



**FEDERAL FINANCIAL  
MONITORING SERVICE**

THE RUSSIAN FEDERATION

**NATIONAL TERRORISM  
FINANCING RISK  
ASSESSMENT 2017-2018**

Public Report



# CONTENT

4	<b>Introduction</b>	16	Vulnerabilities
5	<b>The methodology</b>	16	Opportunities for risk reduction
10	<b>The main threats and stages of financing terrorism</b>	17	Moving funds using bank accounts and bank cards
11	<b>Attraction of funds intended for the financing of terrorism</b>	17	Risk Rating Assessment
11	Financing from legal sources	17	Vulnerabilities
11	Risk Rating Assessment	17	Opportunities for risk reduction
12	Vulnerabilities	17	Measures taken by the Russian Federation on risk management
12	Opportunities for risk reduction	17	Moving funds using money transfers without opening bank accounts
	Measures taken by the Russian Federation on risk management	17	Risk Rating Assessment
12	Attraction of funds in the Internet	18	Vulnerabilities
12	Risk Rating Assessment	18	Opportunities for the risk reduction
13	Vulnerabilities	18	Moving funds using unregulated entities
13	Opportunities for risk reduction	18	Risk Rating Assessment
13	Measures taken by the Russian Federation on risk management	18	Vulnerabilities
13	Illegal means of obtaining funds	18	Opportunities for the risk reduction
13	Risk Rating Assessment	19	Measures taken by the Russian Federation on risk management
14	Vulnerabilities	19	Transfer of funds using non-credit financial organizations and non-financial businesses and professions
14	Measures taken by the Russian Federation on risk management	19	Risk Rating Assessment
14	Attracting funds using non-profit organizations	19	Vulnerabilities
14	Risk Rating Assessment	19	Opportunities for the risk reduction
15	Vulnerabilities of the non-profit organizations sector	20	<b>Use of funds intended for the financing of terrorism</b>
15	Opportunities for risk reduction	20	Vulnerabilities
15	Measures taken by the Russian Federation on risk management	21	Opportunities for the risk reduction
16	<b>The transfer of funds intended for the financing of terrorism</b>	21	Возможности для снижения риска
16	Risk Rating Assessment	22	<b>Conclusion</b>

The current English translation may contain some typos or inaccuracies which will be corrected later on.



# INTRODUCTION

The Russian (national) system for countering the financing of terrorism (hereinafter referred to as the CFT System) contributes to the strengthening of the national security and stability of the financial sector. In connection with the existing terrorist threat, which the whole world community is facing, the need for a deep understanding of the factors that cause the existence and occurrence of terrorist financing in the state (hereinafter - FT) comes out on top. At the same time, in view of the limited resources at the disposal of the national CFT system, their use and allocation should be aimed at minimizing the key risks.

In this regard, there is a need to conduct this national assessment of the risks of financing terrorism (hereinafter - NRA FT), which allows identifying those areas of illegal financial activity

that should be given the highest priority, as well as identifying the most vulnerable areas of the national CFT system.

NRA FT was conducted by Rosfinmonitoring, involving its interregional subsidiaries and other participants of the national CFT system, including 7 state authorities, the Bank of Russia and 22 private sector entities, which allowed to make a comprehensive assessment of the current situation in the CFT area in the Russian Federation.

The results of NRA FT will be recommended for application and use in law enforcement and supervisory practice, when choosing specific measures to mitigate certain FT risks and when allocating resources at all levels of the national CFT system.



# THE METHODOLOGY

The purpose of NRA FT is to identify the most risky methods and instruments used by terrorists or terrorist groups<sup>1</sup> in the Russian Federation in order to attract, move or use funds<sup>2</sup> for criminal purposes. The NRA FT also has the task of assessing existing threats, vulnerabilities of the national CFT system and the resulting risks of FT, understanding the processes in the CFT system and identifying potential initiatives for its development and strengthening.

The NRA FT will provide an opportunity in a certain sequence and promptly make the necessary management decisions regarding threats, vulnerabilities and, in general, the risks of FT, which will improve the effectiveness of counteracting FT in the Russian Federation.

The risk assessment is carried out in accordance with the stages of the financing of terrorism, through which the means of attracting, moving or using funds are determined.

---

<sup>1</sup> The term "terrorist groups" in this document refers to terrorist organizations, terrorist communities, other organized groups (criminal associations), illegal armed groups created or being created to commit crimes under articles 205, 205.1, 205.2, 205.3, 205.4, 205.5, 206, 208, 211, 220, 221, 277, 278, 279, 360 and 361 of the Criminal Code of the Russian Federation, as well as other persons for whom there are sufficient grounds to suspect their involvement in terrorist activities (including financing of terrorism).

<sup>2</sup> The term "funds" in this document means any assets, including financial assets, economic resources, property of any kind, tangible or intangible, movable or immovable, no matter how acquired, and legal documents or instruments in any form, including electronic or digital, granting a right or a share in such property or other assets. Funds include, in particular, cash and monetary instruments (traveler's checks, bills of exchange, checks (bank checks), as well as securities in documentary form, certifying the issuer's (debtor's) obligation to pay money, which does not specify the person to whom such payment is made).

# STAGES OF THE FINANCING OF TERRORISM

## ATTRACTING FUNDS

The initial stage of the FT process, the main objective of which is to attract funds from both legitimate (private donations, collection through NPOs, business, etc.), and from illegal (e.g., proceeds from crime, smuggling, etc.) sources.

## MOVING FUNDS

The technical phase of the FT process, the main purpose of which is the use of legal and/or illegal mechanisms for the transfer of terrorist funds (e.g., wire transfers through banks, transportation of cash, etc.).

## USING FUNDS

The final stage of the FT process, the main purpose of which is the use of funds to support/ensure all activities carried out by terrorists or terrorist groups (terrorist acts, propaganda and recruitment, training and preparation, etc.).

## THE KEY TERMS OF THE NRA FT



### THREAT

To identify the threat, it is necessary to answer two questions: "who?" And "how?". In the case of FT, the answer to the question "who?" is a person or group of persons having the potential to harm the state, society, economy, etc. It should be taken into account that a person or group of persons can be known (for example, they are included in the List of organizations and individuals for whom there is information about their involvement in extremist activities or terrorism<sup>4</sup> (hereinafter - List) or other sanctions lists); and unidentified persons or groups of persons.

The answer to the question "how?" will be the ways to attract, move or use the funds. The threat is assessed based on the following factors:

- the probability of the existence of terrorists or terrorist groups using a method for FT;
- the ability of terrorists or terrorist groups to use a method for FT (e.g. the availability of necessary specialists); - statistics of the use of a method by terrorists or terrorist groups for FT.

<sup>4</sup> The list of organizations and individuals for whom there is information about their involvement in extremist activities or terrorism that is formed in accordance with paragraph 2.1 of Article 6 of the Federal Law of 07.08.2001 No. 115-FZ "On Countering the Legalization (Laundering) of Proceeds from Crime, and financing of terrorism".



## VULNERABILITY

To determine the vulnerability, it is necessary to answer the question "why terrorists or terrorist groups use this method?". The answer will be a combination of accessibility and visibility factors to attract, move or use funds, in which they can be used to implement the threat. At the same time:

- **the availability of the method** – the convenience and ease of the use of a method for FT purposes;
- **the visibility of a FT method for the participants of the national CFT system** – the extent to which the method is regulated by national legislation or is subject to other mitigating measures, including the possibility of identification during the implementation of operational measures.



## CONSEQUENCES

The consequence of FT is the answer to the question "What this will lead to?", specifically, a terrorist activity itself.

**Given this fact, it is believed that the consequence** - is a constant value based on an assessment of the potential for attracting and moving funds:

- **for operational purposes** - use of funds for the direct implementation of a specific terrorist activity (eg, terrorist act, relocation of militants and preparation of an attack);
- **for organizational purposes** - use of funds to support the needs of and to maintain a terrorist group (e.g., recruitment, training, maintenance of training camps, radical centers).



## RISK

It is considered as a function of the three factors: threat, vulnerability and consequence in the following formulation:

The probability that terrorists or terrorist groups may attract, move or use funds due to a number of circumstances (accessibility and visibility), which leads to terrorist activities.



## PRIORITY

Priority is the assessment of the priority of taking risk management measures with respect to time. Risks in relation to which it is necessary to take measures in the shortest possible time to mitigate them, belong to the high-level risk group. Risks that need to be monitored and, if necessary, take restraining measures, belong to the group of medium-risk risks. Risks that can potentially develop and that may require start working to mitigate them are among the low-level risks.

---

Table 1 – Threat matrix

		The correlation of use of a FT method with identified individuals		
		Low	Medium	High
Frequency of detection	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Medium	Medium

Level of threat	
High	Terrorists or terrorist groups are highly likely to use the method for FT purposes on a regular basis.
Medium	Terrorists or terrorist groups are likely to use the method for FT purposes.
Low	There is a low probability that terrorists or terrorist groups use the method for FT purposes.

Table 2 – Vulnerability matrix

		The correlation of use of a FT method with identified individuals		
		Низкая	Средняя	Высокая
Visibility	High	Less vulnerable	Less vulnerable	Vulnerable
	Medium	Less vulnerable	Vulnerable	More Vulnerable
	Low	Vulnerable	Vulnerable	More Vulnerable

Level of vulnerability	
More Vulnerable	The method is used by terrorists or terrorist groups for the purposes of FT because of the high level of accessibility and medium or low visibility.
Vulnerable	The method can be used by terrorists or terrorist groups for FT purposes due to a certain level of the aggregate availability and visibility.
Less vulnerable	Terrorists or terrorist groups cannot practically use the method for FT purposes due to existence of a necessary level of the aggregate visibility and accessibility.

Table 3 – Risk matrix

		Threat		
		Low	Medium	High
Vulnerability	More vulnerable	Medium	High	High
	Vulnerable	Low	Medium	High
	Less vulnerable	Low	Low	Medium

Level of risk	
High	The method is used by terrorists or terrorist groups for the purposes of FT because of the high level of accessibility and medium or low visibility.
Medium	The method can be used by terrorists or terrorist groups for FT purposes due to a certain level of the aggregate availability and visibility.
Low	Terrorists or terrorist groups cannot practically use the method for FT purposes due to existence of a necessary level of the aggregate visibility and accessibility.

# THE MAIN THREATS AND STAGES OF FINANCING TERRORISM

In the Russian Federation, the main threat of terrorism comes from the following types of terrorists or terrorist groups that use or can apply one of the ways to attract, move or use funds for FT purposes:

1. illegal armed groups operating in the North Caucasus;
2. cells of international terrorist organizations on the territory of the country;
3. Russian citizens traveling to areas with increased terrorist activity for the purpose of joining international terrorist organizations, as well as returning from these zones;
4. foreign citizens traveling to zones with increased terrorist activity for the purpose of joining international terrorist organizations, as well as returning from these zones, and using the Russian Federation as a transit territory;
5. participants of terrorist organizations, illegal armed formations and radical groups outside the territory of the Russian Federation, and involving Russians in terrorist activities through the Internet.

The risks of FT are divided in accordance with the stages of the financing of terrorism:



**ATTRACTING FUNDS**



**MOVING FUNDS**



**USING FUNDS**

# ATTRACTION OF FUNDS INTENDED FOR THE FINANCING OF TERRORISM

## FINANCING FROM LEGAL SOURCES

 Risk rating

### RISK RATING ASSESSMENT

Due to the wide range of possibilities for raising funds from various sources, the likelihood of using legitimate sources (income from commercial activities, donations from ethnic groups, wages, sale or lease of real estate, obtaining loans and/or credits and material assistance from relatives) for the purpose of financing terrorism is at a low level.

However, the facts of self-financing by terrorist groups are revealed by using part of the income from the sale or leasing of their real estate to finance terrorism, due to the lack of control over the expenditure of income derived from the above actions.

In addition, it should also be mentioned that often real estate lease contracts are concluded

for less than a year, which are not subject to state registration. In such cases, the controlling bodies do not have information about the parties to the contract and the amount of income received. These circumstances lead, in particular, to the formation of an "uncontrolled" amount of money.

The threat of terrorist financing mainly arises if funds or other property are acquired and transferred to terrorists (real estate, transport, etc.) on behalf of a legal entity.

The low threat of using legitimate sources for financing of terrorism is also due to the low frequency of identifying these facts within the practice of law enforcement agencies and the financial intelligence unit.

## VULNERABILITIES

A separate vulnerability is the absence of restrictions for persons included in the List of terrorists, to be founders or managers of legal persons.

## OPPORTUNITIES FOR RISK REDUCTION

To consider the application of legislative restrictions for persons included in the List of terrorists for establishing or managing legal persons.

## MEASURES TAKEN BY THE RUSSIAN FEDERATION ON RISK MANAGEMENT

In accordance with Article 7 of Federal Law No. 115-FZ of 07.08.2001 "On Counteracting the Legalization (Laundering) of Proceeds from Crime and Financing of Terrorism", financial institutions apply restrictions on opening accounts to legal entities if this legal entity and (or) a person entitled to act on behalf of this legal entity and (or) its beneficial owner (one of its beneficial owners) and (or) its participant (one of its participants), with the exception of a shareholder, which is a legal entity and owns more than 25 percent of the capital of a legal entity, is a person included in the List.

## ATTRACTION OF FUNDS IN THE INTERNET



Risk rating

### RISK RATING ASSESSMENT

This method of raising funds for the financing of terrorism is relevant and is widely used by terrorist groups. A significant threat is that funds can be obtained not only from persons involved in the financing of terrorism, but also from individuals who are unaware of the true purpose of raising funds.

It is also necessary to take into account that in social networks there are technological platforms that allow the transfer of funds by simply specifying the identification number of the recipient's page, account numbers, bank cards, e-wallets or other requisites of the sender. Thus, this method allows terrorist groups to collect money without attracting additional specialists.

Given that this method does not require documentary confirmation of the purposes of the transfer and the public placement of financial details and the identity of the recipients of funds, it is likely that funds, for example, received as financial assistance from a wide range of persons, can be used to finance terrorism.

The high threat of using social networks in the Internet to finance terrorism is also due to the high frequency of these facts revealed in the practice of law enforcement authorities and the financial intelligence unit.

## VULNERABILITIES

Social networks are widely available tools that can involve the Internet audience almost from all over the world. Data management processes can be carried out from anywhere in the world where there is an Internet connection.

The use of technology platforms in social networks reduces the level of visibility of this method. Potential vulnerabilities in the area of online payments are used by terrorist groups to camouflage sources of origin of funds and to confuse "financial traces".

## OPPORTUNITIES FOR RISK REDUCTION

To develop a mechanism for blocking not only users' pages in social networks on suspicion of collecting and transferring money for terrorist financing, but also a "simplified" (pre-judicial/

extrajudicial) procedure for blocking/freezing all collected funds.

Improvement of regulatory legal acts that would address the vulnerabilities associated with the use of non-personal electronic means of payment.

## MEASURES TAKEN BY THE RUSSIAN FEDERATION ON RISK MANAGEMENT

A draft law has been prepared which provides for the development of a mechanism to block bank cards and other financial instruments, the details of which are placed on the Internet for the purpose of financing terrorism.

A draft law has been developed and is undergoing an interagency coordination stage, which establishes a ban on the issuance of cash from prepaid cards.

## ILLEGAL MEANS OF OBTAINING FUNDS

 Risk rating

### RISK RATING ASSESSMENT

The use of illegal sources (kidnapping for ransom, financing from terrorist groups outside Russia, extortion from the local population, entrepreneurs and civil servants, proceeds from common crimes) for the financing of terrorism draws the attention of law enforcement authorities even before the main goal (terrorist act) is reached by a specific terrorist group.

However, there is a possibility that in areas with increased criminal situation the existence of terrorist groups that use this method is possible.

The low threat of using such methods to finance terrorism is also explained by the low frequency of these facts being revealed in the practice of law enforcement authorities and the financial intelligence unit within the framework of countering the financing of terrorism.

## VULNERABILITIES

To assess the vulnerability of this method, it is necessary to conduct separate studies on the establishment of links between terrorists and other criminal gangs, as well as ways of financing them, taking into account the criminal situation in specific regions.

## MEASURES TAKEN BY THE RUSSIAN FEDERATION ON RISK MANAGEMENT

Regular counter-terrorism measures in areas with increased criminal activity are being taken that exclude the possibility of a systematic use of the method.

## ATTRACTING FUNDS USING NON-PROFIT ORGANIZATIONS

 Risk rating

### RISK RATING ASSESSMENT

The existing preventative mechanism contained in federal laws of January 12, 1996, No. 7-FZ "On non-profit organizations", of May 19, 1995, No. 82-FZ "On public associations", of September 26, 1997, No. 125-FZ "On Freedom of Conscience and Religious Associations" and others, provides an effective barrier to the creation of non-profit organizations (hereinafter - NPOs) in order to finance terrorists and terrorist groups.

It is necessary to take into account that many of the existing forms of NPOs in the Russian Federation are characterized by insignificant risks of having any links with the financing of terrorism (for example, NPOs that deal with

housing, housing construction and garage cooperatives, horticultural, gardening and suburban consumer cooperatives, agricultural consumer cooperatives, trade unions, real estate, etc.).

The conclusion about the low threat of using NPOs for the financing of terrorism is also confirmed by the low frequency of such facts revealed in the practice of law enforcement authorities and the financial intelligence unit.

Further work should be done on a systematic assessment of the risks of abusing NPO's for financing of terrorism, including in the form of specific studies aimed at preventing the establishment of any links between NPOs and terrorists/terrorist groups.

## **VULNERABILITIES OF THE NON-PROFIT ORGANIZATIONS SECTOR**

The funds that are collected by NPOs are not always credited to their bank accounts. Such money can remain in cash or be credited to bank cards of individuals or to other means of payment (electronic wallets, mobile phone accounts).

There have been cases revealed where individuals included in the List of organizations and individuals for which there is information about their potential involvement in extremist activities or terrorism participated in the management of NPOs.

## **OPPORTUNITIES FOR RISK REDUCTION**

To consider the issue of legislative regulation of the collection of funds by NPOs, including through their transfer to bank accounts of NPOs while providing identification of persons transferring the funds.

## **MEASURES TAKEN BY THE RUSSIAN FEDERATION ON RISK MANAGEMENT**

The draft federal law "On Amendments to Certain Legislative Acts of the Russian Federation with a view to secure the prohibition to act as a founder (participant, member) of a non-profit organization to persons in relation to whom a decision has been taken to freeze (block) their funds and (or) other property due to sufficient grounds to suspect them of involvement in terrorist activities" has been prepared.

The draft federal law "On Amending the Federal Law" On Charitable Activities and Charitable Organizations" aimed at streamlining legal relations arising in connection with the collection of charitable donations was developed.



# THE TRANSFER OF FUNDS INTENDED FOR THE FINANCING OF TERRORISM

## MOVING FUNDS USING CASH

 Risk rating

### RISK RATING ASSESSMENT

Terrorist groups use cash for financing their purposes, which they can obtain both legally and illegally (for example: illegal cross-border movement (smuggling) of cash). It should be noted that most often cash is used directly before preparing for a crime of a terrorist nature.

In case of illegal cross-border movement (smuggling) of cash or other highly liquid financial instruments, tracing both sources and ways of their further use is difficult. However, the use of large amounts of cash by a terrorist group requires certain conditions and the involvement of outside specialists in "cash withdrawals", which may lead to the disclosure of the group.

The average threat of using cash to finance terrorism is also explained by the frequency of the facts of terrorist financing revealed in the practical work of law enforcement authorities and the FIU.

### VULNERABILITIES

At present, the share of cash in various financial settlements in the Russian Federation can be significant. There are no clear requirements for freezing assets, other than non-cash funds. One of the general vulnerabilities of cross-border movement of cash and BNIs is the relative simplicity of concealing the true sources of transported funds.

### OPPORTUNITIES FOR RISK REDUCTION

To take measures aimed at a step-by-step reduction of the share of cash in circulation.

To introduce regulatory changes in the part of freezing assets of persons involved in terrorist activities, other than non-cash funds.

## MOVING FUNDS USING BANK ACCOUNTS AND BANK CARDS



Risk rating

### RISK RATING ASSESSMENT

The possibility of terrorist groups to use bank cards is due to the high prevalence and simplicity of their use in everyday life. Nevertheless, in cases where proper control within the AML/CFT framework is applied by financial institutions, specifically with regard to customer credit/debit card transactions, a terrorist group can be identified.

At the same time, there is a low risk of using "classic" bank transfers (including using accounts of legal entities) due to the high transparency of these transactions.

The high risk of transferring funds for the financing of terrorism using bank cards (bank cards issued by foreign financial institutions, as well as bank cards issued by Russian financial institutions) is also explained by the high frequency of these facts revealed in the materials of LEAs and the FIU.

### VULNERABILITIES

High availability and widespread use of banking cards (including prepaid (gift) cards).

### OPPORTUNITIES FOR RISK REDUCTION

Introduction of special red-flag indicators developed by the competent authorities into the compliance procedures of financial institutions to improve the efficiency of identifying transactions with bank cards that could possibly relate to the financing of terrorism.

### MEASURES TAKEN BY THE RUSSIAN FEDERATION ON RISK MANAGEMENT

At the moment, Rosfinmonitoring together with the Bank of Russia is conducting a pilot project with the participation of the 10 largest financial institutions (they occupy about 80% of the Russian financial market) on the implementation of special red-flag indicators in the compliance procedures of the banks.

A draft law has been developed and is undergoing an interagency coordination stage which establishes a ban on the issuance of cash from prepaid cards.

## MOVING FUNDS USING MONEY TRANSFERS WITHOUT OPENING BANK ACCOUNTS



Risk rating

### RISK RATING ASSESSMENT

The use of money transfers without the opening of a bank account by terrorist groups is due to the vast geography of transfers, the high speed of their implementation, the difficulty in identifying customer relationships and

the minimum requirements for conducting identification.

The complexity of tracking the purpose of transfers, senders and final recipients, etc. increases the prevalence of the use of money transfers without opening a bank account by terrorist groups.

The high risk of transferring funds for the financing of terrorism through the use of this method is also due to the high frequency of such cases revealed in the materials of law enforcement authorities and the financial intelligence unit.

### **VULNERABILITIES**

When making international transfers without opening a bank account, a foreign financial institution is

not required to fulfill obligations stipulated by the Russian legislation, in particular, to freeze the assets of persons included in the List.

### **OPPORTUNITIES FOR THE RISK REDUCTION**

Further improvement of mechanisms for collecting and analyzing information on money transfers without opening a bank account.

## **MOVING FUNDS USING UNREGULATED ENTITIES**

 Risk rating

### **RISK RATING ASSESSMENT**

The low threat of the transfer of funds for the financing of terrorism through the use of unregulated entities (money transfers made by unregulated entities, transactions using cryptocurrencies) is explained by the low frequency of such cases revealed in the materials of law enforcement authorities and the financial intelligence unit.

It should be noted that this estimation is based on statistical data and may not reflect the real state of affairs, as potentially there are might be some terrorist groups using these methods. However, the lack of state regulation (e.g. in respect of cryptocurrencies) does not allow to objectively estimate the amounts of funds in circulation in the above areas.

### **VULNERABILITIES**

The absence of legislative regulation of crypto currency settlements allows to make "anonymous" transactions without the possibility to determine their goals and final recipients. There are difficulties

with identification of persons making payments using new financial technologies.

### **OPPORTUNITIES FOR THE RISK REDUCTION**

To legally define the status of crypto currencies (its concept and status: cash, commodity or securities, legality or illegality of its use).

To consider the extension of the CFT requirements to new financial technologies and to consider the inclusion of organizations using new financial technologies to conduct financial transactions under the scope of the AML/CFT Law.

### **MEASURES TAKEN BY THE RUSSIAN FEDERATION ON RISK MANAGEMENT**

Work is under way to introduce amendments to the legislation of the Russian Federation that define the status of digital technologies used in the financial sphere, their concepts (including such as "distributed registry technology", "token", "smart contract", etc.).

# TRANSFER OF FUNDS USING NON-CREDIT FINANCIAL ORGANIZATIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS

 Risk rating

## RISK RATING ASSESSMENT

Non-credit financial organizations and non-financial businesses and professions include insurance companies, organizations that purchase, buy and sell precious metals and precious stones, jewelry, lotteries and casinos, real estate agencies, microfinance organizations, telecommunications operators that have the right to independently provide mobile radiotelephone services, as well as operators occupying a significant position in the public communication network, which have the right to independently provide communication services for data transmission, professional participants in the securities market and organizations of the federal postal service.

The analysis made on this method of moving money through the businesses and professions mentioned above showed that, in comparison with others, this method is the least in demand since it requires additional actions on the part of terrorists.

However, certain risks exist within the telecoms operators who have the right to provide mobile radiotelephone services on their own.

## VULNERABILITIES

The possibility of using mobile phone numbers as an instrument on which money can be accumulated and then moved.

## OPPORTUNITIES FOR THE RISK REDUCTION

Strengthening internal control measures for telecom operators by providing clear and regular instructions from authorized bodies.

Making amendments to Federal Law No. 126-FZ of 07.07.2003 "On Communications", taking into account the existing provisions of the AML/CFT Law.



# USE OF FUNDS INTENDED FOR THE FINANCING OF TERRORISM

After passing the stages of attraction and moving of funds for the financing of terrorism, the next stage is the stage of using the funds.

According to the methodology used, the purposes of using funds intended for the financing of terrorism were divided into two components:

## 1. Use for operational purposes (entails more serious consequences, as the result is directly a terrorist act):

- expenses for the direct preparation of terrorist acts (e.g. the acquisition of communication means, transport);
- expenses for the acquisition and manufacture of means for the commission of terrorist acts (e.g. weapons, ammunition, explosives);
- payment of remuneration to direct participants of terrorist acts.

These methods have a subjectively average threat of use as many payments are made in cash, but at the same time in the Russian legislation there are measures to limit public access to weapons, ammunition and explosives.

## 2. Use for organizational purposes (the consequences are long-term, allow terrorist groups to establish their functioning):

- training of militants and the maintenance of terrorist camps;

- payment for propaganda and drills aimed at radicalization and self-radicalization (e.g. publication and distribution of propaganda materials, maintenance of "educational institutions");
- financing the transport costs of foreign terrorist militants and recruited members of terrorist organizations travelling to conflict zones;
- support for terrorist groups (e.g. provision with clothing, uniforms);
- the recruitment of militants;
- the creation and support of "sleeping" terrorist cells (e.g. rent of housing, rare payments of financial aid);
- payment of compensation to the families of dead terrorists;
- corruption payments (e.g. bribery of officials and/or law enforcement officers);
- payment for the services of outside specialists (e.g. doctors, lawyers);
- the support of legal structures representing the interests of a terrorist group (e.g. political parties, non-profit organizations, religious organizations, etc.).

These methods have subjectively both a low and medium threat (in connection with the existing terrorist threat in general).

## **VULNERABILITIES**

The main vulnerability is the difficulty of revealing the fact of directing funds directly for the preparation of a terrorist act, taking into account the fact that inexpensive and simple means are being acquired by terrorists and their supporters for their subsequent adaptation/customization.

In addition, it must be taken into account that the availability of goods and components for the manufacture of explosives, together with the use of cash, makes it difficult to control the financial side of the preparation for a terrorist act.

## **OPPORTUNITIES FOR THE RISK REDUCTION**

The risks can be further mitigated through the application of special red-flag indicators by financial institutions and DNFBPs which should be developed and constantly updated in conjunction with government authorities.

Consideration should be given to the development of a long-term state program, which should provide for a gradual increase in the share of non-cash payments, which will help to reduce not only the risks associated with the financing of terrorism, but also the risks associated with money laundering.

In general, it should be noted that the ways of using funds aimed at financing terrorism cannot be completely identified. They can constantly change and depend on specific goals of a particular terrorist group.



# CONCLUSION

The work carried out on NRA FT made it possible to identify the key risks for the national CFT system at the current moment. The long-term conflict in Syria and Iraq, as well as the formation of the international terrorist organization ISIL, act as a kind of catalyst for the financing of terrorism in the Russian Federation. The terrorists' need for human and financial resources is precisely what determines the risks that all participants of the CFT must pay attention to and take appropriate measures to mitigate the threats and vulnerabilities that form them.

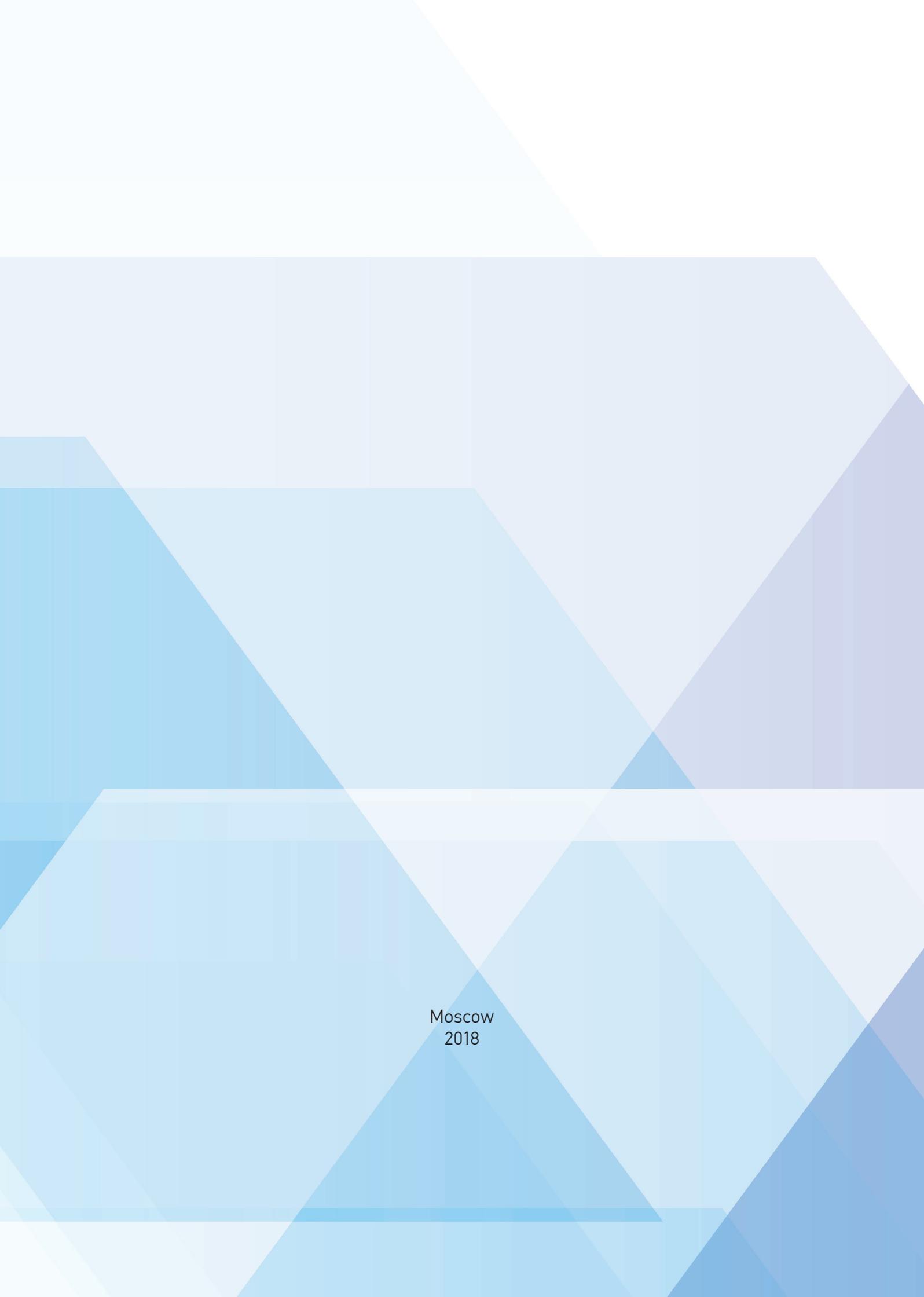
When identifying the channels for financing terrorism, it is noted that most of these crimes are committed by the transfer of cash, which complicates the documentation of these facts. Such crimes can be latent in nature, because of the concealment by terrorists and their accomplices of the true goals of collecting or moving funds.

In practice, during the conduct of counter-terrorism activities, the overwhelming majority of terrorists are terminated on the ground, which deprives the investigation of the possibility of further identifying sources of financing terrorism.

<b>HIGH-LEVEL RISK GROUP</b>	Risk: Attracting funds intended for the financing of terrorism through the Internet.
	Risk: Transfer of funds intended for the financing of terrorism, using cash.
	Risk: Transfer of funds intended for financing of terrorism using bank accounts and bank cards.
	Risk: Transfer of funds intended for terrorism financing using money transfers without opening bank accounts.

<b>MEDIUM RISK GROUP</b>	Risk: Attracting funds intended for the financing of terrorism, using illegal means of obtaining funds.
	Risk: Transfer of funds intended for the financing of terrorism, using unregulated entities.

<b>LOW RISK GROUP</b>	Risk: Attracting funds from legitimate sources.
	Risk: Attracting funds to finance terrorist activities through non-profit organizations.
	Risk: Transfer of funds using non-credit financial organizations and non-financial businesses and professions.

The background consists of several overlapping, semi-transparent geometric shapes in various shades of blue and purple. These shapes include triangles, trapezoids, and polygons, creating a layered, architectural effect. The colors range from light, airy blues to deeper, more saturated purples and blues. The overall composition is clean and modern.

Moscow  
2018