

Guidelines for the presentation of the thematic lesson

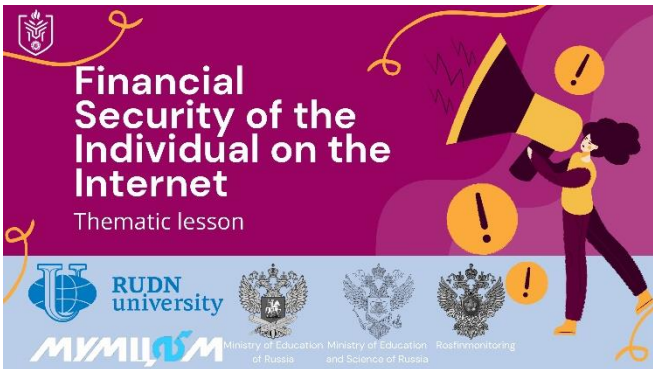
Financial Security of epy Individual on the Internet

The goal of the lesson is to develop the students' basics of financial security

Tasks:

- to develop students' beliefs that financial literacy and financial security both personal (family) and state are the basis of financial well-being;
- to get the students acquainted with the patterns of competent financial behavior, to present the basic financial concepts, to work out an algorithm for solving difficult life situations fraught with the danger of becoming a victim of pyramid schemes;
- to develop the students' comprehension of financial risks in the current economic situation; awareness of the danger of pyramid schemes and ways of discerning them; understanding of the systemic correlation between personal financial security and the financial security of the state; realizing the danger of financial crimes for the state and citizens.

The methodological material is advisory in nature; the teacher can vary the tasks, their number, change the stages of the lesson taking into account the characteristics of the students.

Slide	Commentary for the teacher
<p style="text-align: center;">SLIDE 1</p>  <p style="text-align: center;">SLIDE 2</p>	<p>According to statistics from the National Financial Research Agency (NAFI) ¹, only 10% of the population in Russia demonstrate a consistently high level of financial literacy. Notably, the most financially literate people in Russia are men and women aged 40-49 with higher education, as well as major cities residents.</p> <p>Every second representative of young people (53%) believes that he lacks knowledge about financial security: according to 48% of respondents, they have some knowledge in this area, but it is not enough to protect them from fraud, and 5% say that they have no knowledge about the safe dealing with finances at all. Teenagers aged 14 to 17 are more often unsure of their knowledge (53%).</p> <ul style="list-style-type: none"> • Financial security is a notion that includes a set of measures, methods and means to protect the economic interests of the state at the macro level, as well as corporate structures, financial activities of business entities at the micro level. This definition enables us to distinguish between the levels of financial security: • national, that is, the financial security of the entire state; • regional, i.e., the security of certain parts of the state; • corporate, i.e., financial security of organizations; • personal, i.e., the financial security of a single individual, or personal financial security. <p>Personal financial security is the socio-economic ability of a person to have financial independence to meet their material and spiritual needs, both individually and within a society, as well as preservation of this independence in the future and its further expansion. In other words, personal financial security means independence and stability and that is why it is so important to know how to ensure it for every individual.</p> <p>The financial security of the state is a broader notion. It represents the state of the financial and credit sphere, characterized by balance, resistance to internal and external negative impact, the ability to ensure effective</p>

¹ Data from the portal My Finances. <https://xn--80apaohbc3aw9e.xn--p1ai/article/finansovaya-gramotnost-rossiyan-vyroslo-za-poslednie-4-goda/> (date of access: 01/19/2023).

Statistics 2022

2

Percentage	Belief
47%	Only 47% of teenager respondents believe they have enough knowledge to avoid financial risks in everyday life
48%	48% of teenager respondents note that they have some knowledge, but it is not enough to avoid financial risks
5%	5% of teenager respondents believe that they do not have the knowledge to avoid financial risks - not to become a victim of scammers, to ensure the safety of their savings

SLIDE 3

Financial Security

3

the concept that includes a set of measures, methods and means to protect the economic interests of the state at the macro level, corporate structures, financial activities of business entities at the micro level.

- National**
financial security of the entire state
- Regional**
the security of certain parts of the state
- Corporate**
financial security of organizations
- Personal (family)**
individual security

SLIDE 4

Financial Fraud

4

the commission of illegal actions in the field of monetary circulation by deceit, breach of trust and other manipulations for the purpose of illegal enrichment.

- bank cards fraud
- Internet fraud
- mobile phones fraud
- financial pyramids

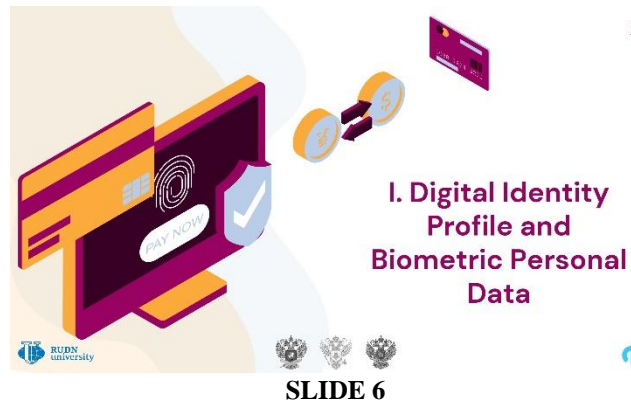
functioning of the national economic system and economic growth, and the level of protection of financial interests at the macro and micro levels of financial relations. This can be only achieved by ensuring the proper level of financial security of an individual and organizations.

Assignment

Analyze the data on slides No. 2-4 and answer the questions

1. Comment on the diagram data on slide No. 2. What conclusions can be drawn from the information provided?
2. Study slide No.3. What is personal financial security? Is personal financial security related to national one? Discuss it.
3. Does a modern person need to learn financial security and financial literacy? List at least three reasons why financial literacy is important to you.
4. Drawing on the information on slide No.4, answer the question How do you think, financial fraud and financial security are related? Provide arguments for your answer.

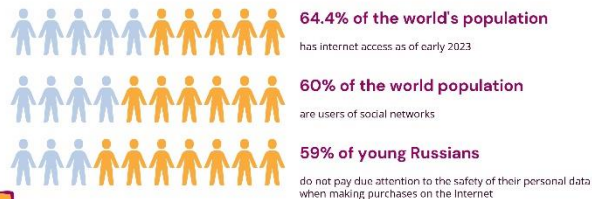
SLIDE 5



SLIDE 6

Global Digital Statistics 2023

use of the World Wide Web and the safety of personal data on the Internet



Think and Discuss:

What conclusions can be drawn from the above data?



5

6

Against the background of digitalization of all spheres of our life, young people are becoming active users of financial services on the Internet. Thus, every third teenager uses a non-cash payment method, and every second makes purchases via a smartphone.

A relatively high level of digital literacy and smartphones allow teenagers to use mobile and Internet banking (56% and 38%, respectively).

Despite the fact that cash remains the most common payment method for teenagers (42%), a large proportion of them make purchases non-cash (32%). Nearly half of teenagers (43%) make contactless payments via their smartphones.

A number of misbeliefs in terms of financial security are common among the Russian youth².

First of all, it is an erroneous perception of the reliability of cryptocurrency as an investment tool: 65% of young people are not aware of the high risks of digital currency and believe that investing in it is a reliable way to protect money from inflation. This position is more characteristic of young residents of major cities (49%) and respondents aged 18 to 24 (46%).

Almost two-thirds of young people (60% of respondents) are mistakenly convinced that there are many simple ways to increase capital. Thus, the lack of understanding of the ratio of risk and profitability of financial instruments creates the prerequisites for the massive involvement of young people in highly profitable and often illegal investment schemes fraught with high risks.

Young people also neglect personal data protection when making online payments. More than half of young citizens (59%) do not pay due attention to their personal data safety when making purchases on the Internet. Mature young people (aged 25 to 35) state it more often than others (57% among the respondents).

In our society at the modern "information" stage of its development, information is the most significant resource, and the information field is the main habitat of a modern person.

Various types of data are at the heart of all available services, which help us, among other things, manage our financial assets and carry out financial transactions. Personal data are directly related to us.

The Internet stores countless numbers of our personal data, which form the so-called "digital profile" of a person. It is a set of all the traces of existence that we leave in the digital world. Over time, such traces get increased: new gadgets are being introduced (for example, smart watches for health monitoring), technologies for tracking location and communication, digital identification of a person.

By adding new data to the already familiar photos, passwords, search history in the Internet browser, areas of interest, we get a digitalized profile of a person. The analysis of a large amount of data about a person (or digital personality analysis) makes it possible to judge their intellectual level, competencies, capabilities, and prospects.

Despite the fact that digital technologies simplify our lives in many ways, they also create many threats. Uncontrolled collection of information about a person creates a number of dangers from harmless but annoying spam calls to manipulation of opinion, consciousness, theft of their "digital identity" and money..

What are "personal data"?

² The All-Russian representative survey of youth was conducted by the NAFI Analytical Center in June 2022 using the Tet-o-Tvet-M online panel. 1,000 people aged 14 to 35 were reviewed. <https://nafi.ru/analytics/kazhdyy-vtoroy-predstavitel-molodezhi-schitaet-cto-emu-nedostatochno-znaniy-o-finansovoy-bezopasnos/> (date of access: 01/19/2023).

SLIDE 7

Statistics 2022

Percentage of those who agree with the statement: "I have sufficient knowledge and skills to protect my personal information on the Internet", is % of those who use the Internet



SLIDE 8

Personal Information

any information that directly or indirectly points to you, or is somehow related to you



general personal data



special categories of personal data



publicly available personal data that one allows to be shared



biometric personal data

Personal data are any information relating directly or indirectly to a specific or identifiable person (personal data subject), that is any information that directly or indirectly points to or is somehow related to a person.

There are several types of personal data:

- general - first name, last name, patronymic, passport details, date and place of birth, registration addresses and place of residence;
- special categories of personal data, which include nationality, political, religious or philosophical views and beliefs, information about the state of health, intimate life, criminal record;
- publicly available personal data authorized by a person for distribution (e.g. information that one provides to an unlimited number of people through social networks);
- biometric personal data - fingerprints, iris pattern, palm vein pattern, DNA code, voice cast;
- depersonalized - data by which it is impossible to identify a person without additional data (table with identifier values).

Assignment:

- Study slides No.6-7 and answer the questions. Comment on the chart data. What conclusions can be drawn from the information provided? Do you think that you have sufficient knowledge and skills to protect your personal information on the Internet?
- How dangerous is the leakage of your personal data?
- Slide No. 8. What do you think is meant by the above types of personal data?
- Give examples of each type of personal data.
- Think about how your personal financial security is related to the security of your personal data on the Internet?

I. Digital human profile and biometric personal data

Today algorithms know much more about a person than their own parents. They have at their disposal not only information about something specific, but a whole layer of data that opens up the possibility of creating a specific personality in the digital world, an analogue of a living person.

The concept of a digital identity has been firmly established in everyday life, and we distinguish it from the concept "profile" in social networks. If the first definition is mostly used in the scientific world, in development, the second one is familiar to everyone. In this vein, the issues of financial security of a digital person should be considered.

How does digital identity theft occur?

SLIDE 9

Digital Personality

personal data with which a criminal can impersonate one, for example, to obtain material benefits

Assignment

Give at least three examples of information, namely elements of your "digital identity" that you publicly release over the Internet. What kinds of your data can be stolen?



SLIDE 10

Why Do They Steal a Digital Identity?



Fraud and extortion



Registration of fake accounts



Getting a loan, bonuses and post-paid services



After the transition of many areas of human activity to the Internet, the digital identity has also acquired a price. It has become a commodity with its own characteristics, value and cost. It does not only refer to taking possession of a password or access rights.

Digital personality analysis is at the heart of all modern marketing. They are willing to pay for information about a person's preferences, lifestyle and needs. Moreover, the more companies are willing to invest, the more data they get at their disposal. This is what makes "smart feeds" work. Targeted ad impressions, tracking the flow of people during advertising do not surprise anyone, but one also does not fully know how far this analysis extends.

Even an adult, not to mention a teenager, is not able to give their informed consent to something that they do not fully understand, while a digital person can easily become the object of illegal actions. Such phenomena as the abduction of a digital identity are already not uncommon in modern reality. If a company works with the financial management of individuals and businesses, a large number of people are concerned about what it does with the information about their financial assets, investment goals, risk appetite, etc.

Digital identity theft – **photos, videos from one's pages on social networks, accounts and profiles, passport data and copies of documents** – can be committed for various purposes, i.e. from the banal sale of information to blackmail and use in fraudulent schemes. The simplest example is the use of phone numbers, names, personal information and voices to deceive and scam.

Do not think that digital identity theft is something from of a science fiction movie about the future. At the beginning of 2019, it was found out that the Genesis marketplace sold more than 60 thousand stolen digital identities, and there was a special browser with a built-in human digital trace generator.

Of course, the users who do not expose important data to the public can also become a victim of intruders. Every tenth child has been scammed through using fake websites/emails. For example, they go to fake online shopping pages that lure them with promotions and discounts, or they fall for quick money ads. However, their purpose is on the contrary to defraud children out of their money rather than give them the opportunity to get it. Any user can become a victim of a data leakage when accounts are exposed online due to technical vulnerabilities or malicious actions. One can check whether these data have been included in an open database by using a special site that accumulates information about account leaks.

Why do they steal a digital identity?

Access to someone's account opens up a wide range of opportunities. One can read correspondence and hold it on behalf of the owner, one can follow them, look for confidential information, publish content on their behalf, ask for money transfers, distribute spam, use it to promote advertising groups. All these things are the threats posed by the loss of personal data that make up the digital identity of a particular person.

1. **Fraud.** Photos and videos of a real person can be used to create a fake social media page and use it as a tool to extort money.

2. **Receiving bonuses and postpaid services.** Some of us have come across ads of betting companies, forex sites, online poker rooms and other sites that offer new customers money into an account that they can use to employ the services. The stolen data will be used by the attacker to create an account in order to receive bonuses. This is usually harmless enough for the victims, the only thing is they will not be able to take advantage of the promotional offer in future. The consequences of acquiring postpaid services with stolen data can be much less rosy, when an attacker registers an account for your data, uses the services, and in the end, instead of paying for them, simply disappears. In this case, a full-fledged fraud is committed on your behalf

	<p>3.Account registration. Photos of people are used to create social media spam accounts, which increases the frequency of successful attacks. Attackers often do not bother to change the data and take the real data of the victim, including the name and surname. On the network you can find offers for the sale of accounts in various social networks and other sites. To register such accounts, attackers also use stolen data, less often such accounts are collected as a result of phishing or data leakage.</p> <p>4.Getting a loan. Today, in a highly competitive environment, online loan companies are everywhere lowering the requirements for borrowers, simplifying the procedure for obtaining a small amount. Such risks pay off high interest on loans, which sometimes reach thousands of percent per year, and heavy penalties for any delay. Minimization of checks and data provided has turned online loans into a tasty morsel for scammers who take loans on other people's data. In some cases, scammers will only need electronic copies of two documents of the victim, for example, a passport and driving license. To get them one can create a job ad and ask potential job seekers for a copy of the documents after "recruiting". Fraudsters know many ways to get copies of documents and to borrow by using them. There are also more sophisticated fraud schemes to obtain loans without the owner. On a Russian-speaking forum, there was an offer to sell air tickets for 50% of their real cost. The service owner assured that there was no fraud, air tickets were not bought with stolen funds. At first, forum visitors were distrustful of a tempting offer, then positive reviews began to attract more and more customers. Clients sent all their data to the attacker, including photocopies of documents. None of the clients had any problems with the flight. Problems arose later, when the bank in which these tickets were issued on credit began to demand a refund of the amount for air tickets, interest and appreciable sums for default on a payment. As a result, the victims paid 200-300 percent of the real cost of the purchased tickets.</p> <p>5.Revenge and damage to reputation. On the net, one can find many stories about how ill-wishers, wanting to take revenge on someone, exhibited their photo and profile on various dubious sites. The main problem is that even if the site has deleted the victim's photo and profile by that time, other sites that copy data may host the profile, and thus, the photo will end up in the search results for images. Removing data from all sites and search engines often becomes almost an impossible task, especially if the victim does not have sufficient funds for this. If you are a reputation addict, detractors may try to ruin your reputation, e.g. to post reviews on products for adults on your behalf. Everyone who will look for information about you in future, whether they are employers or potential partners, will stumble upon similar reviews that do not colour you.</p> <p><u>Assignment:</u></p> <ol style="list-style-type: none"> 1. Slide No. 9. Give at least three examples of information – elements of your "digital identity" – that you publicly release over the Internet 2. Study the information on slide No.10. Think it over and name the ways of misusing your digital identity which are not listed on the slide.
<p>SLIDE 11</p>	<p><i>What to do in case of a leak?</i></p> <p><i>In the event that your personal data got into the network and was posted on one or more sites, the following measures may be effective</i></p> <ol style="list-style-type: none"> 1. <i>Appeal to the site owner.</i> This is the simplest and often the most effective method if your personal data is leaked and posted on one or more sites. Politely, without threats, ask the site owner to help you. If courtesy does not help, warn that you will be forced to take legal action and address the regulator for the sole purpose of protecting your personal data.

<div data-bbox="241 359 356 383" data-label="Section-Header"> <h3>Situation</h3> </div> <div data-bbox="176 391 423 644" data-label="Text"> <p>Deputy of N. city Sh.Sh. Sattorov began to find online reviews on his own behalf, published on various resources. Outwardly, these were inconspicuous reviews containing real details of his family life and a description of the product, but rudeness and disrespect for users were always traced in the reviews, they always caused a negative attitude towards the author in the ordinary reader. As a result, citizen Sh.Sh. Sattorov decided to write to the site owners with a request to remove illegally distributed personal data.</p> </div> <div data-bbox="168 683 250 708" data-label="Image"> </div> <div data-bbox="259 683 385 718" data-label="Image"> </div> <div data-bbox="396 560 593 718" data-label="Image"> </div> <div data-bbox="584 357 732 383" data-label="Section-Header"> <h3>Assignment</h3> </div> <div data-bbox="779 359 801 378" data-label="Text"> <p>11</p> </div> <div data-bbox="544 391 804 595" data-label="List-Group"> <ol style="list-style-type: none"> 1. Read the text. 2. Guess what sort of family life details of Deputy Sh.Sh. Sattorov might have been published along with the product reviews. 3. Drawing on the material of the memo on how to eliminate the consequences of data leakage and on the samples of appeals on the next slide, make a hypothetical appeal from citizen Sh. Sh Sattorov, to the site owners. </div>	<p>2. Appeal to the regulatory body in the field of communications. Write an appeal in which you inform that the specified site distributes personal data without your permission, thus violating the law. Be sure to include a link to the posted data. The maximum that the regulatory body is capable of is to fine the owner if he is identified and is in the same jurisdiction as the regulator itself, or to block it in the territory of the country where the regulatory body is located. For many site owners, blocking in the territory of a particular country is a serious loss of audience, and they immediately remove the content that caused the block.</p> <p>3. Complaint to the hosting provider and registrar. A hosting provider is an organization that provides a site with a server for hosting, a registrar is an organization where the site owner has registered a domain name. You need to go to the websites of the registrar and the hosting provider and find contacts for complaints there; they usually contain the word "abuse". Even if such a contact is not found, write to any available contacts.</p> <p>4. Appeal to the fighters against scammers. If the site is fraudulent (for example, it sells documents, or your personal data are posted there for the purpose of extortion), you should warn the organizations involved in the fight against such sites or the databases of dangerous sites about this.</p> <p>5. Appeal to the court. If the appeal to the site owner, hosting provider and registrar did not bring a positive result, you need to find a lawyer and think about going to court. The court may decide that the page with personal data will be blocked in the territory of your country, as well as oblige search engines to remove your personal data from the issuance. Often, site owners, in order to remove the restrictions put on them, remove the content blocked by a court decision.</p> <p>6. Appeal to law enforcement agencies. In many countries, the distribution or sale of personal data are a criminal offence. It is worth notifying law enforcement agencies about a site that violates the law. Fortunately, today it is not necessary to go to the nearest station, stand in line and write an application for this; it can be done online.</p> <p>7. Change of the documents. If you are afraid that a photocopy of the document that has been posted can be used for fraudulent purposes, for example, to apply for a loan, it would be a reasonable step to contact law enforcement agencies and change the document number. This option is not available in all countries, you'd better contact a lawyer to clarify the details.</p> <p>Assignment:</p> <ol style="list-style-type: none"> 1. Study the situation described on slide No 11. 2. Guess what kind of "details of family life" deputy Sh.Sh. Sattorova could be published along with product reviews. 3. Based on the materials of the Memo on how to eliminate the consequences of data leakage (see Appendix No. 4 to the Methodological Recommendations) and on the sample appeal on slide No. 12, make a hypothetical appeal from citizen Sh.Sh. Sattorov to site owners with a request to delete illegally placed personal data.
<div data-bbox="423 812 548 839" data-label="Section-Header"> <h3>SLIDE 12</h3> </div> <div data-bbox="168 963 423 1329" data-label="Image"> </div> <div data-bbox="273 1000 405 1023" data-label="Text"> <p>Please delete!</p> </div> <div data-bbox="456 971 775 1021" data-label="Section-Header"> <h3>Sample Request for Deletion of Personal Data</h3> </div> <div data-bbox="779 973 801 992" data-label="Text"> <p>12</p> </div> <div data-bbox="441 1029 788 1096" data-label="Text"> <p>Good afternoon, Your website (specify the link) has posted my personal data for public access, namely (specify which data). Please help me to remove them.</p> </div> <div data-bbox="441 1109 788 1209" data-label="Text"> <p>If there is no response to my appeal, I regret to inform you that I will have to file a corresponding application with the regulatory body, as well as ask for the assistance of the domain name registrar and hosting provider serving your site. I hope for your help!</p> </div> <div data-bbox="441 1224 582 1257" data-label="Text"> <p>Sincerely, (applicant's full name).</p> </div> <div data-bbox="168 1295 250 1321" data-label="Image"> </div> <div data-bbox="259 1295 385 1331" data-label="Image"> </div> <div data-bbox="396 1295 548 1331" data-label="Image"> </div> <div data-bbox="544 1295 804 1331" data-label="Image"> </div>	<p>How to prevent digital identity theft?</p> <p>To protect your data, you must follow the basic rules of digital hygiene:</p> <ul style="list-style-type: none"> ✓ do not share a lot of information about yourself on the network;

SLIDE 13

Digital Hygiene Rules:

- create complex and different passwords, use a password manager to create and store them;
- set up two-factor authentication for logging into your account;
- install applications only from official stores and carefully check what permissions you give to installed applications;
- use mail services for transmission with the ability to delete data from the recipient;
- delete email with personal data from the mailbox and messengers;
- do not use social networks for authorization on sites;
- delete all unused accounts;



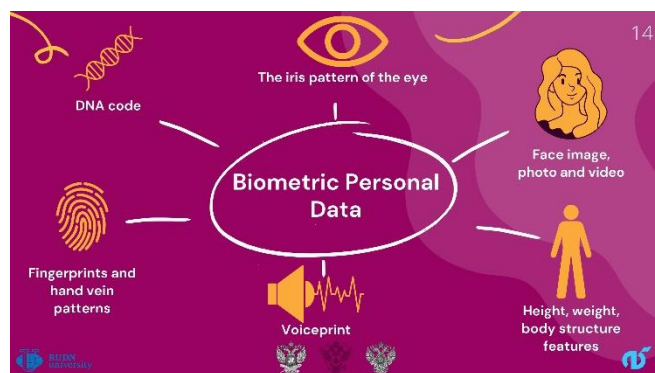
- ✓ create complex and different passwords, or, even better, use a password manager to create and store them;
- ✓ wherever possible, set up two-factor authentication to log into your account;
- ✓ do not store confidential documents and private photos for easy access on devices - smartphones, tablets, PCs;
- ✓ put a security solution on all devices and update it regularly; it is important that it is not just an antivirus, but a comprehensive solution to protect against phishing, online fraud, web spying, with the function of secure payments
- ✓ install applications only from official stores and carefully check what permissions you give to installed applications;
- ✓ do not follow dubious links, do not perceive a tempting offer as a call to action;
- ✓ be wary of calls from unknown numbers, messages from unknown senders, any requests to transfer money;
- ✓ use mail services for transmission with the ability to delete data from the recipient: Gmail has similar functionality, you can delete a sent letter, you can prohibit copying and forwarding data;
- ✓ be sure to delete letters and instant messages containing personal data from your email inbox in case your mailbox is hacked, especially if you sent scans of your documents somewhere;
- ✓ ask the recipient to treat your personal data with respect: when sending an email with documents by mail or in a messenger, accompany it with a request to treat your personal data with respect
- ✓ do not name photocopies of documents with key words: in some social networks, documents uploaded by users are publicly available, therefore, it is better to give any valuable documents, no matter how they are transmitted and stored, with neutral titles, for example, "pic15" or "image1988";
- ✓ do not use social networks for authorization on sites: in exchange for this, you provide the site with access to your personal data, which it collects, sometimes sells and sometimes is stolen by attackers;
- ✓ delete all unused accounts: leaks from websites are one of the most common ways of identity theft;
- ✓ when sending copies of your documents, indicate on them the date and the addressee (or the site where you send the data) using a watermark or a piece of paper attached to the photo of the documents with the addressee's data written on it: even if the copy falls into the hands of intruders, they will not be able to use it on other sites and most likely it will be removed as a defective product.

Compliance with these rules will at least make it more difficult for fraudsters to access an important part of the information about you as a person, and will help reduce the risk of losing money, reputation, and time. If the user himself pays more attention to the data that he provides about himself consciously or automatically, a digital identity theft will not be so elementary.

Assignment:

1. Study the rules of digital hygiene presented on slide No. 13 / in the Memo with the rules of digital hygiene (see Appendix No. 5 to the Guidelines). Discuss in class which of these rules you follow regularly and which you hear about for the first time.

SLIDE 14



In early 2018 the IBM Security division released a global survey on consumer opinion concerning digital identity and authentication. About 4,000 adults in the United States, the Asia-Pacific region (APR) and Europe took part in the IBM Security study "The Future of Identification Systems". According to its results, when logging into applications and devices, users are more concerned about security than usability. Moreover, according to the study, young people place less value on the security of traditional password identification. They prefer to use biometrics, multi-factor authentication, and a password manager to log in to increase their personal level of information security. Biometrics is going mainstream with 67% of respondents successfully using biometric authentication, while 87% of those surveyed said they would continue to use the technology in the future.

Survey results showed that teenagers and young people are leaving passwords in the past: 75% of those surveyed use biometric identification. At the same time, less than half of them use complex passwords to log in, and 41% reuse their passwords. Older people pay more attention to creating a strong password but are less likely to use biometrics and multi-factor authentication.

Against the background of the rapid spread of biometrics as a way of recognizing (identifying) a person for various purposes, for example, for identification in the access control systems of offices, in computer systems, smartphones, payment services and/or identification of users of financial services, the issue of ensuring the protection of this type of personal data becomes especially relevant.

Biometric data are unique for each person, it is not repeated and does not change during life.

Biometric personal data include fingerprints, palm vein pattern, iris pattern of the eyes, DNA code, face image, voiceprint, height, weight, features of the body structure, images of a person (photos, videos), other physiological and biological characteristics of a person (for example, gait).

Threats of misuse of biometric personal data and ways to protect against them

1) **Deepfakes** are realistic photo, audio and video substitution created with the help of neural networks. Using computer algorithms, you can "revive" photos, replace faces with videos, and even synthesize a person's voice.

Almost anyone can create deepfakes due to the availability of training and numerous programs for working with this technology. Such a low entry threshold moves the technology forward, but also increases the number of tools for fraudsters to deceive users and steal their personal data.

Deepfakes can be used to manipulate our minds: for example, this technology can be used to create provocative videos with sharp statements by politicians or a video message from a well-known blogger, which either cause a great resonance in society or call for registration on a website to participate in a raffle prizes. It is especially dangerous if a link to a phishing site is distributed along with such videos. But the most common way to use deepfakes is extortion; pretending to be friends, relatives or superiors, scammers can obtain personal data of a person using voice or video messages as confirmation of their identity

2) **Face recognition programs** - neural networks that analyze the unique features of the human face and compare them with other photographs in various databases.


Most certainly each of us at least once used the image search in the browser. Using algorithms that collect key information about a person from his photo, you can find his social media accounts and use his personal data. For such a search, it is enough to upload a photo of a person, and the program will display information about him from open sources. Thanks to such a "portfolio" on the victim, scammers can easily draw up a suitable scheme of deception in order to extract even more personal data, and then money.

How to protect yourself from fraudsters who use someone else's biometric data?

SLIDE 15

Situation

In 2021, a resident of the city, H. Muqaddas, complained that she fell into the trap of scammers who used a special computer program to "clone" a person's speech, and lost 50,000 conventional monetary units. That was the price to save her friend from revocation of driving license for driving while intoxicated. When a "friend" called from a number unknown to the girl, she had no doubt that she was talking on the phone with a person close to her. Allegedly, he has just changed his phone number and he really needs help, because a police officer is demanding a bribe. Then the phone was handed over to the "employee", who convinced the girl to hand over the money to "resolve" the situation. The girl followed all the instructions for transferring to an unfamiliar number and only after that she turned to the bank, but the payment to the fraudster had already been made.



15

- ✓ Do not use facial recognition programs, because in this way your data will fall into their database, and you will become a much more vulnerable target for scammers.
- ✓ Close your profiles in social networks - so the programs will not be able to find your photos during the analysis.
- ✓ In social networks, add only trusted people whom you know personally as "friends"
- ✓ Fraudsters most often use open resources to create deepfakes. If you restrict access to your accounts in social networks and instant messengers (set up privacy), then they will have less chance of creating something believable with your personality.
- ✓ Publish only the necessary information and make sure that the pages of your friends and acquaintances have a minimum of your personal data, or none at all.
- ✓ Check the details of the prize draws, contests or events on the official website of the company or in the actual account of the celebrity on whose behalf the promotion is being held. You should not follow unknown links, even if the photo accompanying the publication is a real image of a famous person.
- ✓ Be vigilant; always find the source or analyze the material before taking any action. Fraudsters will try to create stressful conditions to force you to make a decision immediately. Do not fall for such tricks, even if at first glance everything looks true.

Assignment:

1. Analyze the situation of Muqaddas, presented on slide No 15.
2. Do you think the loss of money could have been avoided?
3. What precautions could Muqaddas take to avoid being scammed? Formulate the sequence of your actions in such situations.

Suggested response model:

First of all, you need to stop the conversation and call the person in question. If he failed to get through on the phone, you should try to contact other people who may know his whereabouts (colleagues, friends, relatives) to clarify the information.

Most likely, at this stage, you can make sure that they are trying to deceive you.

Despite the unrest for a relative or loved one, you need to understand that if a stranger calls you and demands to bring money to a certain address, he is a scammer.

If a supposedly close relative or acquaintance calls you and says that he is in trouble and is in danger of being prosecuted, and asks you to transfer the money to a police officer who is ready to resolve the issue, you need to ask clarifying questions: "What is the nickname of my dog" or "When and where did we last see each other?", that is, it is necessary to ask such questions, the answers to which only you both know.

If you are talking supposedly with a police officer, specify which department he is from, then call the duty department of this department and ask if your relative or acquaintance was really taken there.

Phishing on social networks

This type of scam comes in many forms and involves the use of popular social media to take over someone else's account, steal sensitive data from victims, or lure them to fake websites for the purpose of gaining financial benefits. Fraudsters may create fake accounts by impersonating someone a potential victim knows in order to lure them into

SLIDE 16



16

II. Financial Security in Social Networks and Online Games

SLIDE 17



17

a trap, or they may even impersonate a customer service account of a well-known company in order to prey on victims who apply to this support company.

Also, through social networks, scammers can offer to buy various goods with big discounts, and when you follow the links offered in your account, you fall into the trap: you do not receive the goods and you lose your money.

How dangerous is phishing on social networks?

By hacking your account and gaining access to your correspondence, sent and received files, subscriber base, fraudsters will have ample opportunities for various types of blackmail, publishing provocative information and social engineering: hiding behind your identity, a fraudster can contact each of the contact list that is how a chain reaction of fraudulent activities can be launched. Often, such mailings occur at night, as scammers often work from other countries (this complicates the process of finding a scammer by law enforcement agencies).

The most dangerous types of phishing:

- 1) Messages asking for a loan, voting in a contest, a link to a "funny video" from one of your friends. When you go to the voting page or to watch a "funny video", you are prompted to enter your login and password on a page similar to the main page of the social network, after which the account is hacked.
- 2) Online stores, cinemas, delivery services and others. Here, the goal is data that allows access to linked bank cards. According to a study by Group-IB, in 2020 such services were the target in 30.7% of fraudulent attacks³. Those who enter payment data in online stores are also at risk: if you make a mistake with the input window, without checking the address in the browser line, you risk sending money to a scammer. Moreover, there are services that simulate a transaction error in order to repeat it, for example, to conduct a transaction twice in a row.
- 3) Playing on feelings and emotions through publication on social networking pages of very emotional stories about children or animals in need of help, backing up the post with photographs, documents and the message "maximum repost". The main thing is to create a post conversion and its distribution from one person along the chain of his friends and contacts. Of course, the money from such "pseudo-charity" goes to scammers!
- 4) Playing on curiosity. You can receive tempting offers in private messages or in the news feed. In any case, you will be asked to follow a link and enter personal data or bank card details.

Basic rules for protecting against phishing in social networks:

- ✓ As soon as you find out that the data were leaked or could potentially be stolen by scammers, change passwords from social networks, mail, payment services as soon as possible. And it is better to change passwords every three months!
- ✓ Never use the same passwords. The rule "one password, one service" will help to interrupt the running phishing chain to check if your login and password match other popular services. Today, scammers use automatic services that allow to quickly check where else your data can go.

³ Group-IB official website <https://www.group-ib.ru/resources/threat-research.html>

SLIDE 18

Situation

In August 2019, Estoppers reported on a phishing campaign launched on Instagram, in which scammers sent private messages to Instagram users, warning them of image copyright infringement and requiring them to fill out a special form to avoid getting banned. One of the victims received a private message from a supposedly official North Face account alleging copyright infringement. The victim followed a link in a message to a seemingly legitimate site, Instagram Help Notice.com, where the user was asked to enter their login credentials. The victim, trapped, eventually gave the hackers access to her account information and other personal data associated with her Instagram account.



SLIDE 19

Checklist: Am I protected from phishing?

Check which of the rules you follow regularly:

- ☒ Check which of the rules you follow regularly:
- ☐ I never use the same passwords on different services
- ☐ I carefully check where I enter my login, password and payment information
- ☐ I use two-factor authentication
- ☐ I do not click on suspicious links
- ☐ I do not believe unreasonably good offers



- ✓ *Be cautious. Avoid rushing when entering your login, password and payment information. Check the address bar, look at the design elements. If something confuses you, do not enter your data!*
- ✓ *Use two-factor authentication. If your login and password are in the hands of hackers, you will have to enter the code received on your phone to enter or use an additional application.*
- ✓ *Do not trust dubious offers and links. A link hidden by a short URL service like bit.ly can lead to scammers. If the style of messages or the way your friend communicates in the chat has changed it is the reason to call him and make sure that he is the one who is writing to you.*

Assignment:

1. Read the information provided on slide No 17 and answer the questions.
2. Have you ever encountered any type of phishing on social networks? If so, were you able to recognize the scam or did you not think about a possible scam?
3. Together with classmates, formulate 1-2 rules that will help you recognize each of these types of phishing and avoid becoming a victim of scammers.

Suggested rules (possible student responses):

1. Requests from friends to help with money:

- call your friend and ask if he really needs money;
- never transfer money to unknown numbers without confirmation from a friend;
- check if there is other suspicious activity on your friend's page.

2. Pseudo Charity:


When transferring funds to charity, you should pay attention to:


- how long the page exists;
- quality and quantity of content;
- excessive pressure on pity;
- transferring money to a personal card;
- urgency of collection;
- response to clarifying questions;
- the presence of a link to the charity foundation website (or whether the link is genuine).

3. Funny videos, high-profile news and other messages that involve clicking on external links:

- set privacy settings so that only your friends can send you messages;
- if you received such a message from a friend, call him by phone and make sure that his page has not been hacked;
- do not click on suspicious links;
- when connecting to a social network, check that the page address is correct;
- do not trust loud headlines in posts in the feed;
- pay attention to the address of the page you are going to.

4. Study the situation presented on slide #18. Which of the rules you formulated earlier apply to this situation and could prevent it?

	5. Slide number 19: work with the checklist "Am I protected from phishing?". Check how many anti-phishing rules you follow on a regular basis
<p style="text-align: center;">SLIDE 20</p>  <p style="text-align: center;">Fake Accounts 20</p> <p style="text-align: center;">— fake social media profiles that can be used to extort money and personal data from social media users</p> <p>Online stores and fake charities</p> <ul style="list-style-type: none"> • check information about promotions on the official websites of stores and charities • large stores are unlikely to send news about the draw days, and likes/ comments should correspond to the number of subscribers <p>Accounts for extortion and involvement in the financing of terrorism</p> <ul style="list-style-type: none"> • check the activity on the page - posts should be published at different intervals (not 10 posts in 1 day) <p>Celebrity accounts</p> <ul style="list-style-type: none"> • check if the celebrity page is verified - trusted profiles are marked with a blue checkmark • check profile creation date and post originality <p>RUDN university</p>	<p>Fake accounts: why are they dangerous and how to recognize them?</p> <p>A fake profile on a social network is one of the ways to swindle users' personal data and money.</p> <p>Fake pages can be created for various reasons.</p> <ol style="list-style-type: none"> 1. The most harmless of them is when a person, for some personal reason, does not want to advertise his presence on a social network. Last name and first name are usually fictitious. Instead of an avatar, flowers or cats, there are few or no friends. 2. Websites of shops and pages of fake charitable foundations to help people in trouble. These stores often offer popular or hard-to-find items at very low prices, and usually ask for a full refund before the item is shipped. And behind the facade of a charitable foundation, terrorist or extremist groups may be hiding, which are raising money to finance their illegal activities. And even if at the last moment you changed your mind about paying in advance, you probably sent personal data to the scammers: to whom to deliver and where. They will be happy about this too - and they will certainly figure out how to use your personal information. <p>What to do:</p> <ul style="list-style-type: none"> ✓ check information about promotions on the official websites of stores; ✓ remember that large stores are unlikely to send news about the draw through social networks, for this they rather use SMS or email; ✓ you should be alerted if you are asked to tell a large number of friends about the promotion - this is a typical way for scammers to spread their links <ol style="list-style-type: none"> 3. Hacked account of a real person. From such profiles, messages with spam (most often prohibited information or malicious links) may come, or aggressive and offensive letters designed to provoke you to inquire about the identity of the "hater" and, possibly, follow the link (often the only one) posted in his profile. From such accounts, if they belonged to a girl, attempts can be made to meet the opposite sex in order to extort money and personal data. But more often, scammers send letters to all friends asking for financial assistance or simply to help out with money until tomorrow. In addition, such accounts can be used to engage users of social networks in the financing of terrorist and extremist activities. If you suddenly receive letters from friends with such pleas, be sure that this is most likely a hoax. In order not to be deceived, it is better to ask a friend personally by calling him. <p>What to do:</p> <ul style="list-style-type: none"> ✓ do not react to negative comments: just block the user and delete the message; ✓ do not go anywhere from the pages of users you do not know, especially if the only available option on them is to click on the proposed link; ✓ carefully check all pages where you are asked to enter personal data: look at the domain name, https protocol and lock icon; ✓ set up two-factor authentication in all social networks, where possible (see Memo - Appendix No. 6 to the Guidelines). ✓ in the privacy settings, prohibit strangers from leaving comments and hide your publications from them to avoid spam and insults. <ol style="list-style-type: none"> 4. Creating a celebrity profile - a favorite performer suddenly announced a collection, for example, to help some person, or a prize draw..

	<p>What to do:</p> <ul style="list-style-type: none"> ✓ check if the page of the famous person you want to chat with on social networks has been verified – reliable profiles are marked with a blue checkmark; ✓ check the creation date of the profile and all posts, if the photos were uploaded two days ago, its author is probably a scammer; you can determine the originality of the photo using the "image search" function in Google or Yandex; ✓ view the content of the account: malicious links or obscene expressions are a reason not to be friends with such a public page. ✓ analyze the activity: read the comments and study the feed and the speed of its filling - fake profiles are filled quickly, and they are filled with the same type of comments, and also subscribe to everyone in a row. <p>✓</p>
<p style="text-align: center;">SLIDE 21</p> 	<p>Financial security in online games</p> <p>Computer games have long ceased to be something unusual and mysterious, and they are played by a huge number of people around the world. According to Microsoft, the total audience of video games is more than three billion people.⁴</p> <p>With the development of the Internet, a separate class of computer games has appeared that can be played not only locally on your computer or with a partner on the same keyboard, but with thousands and tens of thousands of players from all over the planet.</p> <p>The increase in the number of players in online games entails an increase in threats, as scammers try to make the most of the current situation. Online games store not only game currency and purchased game items, but real money - all this is of particular interest to attackers.</p> <p>Key dangers in online games</p> <ol style="list-style-type: none"> 1) Identity theft Perhaps the most common type of online fraud. 2) Stealing money Game currency, game items and real money in a virtual wallet are the main interests of scammers. Experts warn that for a gamer, the risk of being scammed is highest when he opens an account for payment, without which often many games do not "launch" at all. 48% of fraud cases occur just at the time of payment. 3) Account theft Having stolen the account, the scammers begin to blackmail the user and demand money for the return of the account. 4) Malware For example, the user is prompted to download a plugin for a game. Unaware of the trick, he follows a link to another site running malicious software. The purpose of such software is to harm the security and privacy of the user's device. In addition, viruses can be embedded in the game files, and unknowingly, the user can let them into his system during installation. 5) Violation of privacy

⁴ Source: <https://news.microsoft.com/2020/09/21/microsoft-to-acquire-zenimax-media-and-its-game-publisher-bethesda-softworks/>

SLIDE 22

Key Threats in Online Games

22



Identity theft

personal data is a direct access to the wallet



Personal data is a direct access to the wallet

after stealing an account, scammers begin to blackmail the user, demand money for a refund



Cash theft

about half of the fraud cases at the time of opening an account to pay for game currency, purchase add-ons, launch the game



SLIDE 23

Key Threats in Online Games

23



Malware Injection

the user is prompted to download the plugin for the game by clicking on a link to another site where the malware is running



Breach of privacy

Intruders can gain access your other accounts, register new accounts in your name



Hidden fees

to get access to all the features and functions in the game, you need to pay by linking a bank card to your account, payment is made automatically



By matching the data obtained from games and other sources, attackers can gain access to your other accounts, such as social networks, as well as register new accounts under your name or even create digital identities.

6) Hidden fees

Some online games are released in a shareware version: some of the content is provided for free, but you need to pay to get access to all the features and functions. To do this, you need to link a bank card to your account, and payment will be automatically debited from the card when the user purchases new items or services.

Assignment:

1. Slide No 24: Read the text on slide No25. Analyze Akram's situation.
2. What happened next? Assume further developments based on your knowledge of possible types of fraud in online games.
3. What conclusions can be drawn from this situation?

Akram, 20 years old:

“When I was a schoolboy, I found some server in Counter-Strike: Source where there was a dude in the Iron Man skin. When he died, his ragdoll made cool metallic noises - in general, I was impressed. I asked in the general chat how to get such a skin, and the server admin replied that the model is only available for admins, but offered it for nothing.

He activated the skin for me on the server, and everything seemed to work fine, but then he wrote that the model, they say, needs to be activated on Steam so that it does not disappear. At his request, I installed TeamViewer and gave access to the computer. He connected, opened Notepad right on my desktop, and wrote what to do there.

Suggested response model:

Using open access to the computer, the scammer logged into Akram's gaming account to allegedly activate the skin. Akram gave him all the data and codes from the mail, having lost his account on Steam.

Conclusions from the situation:

Installing third-party software, and even more so transferring computer control to strangers, is a big risk.

You can't tell strangers your game account login and password, even if they offer help / advice / game goods / promise to set up a cool feature or fix a serious problem, as scammers from fake technical support often do.

If you need help from a tech-savvy friend, let him explain in words how to solve the problem, but on your computer, follow the instructions yourself.

SLIDE 24

Akram, 20 years old



Assignment

24

1. Read the text on the next slide.
2. **What happened next?**
Assume further developments based on your knowledge of possible fraud in online games.
3. What conclusions can be drawn from the situation?



SLIDE 25



Akram, 13 years old



Situation

25

"When I was a schoolboy, I found some server in 'Counter-Strike: Source' where there was a dude in the Iron Man skin. When he died, his ragdoll made cool metallic sounds – anyway, I was impressed. I asked at in a general chat how to get such a skin, and the server admin replied that the model is available only for admins, but offered it for nothing. He activated the skin for me on the server, and everything seemed to work fine, but then he wrote that the model, needed to be activated on Steam to keep it from disappearing. At his request, I installed TeamViewer and gave access to the computer. He connected, opened Notepad right on my desktop, and wrote what to do to activate the skin."



It is impossible to consider the issues of protecting human rights in the financial sector without defining the concept of "human rights". These include the right to life and liberty, freedom from slavery and torture, freedom of opinion and their free expression, the right to work, education, etc. These rights should be enjoyed by all people without exception, regardless of their gender, age, race and ethnicity, religion, etc⁵. The Universal Declaration of Human Rights, adopted in 1948, contains a list of core human rights and freedoms, and other instruments have since been created to expand and refine the list of human rights in various fields⁶.

⁵ Human Rights / United Nations Organization. URL: <https://www.un.org/ru/global-issues/human-rights> (date of access: 07/04/2022)

⁶ Universal Declaration of Human Rights, 1948. / URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (Date of access: 07/04/2022)

SLIDE 26



26

SLIDE 27



27

Many of the above-mentioned human rights mentioned are not directly related to the financial sector, but it would be wrong to think that human rights cannot be violated in the financial sector. Factors that directly threaten human rights in the financial sector⁷ include:

1. *Discrimination in lending practices:* lending can affect human rights, regardless of the size and term of the loan. So, a person may be denied a loan because of his race, religion or creed. And the development of automatic credit checks allows such practices to be disguised.
2. *Lack of an objective view of the client:* all financial institutions must carry out a full range of checks before issuing a loan, including when working with people. Failure to comply with this principle and issuing credit without verification can lead to serious human rights violations later.
3. *Lack of an objective view of the sector in which they plan to invest:* financial institutions must ensure that their investments in various types of projects do not lead to violations of human rights.
4. *Confidentiality of customer and employee data:* weak protection of this kind of information can lead to a violation of human rights, especially if third parties have access to information about important aspects of a person's financial situation. It is important for financial institutions to ensure data protection so that this does not happen, as well as to increase the competence of employees in terms of information protection.

5. *Equity in pay:* Organizations in the financial sector (as in any other field) must provide fair pay based on an assessment of the performance of the employee, his professional, and not any other qualities. Otherwise, one of the basic premises of the concept of human rights is violated - the idea of universal equality.


Measures to protect human rights in the financial sector can be divided into reactive (working on fraud already committed, for example, based on complaints from victims) and preventive (when potential human rights violations are identified before someone is harmed by them). **The Central Bank** operates in both directions. You can contact it and report that a financial organization violates human rights in the financial sector. The Central Bank does not interfere in the contractual relationship between the organization and the client, but can initiate an audit of the organization's activities and take action if violations are detected. The Central Bank keeps statistics on filing complaints against various types of organizations. More than half of all complaints about violations of human rights in the financial sector are accounted for by credit organizations.


Antimonopoly authorities can also be attributed to organizations that guard human rights in the financial sector. One of its key tasks is to ensure competition in the financial services market. Along with this, she monitors compliance with legislation in the field of advertising. Among the areas of activity:

- prevention and suppression of advertising that can mislead the user or harm his health;
- protection from unfair competition;
- bringing subjects of advertising activity to responsibility for violation of the law;
- interaction with advertising regulators.




Speaking about organizations that protect the rights of consumers of financial services, one cannot fail to note the work of the **internal affairs bodies and the police**. They are engaged in the investigation of crimes and are obliged

⁷ Human Rights Priorities for the Financial Sector // BSR. URL: <https://www.bsr.org/en/our-insights/primers/10-human-rights-priorities-for-the-financial-sector> (дата обращения: 04.07.2022)


	<p>to accept citizens' appeals at any time, regardless of the place of the crime and the completeness of the data about it. The application should specify the nature of the event, date, time and place.</p> <p>. It is also important to provide information on the extent of damage caused. After submitting an application, you must receive a coupon notification of its acceptance. The decision on the application must be taken within seven days from the date of its submission. If no response has been received, you need to contact the head of the police department, and if you can't get an answer from him, you need to contact the prosecutor's office.</p> <p>The Prosecutor's office plays a special human rights role, since its bodies have the relative autonomy of the functional branches of state power and sufficiently extensive, providing almost universal access to them for the population. The Prosecutor's Office has the authority to protect human and civil rights and freedoms, both in supervisory and non-supervisory activities.</p>
<p style="text-align: center;">SLIDE 28</p> 	<p>Let's summarize. Assignment:</p> <p>1. Answer the questions presented on slide No28.</p> <p><u>Answers:</u> 1 – a), b), c), e); 2 – a), c);</p> <p>2. Solve test tasks (see Appendix No. 3 to the Methodological Recommendations)</p> <p><u>Answers:</u></p> <p>1 – a) 2 – b 3 – c 4 – b 5 – b 6 – c 7 – b 8 – a b c 9 – a d</p>
<p style="text-align: center;">SLIDE 29</p>	<p>Familiarization of students with the opportunity to take part in the International Financial Security Olympiad.</p>





International Financial Security Olympiad






Ministry of Education of Russia
Ministry of Education and Science of Russia
Rosfinmonitoring




RUDN university


SLIDE 30



Olympiad Goals

- Improving the general information, financial and legal literacy of young people, shaping a new form of thinking and a new format of activity, identifying talents in the field of financial security
- creating conditions for an individual educational trajectory, promoting vocational guidance of students to form the human resources of the financial security system;
- stimulating educational, cognitive and research activities of students, developing scientific knowledge in the field of financial security.

SLIDE 31



Olympiad Pathway

Thematic lesson on financial security

1 INVITATION STAGE OF THE OLYMPIAD

- held on the platform and website of the Olympiad
- Deadline is April 7, 2023.

2 PRELIMINARY STAGE OF THE OLYMPIAD (university)

- is held at the sites of the universities participating in the International Network Institute in the field of AML / CFT
- Deadline is May 19, 2023.
- The winners get the right to participate in the next stages of the Olympiad


3 SELECTING STAGE OF THE OLYMPIAD

- sending motivation letters (essays)

4 FINAL STAGE OF THE OLYMPIAD


- held on the federal territory "Sirius" (Sochi, Russia)
- Date: October 2-6, 2023
- winners and prize-winners are granted additional rights upon admission to higher education programs

SLIDE 32




We invite you to participate:


Students of educational organizations from Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Armenia, Brazil, India, China, South Africa, Russia, Iran, Pakistan, Namibia




32




RUDN university





Ministry of Education and Science of Russia



Rosfinmonitoring

More information:
www.fedsfm.ru - Rosfinmonitoring
www.mumcfm.ru - ITMCFM
www.rudn.ru - RUDN University
rosfinolymp.ru - website of the Olympics
E-mail: olimpiada@mumcfm.ru