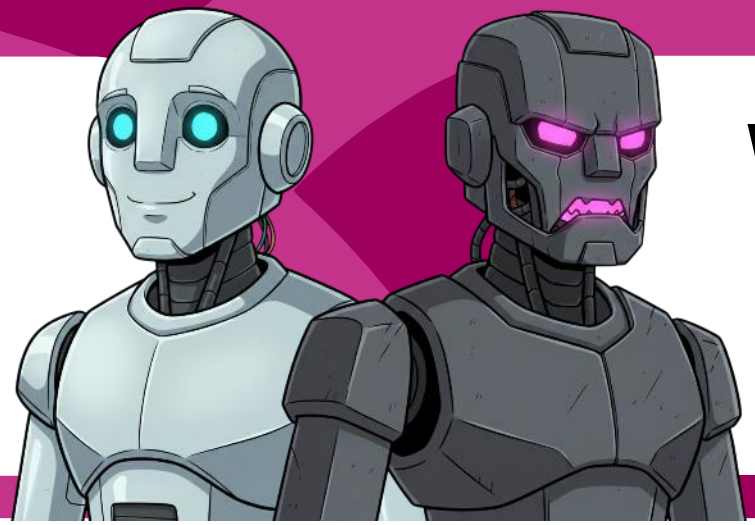
„CEO‘s" calls a subordinate
with an urgent order to transfer funds to a supplier

€220 000
transferred to scammers' account

«Evil Twin»

Nature of the attack

Fake Wi-Fi network, copying a real one



What is stolen

- logins and passwords
- bank card details
- correspondence and browser history

Как работает схема

Network cloning
same SSID, stronger signal

→

Victim connection
cafes, airports, shopping centers

→

Man-in-the-Middle
interception of all traffic

→

Phishing
fake login page

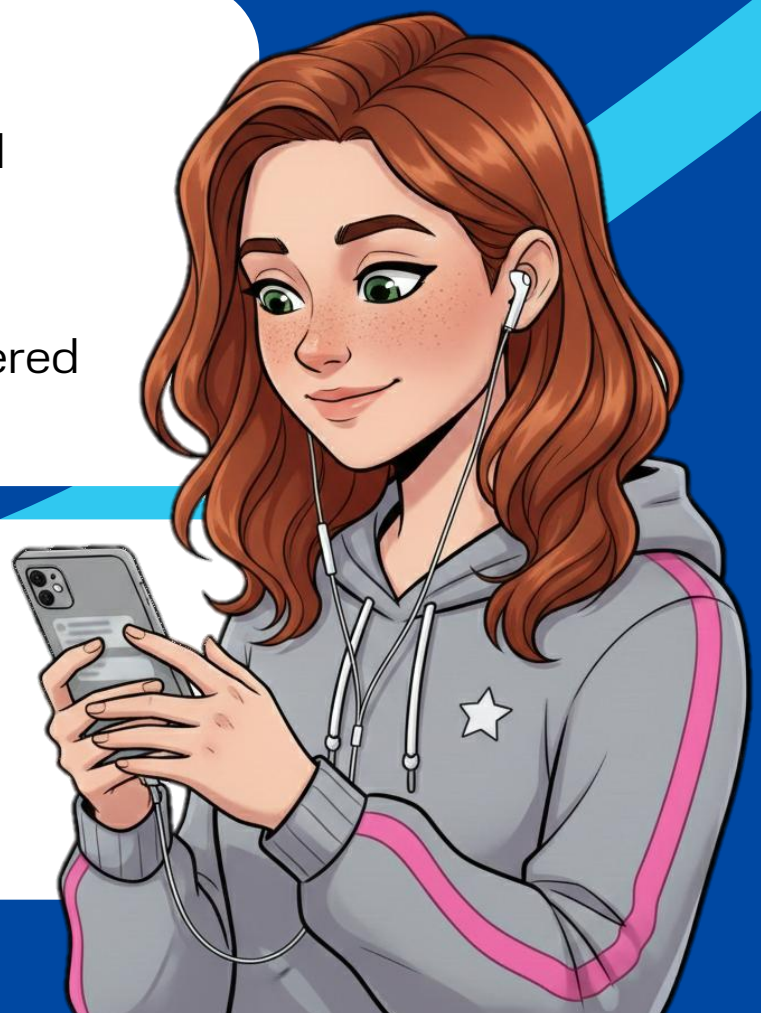
«Evil Twin» at the airport

Case

- A schoolgirl connected to Wi-Fi with the airport's name
- The network was first in the list
- The code turned out to be a one-time password

Critical mistakes

- Warnings about unsecured network ignored
- Phone number entered
- Code from messenger entered



Results

- Loss of access to messenger
- Compromise of personal data

Important!

Codes from messengers are never entered when registering for Wi-Fi

AI-Phishing

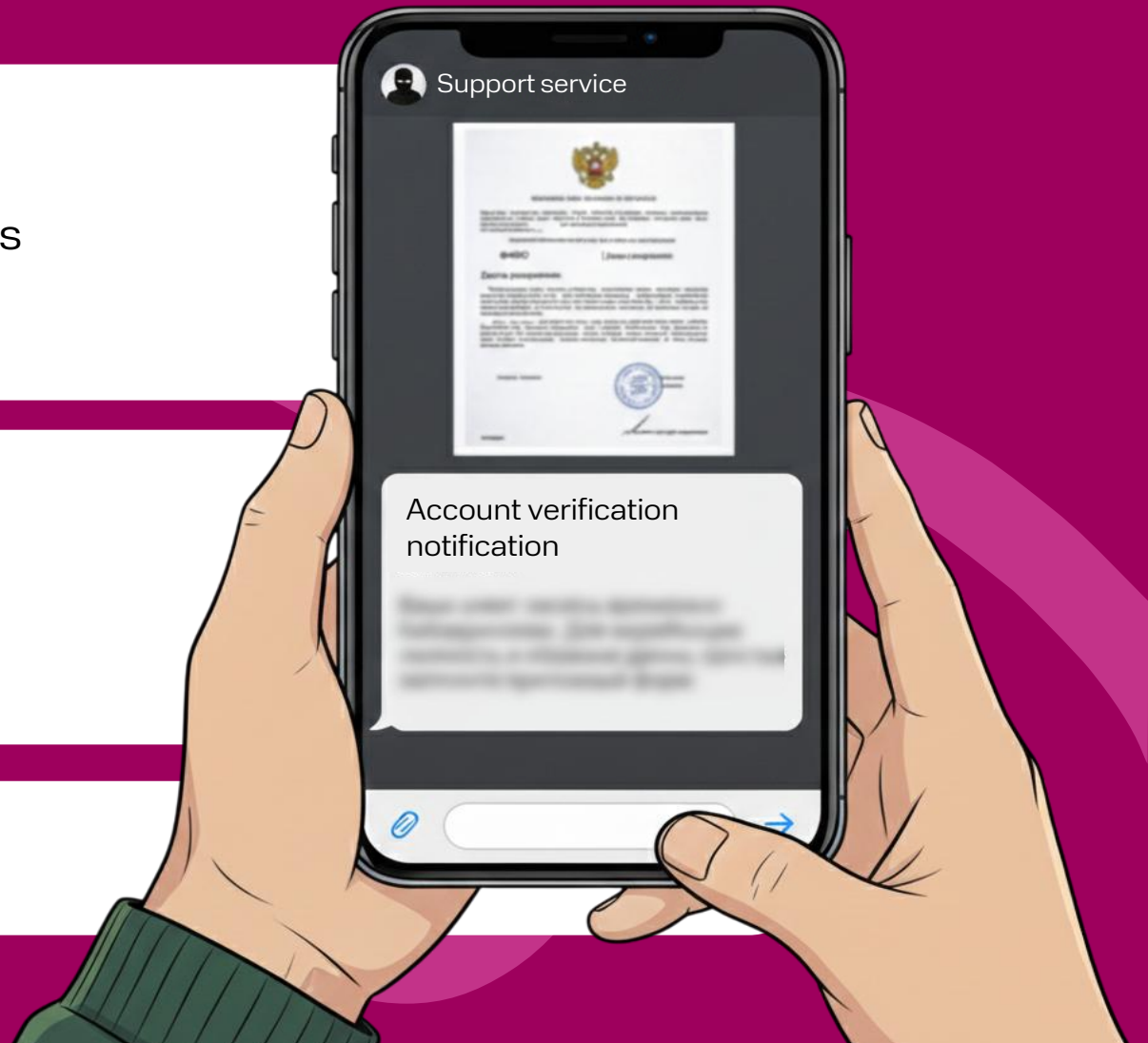
Before starting work, AI

- analyzes data from social networks, websites, leaks
- generates "ideal" letters and messages

Sends personal messages

- without errors and stock phrases
- looks like real official communication

Result – loss of money



AI-Vishing

AI-Vishing

(vishing = voice + phishing)

- Voice variant of deepfake
- AI copies a voice from a few seconds of recording
- Allows you to conduct a dialogue with the victim

AI makes fraud maximally realistic

Romance Scam

Nature of the Attack

- AI conducts conversations with thousands of people simultaneously
- Creates an illusion of trust, uses social media data to personalize communication

How the scheme works

Chat conversation
personal questions, voice messages

→

Investment offer
bets, cryptocurrency, financial pyramids

→

Demonstration of "success"
via photos, screenshots, gifts

Safety on public Wi-Fi

Do not use unsecured networks

"Evil twins" are almost always open

Never enter passwords or card details

Public Wi-Fi intercepts traffic

Use only HTTPS sites

Padlock icon → connection is protected by end-to-end encryption

Pay attention to warnings

They signal a real threat

Enable multi-factor authentication (MFA)

Password + one-time code

Do not panic!!

A simple but reliable way to protect against AI voice forgery

1. **Hang up** at the first suspicion
2. **Call back a relative or friend** from your phonebook to check
3. **Use a family code word** to verify identity
4. **Ask personal questions,** known only to close ones (e.g.: "What is our dog's name?")

Observe digital hygiene!

How not to let AI clone your voice

- **Restrict access to social networks** (only for friends)
- **Do not post** voice recordings in public access (statuses, streams, messengers)

Control your emotional state

- Any information causing strong emotions and requiring immediate action, is most likely a deception
- Discuss the situation with loved ones

The main weapon is critical thinking

Remember: government agencies (Central Bank of the Russian Federation, FSB, Federal Tax Service) do not resolve "important issues" over the phone

Cut off suspicious contacts

How to act if you encounter fraud

- Stop the conversation when money, bets, cryptocurrencies are mentioned
- Use critical thinking
- Block the scammer
- Do not transfer any money to a person you have not met in person
- If necessary — report to law enforcement agencies and the platform administration

Romance scam is a game of trust,

and the final stake is your money

Droppers — intermediaries in financial schemes of scammers

Who are the drops

- People accepting stolen money
- Transfer or withdraw money for handlers
- Pass a card with online banking access

Drops participate in a criminal offense

**"Acquisition or transfer of a card by persons who are not bank clients" –
for this violation the penalty is: imprisonment for up to 6 years with a fine.**

Article 187 of the Criminal Code of the Russian Federation "Illegal circulation of means of payment"

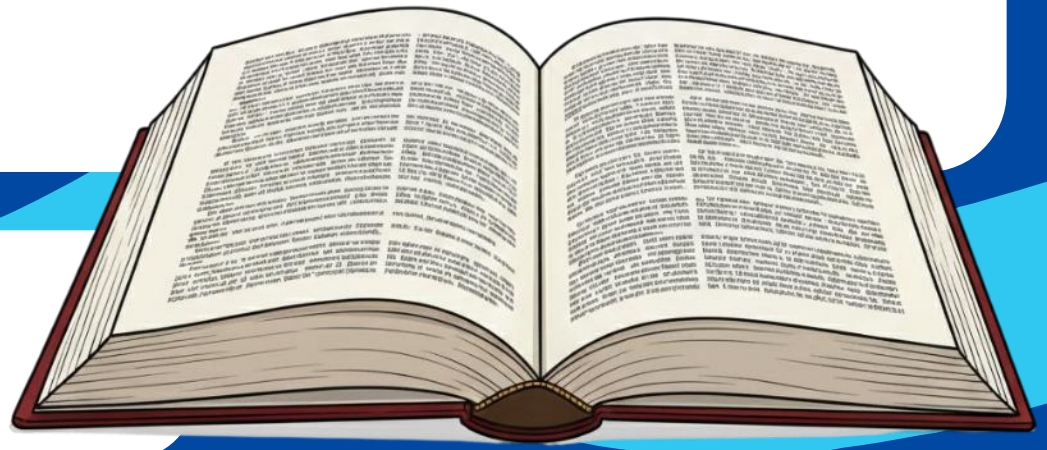
Dropper statistics in the Russian Federation

> 1 mln
drop-clients
in banks

~ 20%
teenagers unaware of the
consequences

Droppers are an important link in the laundering of stolen funds

may be subject to criminal liability under **Article 174 of the Criminal Code of the Russian Federation "Legalization (laundering) of funds or other property acquired by other persons through criminal means"**



Awareness and caution are critical

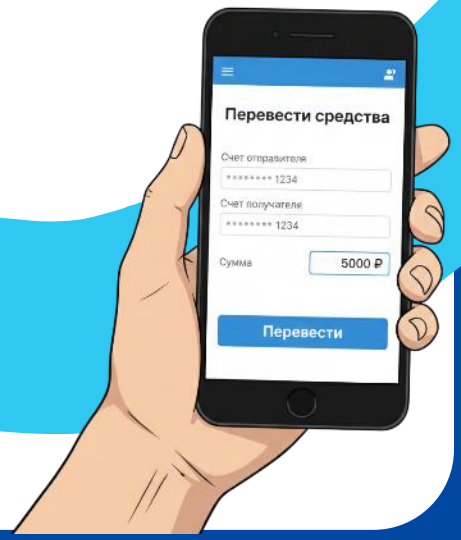
Types of droppers by function

Pourers

- receive cash → deposit into account → transfer onwards

Transiters

- receive transfers → redirect to other accounts or wallets



Cashers

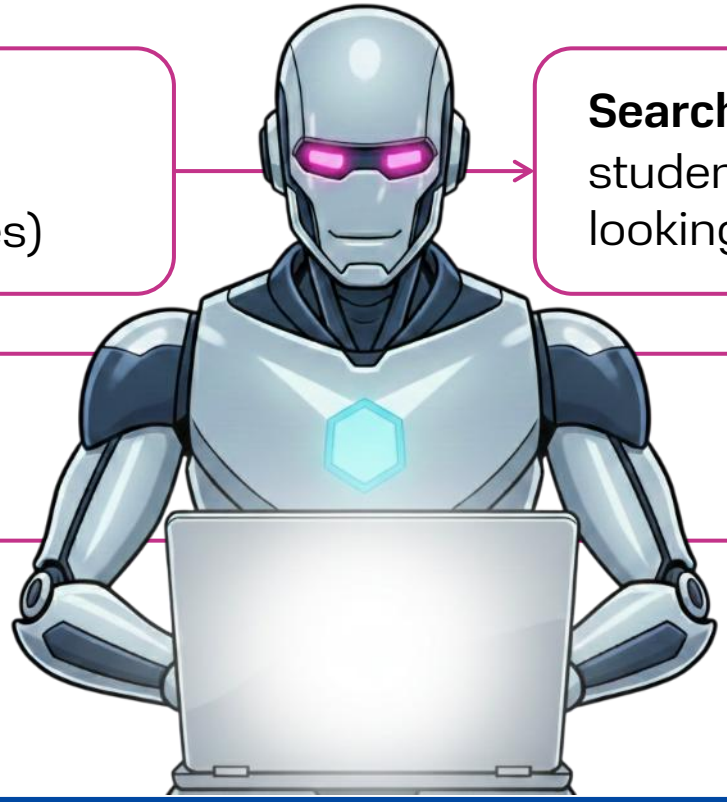
- withdraw money from ATMs → hand over to organizers

Recruitment of droppers using AI

Как работает схема

Neural networks and NLP
analyze open sources (social networks, forums, marketplaces)

Search for vulnerable groups
students, unemployed people, looking for "easy income"



Assessment of victim‘s psychology
posts, communication style → suggestibility, greed

Initial contact
chat bots, use of deepfake avatars

«Simple Part-time Job»

Typical Scenario

- No experience or education required
- Work from home, 2-3 hours a day
- A bank card or online banking required

A person unknowingly becomes a dropper and an accomplice to a crime

«Erroneous Transfer»

How the scheme works

" Random" transfer
received into account

→

Call with a request
to urgently return the money to the "correct" account

→

Transfer of money
using the attackers' details

The only right decision

- Contact your bank immediately
- Follow their instructions strictly.

SMS from: Unknown subscription
Amount: 50,000 rubles

Accidentally transfered, please forward the money to this number

«Lottery Administrator»

What does recruitment look like?

- They offer "technical work"
- The job is to distribute cash prizes to the "winners."

What's really going on

- The hired person becomes a dropper
- The money on the card is stolen funds from other victims
- Transfers are registered as "winnings," but go:
  - to other droppers or front men
  - directly to the scammers

Key role of the dropper

- Fragments and "cleanses" the criminal money flow
- Significantly complicates detection of the scheme by banks and law enforcement

Recruitment via social networks

Recruitment via social networks

- AI analyzes social networks: posts about job search, participation in giveaways
- Vulnerable people are selected

How recruitment happens:

- "Live" account with stolen photos
- Messages offering part-time work, help, a "social" project
- Convince of the scheme's legality
- Ask to transfer money via personal card

Typical legends

- "Donation Administrator"
- Assistant to a blogger or streamer
- Volunteer accepting donations

No legitimate organization uses a random person's card

Criminal liability in the Russian Federation

Articles providing for punishment for droppering

- **Article 174** of the Criminal Code of the Russian Federation "Legalization (laundering) of funds or other property acquired by other persons through criminal means"
- **Article 187** of the Criminal Code of the Russian Federation "Illegal circulation of payment instruments"
- **Article 159** of the Criminal Code of the Russian Federation "Fraud"

Remember the main thing:

- **Dropping** is not "easy money," but a **criminal offense.**
- **Both** organizers **and ordinary participants bear responsibility.**

Safety rules

If signs of recruitment are detected :

- Stop all contact with the scammers
- Do not transfer anything, even if you receive a suspicious transfer
- Block your card and notify the bank
- Save the correspondence, details, and phone numbers of the scammers
- Contact law enforcement

All offers of "easy money" are suspicious

especially if they require personal data or access to bank cards

History and features

What is cryptocurrency:

- Digital money without the participation of state banks
- Operates on blockchain — a decentralized transaction ledger

January 3, 2009.

first block of Bitcoin generated

Phenomenal value growth

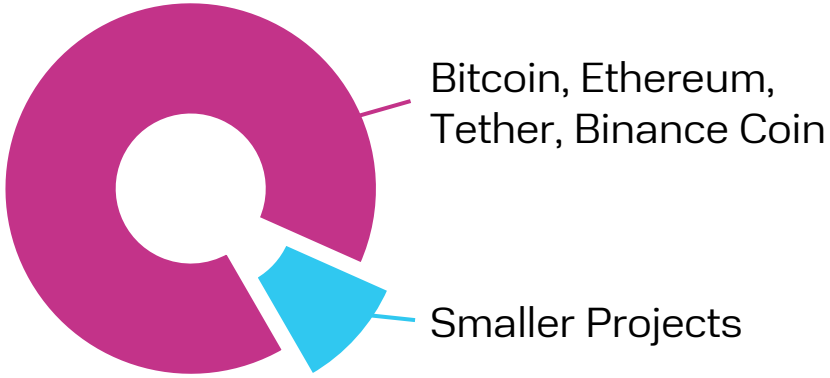
2009 | **1 cent**

2025 **$126 200**

Past performance ≠ future performance

Primary Cryptoassets

2026

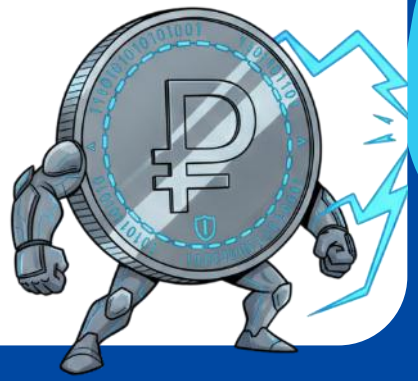


Digital Ruble vs Cryptocurrency

Digital Ruble

- Complements cash and non-cash funds
- Controlled by the Central Bank of the Russian Federation, access via mobile apps and internet banking
- Mandatory KYC procedure to protect against fraud and money laundering

A state-controlled and regulated asset



Cryptocurrency

- Decentralized - no single control by states or banks
- Used as an asset/property, not always legal tender
- Pseudonymous: linking to a public wallet address, security risks

A decentralized asset with high volatility

Cryptocurrency and fraud

Share of criminal transactions

Entities with signs of illegal activity

Statistics of the Central Bank of the Russian Federation

3346
Jan–Jun 2024

4183
Jan–Jun 2025

Use by criminals

- Drugs, gambling, intellectual property theft
- Money laundering, financial pyramids
- Cryptocurrencies — a way to attract funds and investments with promises of quick income

Cryptocurrency is convenient for young people,

but it is a tool for fraud, especially when using AI for mass reach

Fraudulent P2P Triangle

How the scheme works

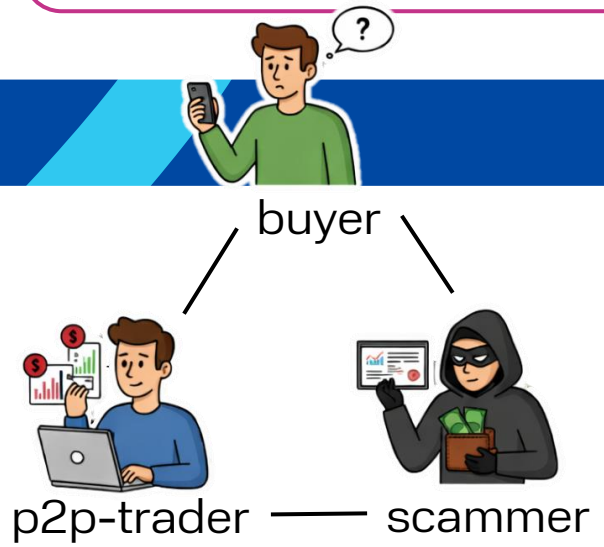
Fake ad
Selling goods
at below-market price

→

Replacement of details
P2P trader's card,
not the seller's

→

Transfer money to P2P trader
cryptocurrency purchase
for fraudsters



How to reduce risks

- Check counterparty ratings and history
- Choose popular and verifiable payment methods
- Sell goods only through trusted trading platforms

SQUID Cryptocurrency Scam

What happened

- The Squid token was promised to be used in an online game based on a popular series
- **In 2 days, growth 44,000%, price $2860**
- Soon depreciated to 0
- **Fraudsters withdrew >$3 million**, 40,000+ investors suffered

Danger signals

- Inability to sell the token
- No listing on major exchanges
- Errors on the website

Important

- Before investing, check the project creators and available information
- Caution and critical thinking = protection from financial fraud

Bitconnect Pyramid

Nature of the scheme

- **Disguise** as a crypto platform with AI for trading
- **Promise of high profits** with minimal risks
- **Referral program**: 7-15% from deposits of new participants

Consequences

- Investors from **40+ countries** suffered
- Losses amounted to **17 million$**

Mechanism of deception

- Money from new investors → payments of "profits" to old ones and bonuses → organizers' pockets
- The trading robot did not exist

Guarantees of high income
+
referral bonuses
=
a clear signal of financial scam

Finiko Financial Pyramid

Nature of the scheme

- Getting rid of loans through investments
- Use of "mathematical models" and AI to "reduce risks“
- Opportunity to buy an apartment or car for **35% of the cost**
- **Deposits with a yield of 20-30% per month**

Features

- All operations were conducted in Bitcoins and Tether
- Account replenishment with fiat money was prohibited
- The scheme's popularity grew due to large "profitable" offers

High income + inability to use ordinary money = a clear signal of fraud

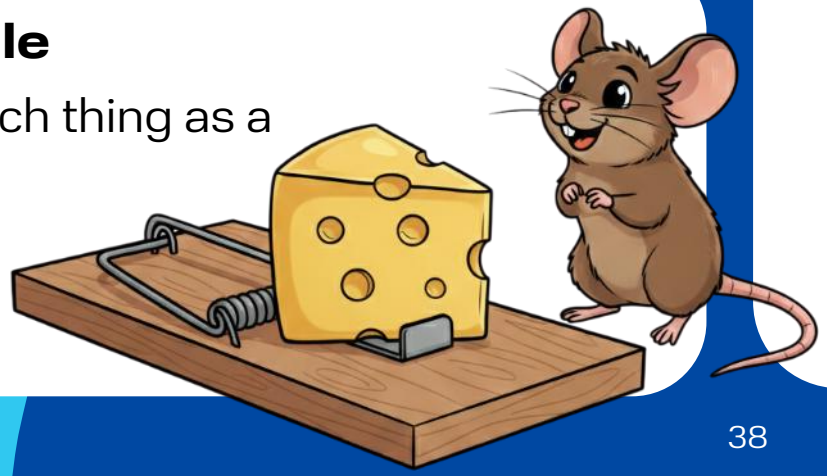
Safety Rules

Check legality

- All financial organizations must have a license from the Central Bank of the Russian Federation
  Check via the directory:
  cbr.ru/inside/warning-list

The main rule

"There is no such thing as a free lunch!"



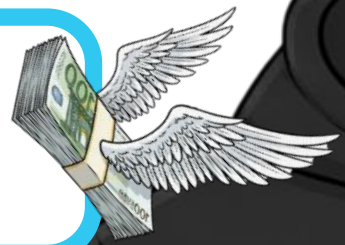
Signs of a Financial Pyramid

- Unrealistic promises of profitability, many times higher than the market
- Referral program
- Lack of license and documents
- Aggressive advertising and urgency ("only today!")
- Opacity: no information about management or registration
- Acceptance of cash or cryptocurrency without documents

The main goal of attackers

Reduce vigilance and disable the victim's critical thinking

Schemes change,
the essence remains the same



Phishing Stores and Sites

Scammer's Scheme

Scammers create copies of store websites, airlines, banks, etc.

→ They offer goods, tickets, tour packages at a discount, luring the victim

Правила безопасности

Buy only through official apps

Do not follow links from emails

Check that the site uses https, not http

Separate card for online purchases

Check for errors in the text and site name

Используйте антивирусное ПО

Flower Delivery and "Gosuslugi"

Scammer's Scheme

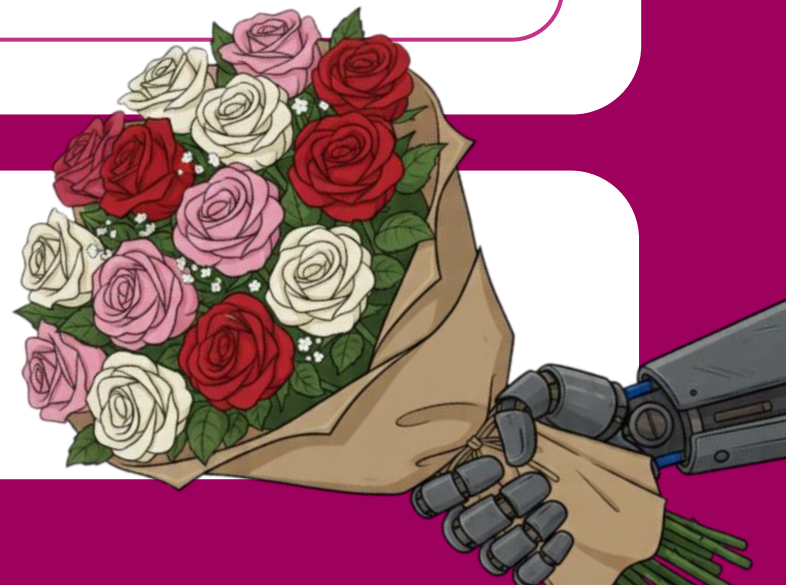
Call from "delivery service"»
provide SMS code for "confirmation"

→

Call from "Roskomnadzor"
report an allegedly unsafe situation

→

Second call from "security service"
help restore access to "Gosuslugi"



Safety Rules

- Never disclose SMS codes – these are codes for microloans
- Ask yourself: were you expecting a delivery? If not → fraudsters

Card Blocking Using AI

Fraudster's Scheme

Call the bank as the "client"
Provide personal data, imitate voice with AI

→

Block the card
Reasons: loss, theft, etc.

→

Threaten the victim
Demand money

Safety Rules

Call the bank only on the official number

Under no circumstances transfer money

Tell all relatives about the scheme

Global Problem

Adult population of the world

57%
encountered fraud

54%
suffered during online purchases

48%
from investment fraud

Psychological consequences

69%
experience severe stress

14%
family relationships worsened

17%
lose self-confidence

The main shield is critical thinking and digital literacy

- Almost 1 in 4, who consider themselves cautious, still lose money
- Fraudsters constantly improve tactics and basic vigilance is no longer enough

International Financial Security Olympiad

Olympiad tasks are based on programs

School students

- Mathematics
- Computer Science
- Social Studies

University students

- International Relations, Foreign Regional Studies
- Economics, Finance, Economic Security
- Mathematics, Information Security
- Law

Prizes and benefits

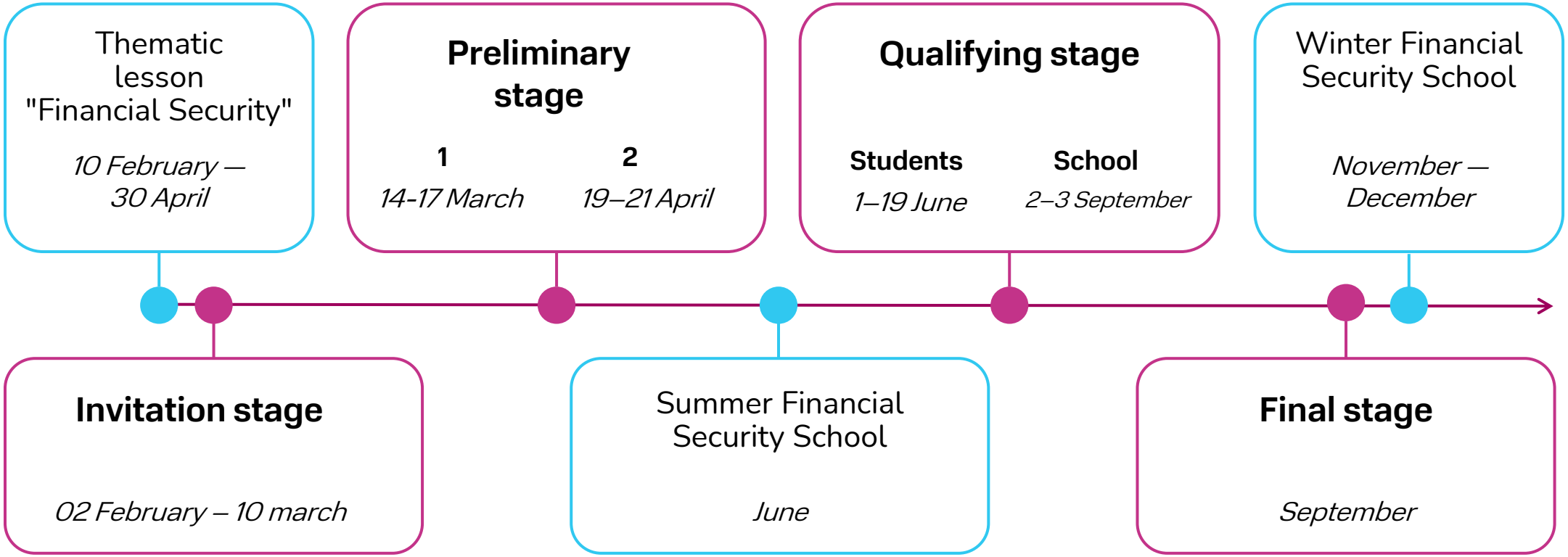
✓ **Benefits for admission to universities**
International Networking Institute (bachelor's, master's, and postgraduate programs)

✓ **Opportunity to intern at Rosfinmonitoring and other organizations**

rosfinolymp.ru

International Financial Security Olympiad

sodrujestvo.org



Partners

FEDERAL SERVICE FOR FINANCIAL MONITORING

MINISTRY OF EDUCATION OF THE RUSSIAN FEDERATION

MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION

РУДН

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION

МУМЦУМ

содружество

ПСБ

ЦЕНТР МЕЖОЛИМПИАДНОЙ ПОДГОТОВКИ