DOI: https://doi.org/10.17816/RJLS642661

Countering the financing of anti-Russian decentralized sabotage and terrorism

A.D. Kerimov[1], V.V. Krasinsky[2]

[1] Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia
[2] Institute of Financial Technologies and Economic Security, Moscow, Russia

ABSTRACT

The article discusses the problem of counteracting the financing of anti-Russian decentralized sabotage and terrorist activities of network structures. The authors analyze the illegal activities of founders, coordinators, sponsors, and beneficiaries of sabotage and terrorist network movements in online platforms and Internet messengers. The work provides the criminal and criminological characteristic of decentralized sabotage and terrorist activities. The article presents changes in terrorist tactics and modern mechanisms for financing sabotage and terrorist activities using cryptocurrencies, taking into account the high-tech present-day terrorism, the introduction of distributed financing mechanisms and resource provision of sabotage and terrorist activities. It also demonstrates the relationship between anti-Russian subversive and terrorist networks and Ukrainian special agencies, as well as the involvement of a number of Ukrainian financial institutions and virtual asset service providers in quasi-legal financial schemes, money laundering, and terrorist financing.

Keywords: decentralized subversive and terrorist activities; subversive and terrorist networks; terrorist financing; shadow financial infrastructure; cryptocurrencies; virtual assets.

To cite this article

Kerimov AD, Krasinsky VV. Countering the financing of anti-Russian decentralized sabotage and terrorism. *Russian journal of legal studies.* 2024;11(4):7–13. DOI: https://doi.org/10.17816/RJLS642661

Received: 21.10.2024 **Accepted:** 07.12.2024 **Published online:** 30.12.2024

Article can be used under the CC BY-NC-ND 4.0 International License
© Eco-Vector, 2024

УДК 338

DOI: https://doi.org/10.17816/RJLS642661

Противодействие финансированию децентрализованной диверсионно-террористической деятельности антироссийской направленности

А.Д. Керимов[1], В.В. Красинский[2]

[1] Институт государства и права Российской академии наук, Москва, Россия
[2] Институт финансовых технологий и экономической безопасности, Москва, Россия

АННОТАЦИЯ

В статье рассматривается проблема противодействия финансированию децентрализованной диверсионно-террористической деятельности сетевых структур антироссийской направленности. Авторы рассматривают противоправную деятельность учредителей, координаторов, спонсоров и бенефициаров диверсионно-террористических сетевых движений в онлайн-платформах и интернет-мессенджерах. Дана уголовно-правовая и криминологическая характеристика децентрализованной диверсионно-террористической деятельности. С учетом высокотехнологичного характера современного терроризма, внедрения распределенных механизмов финансирования и ресурсного обеспечения диверсионно-террористической деятельности в работе показаны изменения тактики террористов и современные механизмы финансирования диверсионно-террористической деятельности с использованием криптовалют. Показана связь диверсионно-террористических сетей антироссийской направленности с украинскими спецслужбами и вовлеченность ряда украинских финансовых институтов и провайдеров услуг виртуальных активов в «серые» финансовые схемы, отмывание преступных доходов и финансирование терроризма.

Ключевые слова: децентрализованная диверсионно-террористическая деятельность; диверсионно-террористические сети; финансирование терроризма; теневая финансовая инфраструктура; криптовалюты; виртуальные активы.

Как цитировать

Керимов А.Д., Красинский В.В. Противодействие финансированию децентрализованной диверсионно-террористической деятельности антироссийской направленности // Российский журнал правовых исследований. 2024. Т. 11. № 4. С. 7–13. DOI: https://doi.org/10.17816/RJLS642661

Рукопись получена: 21.10.2024 **Рукопись одобрена:** 07.12.2024 **Опубликована:** 30.12.2024

ЭКО•ВЕКТОР

Статья доступна по лицензии CC BY-NC-ND 4.0 International
© Эко-Вектор, 2024

The particular significance of the study dealing with decentralized anti-Russian subversive and terrorist activities lies in the understanding of high-tech present-day terrorism and distributed management, financing and sourcing mechanisms of terrorist networks and subversive communities (cross-platform messengers, crowdfunding, DeFi, drops, etc.).

Today, the scientific foundations for studying subversive and terrorist network movements are only being laid. Available works mainly discuss issues of criminal law qualification or specific aspects of media security [1–4].

Considering a high degree of danger of subversive and terrorist network movements to the public, significant operational and combat potential of subversive and terrorist organizations, a need to simulate, forecast, and analyze decentralized subversive and terrorist networks with an anti-Russian focus, in-depth theoretical insights in this criminal activity as an independent subject of academic research appear feasible.

The majority of subversive and terrorist movements that coordinate and support subversive and terrorist acts, and provide financial assistance or aid to terrorist organizations and subversive communities in the Russian Federation operate as decentralized online communities in social media.

In addition to large scale, visibility, and a common antisocial ideological platform, the network nature of subversive and terrorist activities allows the sponsors of terrorist organizations and subversive communities to provide a system of stable communication and control, a certain independence of structural links, recruitment of like-minded people, cross-advertising, and funding.

The existing anti-Russian subversive and terrorist movements are heterogeneous and represented by the combat wings of separatist organizations (*Movement for Zeleny Klin Independence*, *Zeleny Klin—My Fatherland*, *Free Idel-Ural*, *Malinovy Klin—Independent Kuban*, etc.), terrorist ethno-national illegal armed volunteer groups, including structural units of the *Foreign Legion* of the Armed Forces of Ukraine (*Russian Volunteer Corps*, *Freedom of Russia Legion*, *Siberian Battalion*, *Karelian National Battalion*, *Ural Battalion*, *Bashkortostan Company*, etc.), independent subversive and terrorist organizations (*Combat Organization of Anarcho-Communists*, *Right of Power Russian Movement*, *Black Bridge, Black Bridge Support*, *Exposition of Revolutionary Anarchism*, etc.).

Anti-Russian separatist activities have emerged in the Russian Internet and social media long before the Special Military Operation.

Back in 2008–2010, pseudohistorical pages were created in *Wikipedia* to promote the ideas of national autonomy and regional separatism in areas where small Ukrainian communities reside.

Since the outset of the Special Military Operation, the inactive, "dormant" accounts *Zeleny Klin—My Fatherland* and *Malinovy Klin—Independent Kuban* have been posting personal data of Russian law enforcement officers, advertising the terrorist organizations (*Freedom of Russia Legion*, *Russian Volunteer Corps*), and suggesting people help "partisan units" in acts of sabotage.[1]

In 2018, a separatist organization *Free Idel-Ural*[2] was registered in Ukraine and declared that its main goals were "collapse of Russia and creation of new states on its ruins" by the peoples of the Urals and the Volga Region inhabiting Tatarstan, Bashkortostan, Chuvashia, Mordovia, Udmurtia, and Mari El. Since the outset of the Special Military Operation, the moderators of the *Idel-Ural* online movement began calling for separatist supporters to seize gun storage rooms, munition depots of military units, participate in military operations on the side of Ukraine, and commit acts of terrorism and sabotage in the Russian territory.

A conspicuous separatist online initiative is the *League of Free Nations* founded in May 2022.[3]

The movement is aimed at drawing attention to "discrimination of enslaved peoples in Russia," consolidation of "anti-imperial forces," and attaining state sovereignty by the constituent entities of the Russian Federation.

The ideologues of the *League of Free Nations* describe it as a social and political platform for nationalist movements of the Bashkirs, Buryats, Ingrian Finnish, Cossacks, Kalmyks, Tatars, and Erzyans.

We note increased network activity and promotion of the so-called *Forum of Free Peoples of Post-Russia* (FSNPR)[4] founded by the nationals of Poland, Ukraine, Great Britain, and the USA in social networks and cross-platform Internet messengers.

To implement the separatist program of destroying federalism and the territorial integrity of the Russian Federation, the tactics of terrorist acts are mainly used, including various types and methods of counter-state struggle.

The officials of the FSNPR call for armed struggle against the "regime," acts of civil disobedience, and create ethnically based anti-Russian military groups to "protect indigenous peoples and enslaved regions." The policy documents of the FSNPR set out the goal of a *coup d'etat* using the nationalist and separatist underground.

The identified members of the FSNPR were involved in a series of terrorist crimes in 2022–2024 under

[1] By the Decision of the Supreme Court of the Russian Federation dated June 07, 2024, *Zeleny Klin—My Fatherland and Malinovy Klin—Independent Kuban* were declared extremist and banned in Russia.

[2] In February 2022, the public organization *Free Idel-Ural* (Ukraine) was declared undesirable in the Russian Federation and extremist in June 2024.

[3] On February 17, 2023, the *League of Free Nations* registered in Lithuania was declared an undesirable organization in the Russian Federation; and on June 7, 2024, it was declared an extremist association.

[4] On November 22, 2024, the *Forum of Free Peoples of Post-Russia* was declared a terrorist organization and banned in Russia.

DOI: https://doi.org/10.17816/RJLS642661

Articles 205, 205.1, 205.2, 205.3, 205.4 of the Russian Criminal Code.

In addition to propaganda and independent subversive and terrorist acts, most participants in special subversive and terrorist movements (*Rospartizan*, *Russian Movement Right of Power*, *Black Bridge*, *Exposition of Revolutionary Anarchism*) cooperate with Ukrainian secret services and armed groups. A chatbot system is used to recruit volunteers to join the so-called *Foreign Legion* of the Armed Forces of Ukraine. Subversive and terrorist movements transfer part of their funds to terrorist organizations (e.g. *Freedom of Russia Legion* or *Russian Volunteer Corps*).

It should be considered that participation of Russian nationals in an armed conflict as part of armed units of Ukraine directly opposing the Russian Federation constitutes high treason by joining the enemy's side (Article 275 of the Russian Criminal Code).

In addition to one-time ideological acts of terrorism and sabotage, the sponsors of decentralized subversive and terrorist networks call for systematic paid acts of sabotage and terrorism as a permanent source of criminal income. Thus, their actions have attributes of terrorism and sabotages financing, which entails more severe criminal penalties.

A new element of financing extremist, separatist, subversive and terrorist activities is a widespread use of cryptocurrencies [5].[5]

We observe a change in fundraising tactics. If fundraising through pinned messages in profiles or links was historically open (before 2023), financial details are now sent to interested parties in a direct message.

We record the use of criminal blockchain analytics services (AML bot, Antinalysis, etc.) allowing to analyze the use of transactions from the point of view of law enforcement agencies. A user receives a probability score of marking his or her transactions as suspicious and blocking his or her cryptocurrency assets [6]. It allows criminals to test their money laundering / terrorism financing (ML/FT) methods.

The degree of conspiracy is growing, coordinators of crimes tend to change the IP addresses of their accounts, and publish verification QR codes as stricter security measures.

It is recommended to use a VPN and safe browser mode for financial transactions.

The common practice is the use of dropper services (issuing cards to third parties) and purchase of identifiers (e-mail, Telegram accounts), verification in payment systems and on crypto exchanges, withdrawal of funds to crypto wallets in various currencies, and cash withdrawal through "gray" exchangers.

The coordinators are aware of open cryptocurrency blockchain databases and successful deanonymization of cryptocurrency transaction parties by law enforcement agencies, the sponsors of network movements suggest using anonymity-enhanced cryptocurrencies (primarily, Monero) and shadow financial infrastructure (gray crypto exchangers, mixers, shadow cross-chain bridges) to collect donations.

It is worth noting that financing of organizations, extremist associations, and movements undesirable in the Russian Federation; terrorism and subversive activities are criminal offenses (Part 2, Article 284.1 of the Russian Criminal Code *Activities of a Foreign or International Organization Declared Undesirable in the Russian Federation*; Article 282.3 of the Russian Criminal Code *Financing of Extremist Activities*, Article 205.1 of the Russian Criminal Code *Assistance to Terrorist Activities*, and Article 281.1 of the Russian Criminal Code *Assistance to Subversive Activities*).

However, the lawmakers have provided special grounds for exemption from criminal liability under these articles, if a person assisted in prevention or suppression of a crime that he or she financed or assisted in, unless his or her actions have another *corpus delicti*. To be exempt from liability for financing extremist activity (Article 282.3 of the Russian Criminal Code), the following condition must be met: the crime is committed for the first time.

For purposes of a research on financing arrangements of decentralized subversive and terrorist networks, we will review open blockchain data on the financing of some subversive and terrorist movements obtained by publicly available tools of cryptocurrency transaction monitoring.

The criminological significance and evidentiary foundations of publicly available graphs of cryptocurrency transactions of subversive and terrorist network movements lie in documenting the criminal activity of all participants and their connections. The decentralized blockchain base provides a reliable and consistent record of any financial cryptocurrency transactions, including suspicious and criminal. Data registered in the blockchain cannot be deleted or changed (blocks are linked by a system of cryptographic proofs, and eventual changes of data require enormous computing power).

Thus, the analysis of transactions of a public crypto wallet of the extremist movement *League of Free Nations* shows the withdrawal of funds to the Ukrainian crypto exchange Whitebit, the gray cryptocurrency exchanger Obmenka SU, and criminal darknet platforms, including Mega DarkMarket and OMG, used for the illegal sale of drugs and criminal services.

A special feature of *Free Chuvashia—Volga Bulgaria* Telegram channel (the movement is declared extremist), which raises donations for the needs of the Armed Forces of Ukraine and terrorist organizations (*FRL*, *RVC*), is its business nature. The channel's administration constantly advertises the so-called "Chuvash cryptocurrency."

It is planned to create a system of personal accounts, where you will be able to control cryptocurrency assets by

[5] Social Media and Terrorism Financing. Asia/Pacific Group on Money Laundering / Middle East and North Africa Financial Action Task Force. January 2019. P. 6, 11–14. URL: www.apgml.org (accessed on December 01, 2024).

confirming Chuvash origin (knowledge of the language or any documents) or paying a certain amount in tokens. Those who have passed this verification may vote on the distribution of tokens or delegate their vote to a representative. The cryptocurrency will be transferred to *Chuvashia Liberation Fund* for "de-occupation of the homeland."

The project resembles a private, ethnically oriented financial cryptocurrency "Ponzi scheme" with attributes of an illegal financial market player (no regulatory licenses, declared guarantees of profitability, no protection of rights of consumers of financial services).

From the crypto wallet of the *Rospartizan* subversive and terrorist movement published in an open Telegram channel, funds are withdrawn to the Dubai exchange Bybit and the Ukrainian exchange Kuna (in breach of FATF standards and anti-money laundering laws, the provider does not have a mandatory verification of transaction parties).

Study of a transaction via the *Rospartizan* wallet on June 23, 2024, allows to identify a transit IP address from which money is provided both for the *Rospartizan* subversive and terrorist movement and for the terrorist organization *Freedom of Russia Legion*.

An analysis of financial transactions via the donation wallet of the subversive and terrorist movement *Black Bridge Support* shows that the transaction parties use the high-risk mixer Coin Join Mixer, cryptocurrency transit through the wallet of the Polish organization *Civic Council* (declared undesirable in the Russian Federation), and withdrawal of funds to the Ukrainian exchange Kuna in breach of ML/FT laws.

The Ethereum IP address of *Black Bridge Support* crypto wallet is also of interest. The financial transaction scheme has recorded a withdrawal of funds to a shadow cross-chain bridge with further exchange of cryptocurrencies. Ethereum analyzers record the exchange of Bitcoins for Litecoins, and the use of the automatic crypto exchanger EXch supporting multi-currency transactions with Bitcoins, Litecoins, Ethereums, and Moneros. This example demonstrates the use of a digital alternative of the hawala system to finance terrorist activities.

The funds from the crypto wallet of the terrorist organization *Russian Volunteer Corps* are transferred, *inter alia*, to a Hotwallet account (similar to a correspondent account) registered in the USA, which indicates that one of its sponsors/coordinators is in the United States. Thus, American regulators and crypto service providers, who have imposed sanctions on Russian payment and financial messaging systems and frozen crypto accounts of Russian nationals, are turning a blind eye to deliberate financing of terrorist activities in the Russian Federation.

Most accounts related to the Ukrainian cryptocurrency industry and registered in the relevant jurisdiction are involved in or directly serve shadow and criminal financial activities. For example, the Ukrainian online exchanger BTCBank (https://btcbank.com.ua). This financial platform has long specialized in supporting major drug trading platforms, including RAMP and HYDRA, in transit, cash withdrawal and laundering of proceeds from online contactless sale of drugs and psychoactive substance, and gambling (a connection with 16,410 criminal transactions has been documented).

Blockchain databases show 1,288 transactions worth 74.13 Bitcoins from BTCBank to RAMP and 44 transactions from RAMP to BTCBank worth 34.1 Bitcoins. There were 3,022 transactions worth 23.9 Bitcoins from BTCBank to HYDRA, and 220 transactions from HYDRA to BTCBank worth 51.6 Bitcoins. 92.3 Bitcoins (3,922 transactions) were transferred from BTCBank to the online casino 999.Dice.[6] In turn, 93.7 Bitcoins (2,667 transactions) were transferred to BTCBank.

A similar cash flow structure is typical for the Ukrainian exchangers CoCO-Pay (a connection with 5,216 criminal transactions has been documented) and MINE.exchange. Cryptocurrency transaction graphs show a withdrawal of 35.9 Bitcoins from CoCO-Pay to HYDRA, and 9.62 Bitcoins to Mega. 12.22 Bitcoins were transferred to 1XBET[7] online casino.

We can track transfers of 3,209 Bitcoins (119,919 transactions) from MINE.exchange to HYDRA. In turn, 11,586 transactions worth 707 Bitcoins were transferred from HYDRA to MINE.exchange.

Analysis of financial transactions shows that crypto exchangers BTCBank, CoCO-Pay, and MINE.exchange do not have anti-money laundering compliance control and act as a technical cash withdrawal and laundering platform for organized crime.

CONCLUSIONS

Most of contemporary anti-Russian separatist, and subversive and terrorist movements emerged long before the Special Military Operation. These online movements are supervised by Ukrainian secret services. This is indicated by the founders of separatist, and subversive and terrorist projects (parliamentary associations and commissions of Verkhovna Rada of Ukraine, coordination by the Office of the President), the place of registration of separatist organizations, IP addresses of accounts and public pages, and payment details.

All separatist and subversive and terrorist networks use cryptocurrencies (primarily anonymity-enhanced cryptocurrencies), the Ukrainian shadow financial infrastructure that breach anti–money laundering standards, and services of criminal exchangers (OMG, Mega, RAMP, etc.) [7, 8].

[6] Social Media and Terrorism Financing. Asia/Pacific Group on Money Laundering / Middle East and North Africa Financial Action Task Force. January 2019. P. 6, 11–14. URL: www.apgml.org (accessed on December 01, 2024).

[7] 1XBET is included in the register of blocked sites of the Federal Tax Service of Russia.

Most terrorism and extremism financing schemes are obviously similar to suspicious financial transactions related to illegal online drug distribution (numerous intricate transactions with long chains of intermediate transactions that have no clear economic purpose are recorded). To identify the organizers and accomplices of subversive and terrorist activities, it is required to analyze financial connections of the perpetrators.

Social media data parsing and macro analysis of some Ukrainian financial institutions and virtual asset service providers (Privatbank, Monobank digital bank, crypto exchangers BTCBank, MINE.exchange and CoCO-Pay, crypto exchange Kuna, etc.) show their involvement in gray financial schemes and a certain focus on money laundering and financing of terrorism. This is a sufficient ground for nominating Ukraine to the FATF sanctions lists.

Regardless of their ideological connotations and profiles, any radical network movements are interested in advertising, branding, and financing, therefore they exploit a variety of topics and, due to the attitudes of supervisors / main sponsors / end beneficiaries and opportunistic interests, may cooperate in a wide range of areas.

To document decentralized subversive and terrorist activities, law enforcement agencies need to prove involvement of the individuals in an online movement, including the similarity of goals, use of a brand, name, abbreviation, symbols, cross-advertising and financing, cross-posting, identical founders and beneficiaries.

Most special subversive and terrorist movements (*Rospartizan*, *Russian Movement Right of Power*, *Black Bridge*, *Black Bridge Support*, *Exposition of Revolutionary Anarchism*) have neither been banned in the Russian Federation nor declared terrorist, which requires a proper response from the State. The special agencies of Ukraine that supervise them (Main Intelligence Directorate and Security Service of Ukraine) are not declared terrorist.

When preparing motions for injunction, it is advisable to use the widest possible range of alternative names for the structure. It allows to identify, document, and suppress various links and organizational types of criminal networks. Participation in such criminal online movements should be qualified under more strict *corpora delicti* of the Russian Criminal Code.

In addition, the above facts and analysis of online subversive and terrorist activities could be used by Russia on international anti-money laundering (FATF, similar regional groups, the Egmont Group) and anti-terrorist platforms (special-purpose committees of the UN, RATS of SCO, ATC of CIS) as arguments to challenge the claims of the collective West and defend our national interests.

REFERENCES

1. Davitadze MD. Criminal liability for sabotage. *Bulletin of the Moscow university of the ministry of internal affairs of Russia.* 2020;(3):169–173. EDN: SOYWGE doi: 10.24411/2073-0454-2020-10163

2. Lisovskij DG, Moiseenko EE. The criminal-legal and social essence of sabotage. *E-Scio.* 2022;(4):181–185. EDN: IRAREM

3. Tutukov AYu, Tatarov LA. The correct qualification of act of terrorism and its distinction from diversion. *Gaps in Russian Legislation.* 2018;(6):166–170. EDN: YPOQYX

4. Hrustalev MA. Sabotage and terrorist warfare as military and political phenomenon. *International Trends.* 2003;(2):55–67. EDN: OIPOIP

5. Teichmann F., Park E. Terrorismusfinanzierung durch Kryptowaehrungen. *ZRFC.* 2018;(2). doi: 10.37307/j.1867-8394.2018.02.05

6. Krasinsky VV. Countering the financing of terrorism using cryptocurrencies. *Modern Law.* 2022;(9):108–115. EDN: LDHFOO doi: 10.25799/NI.2022.58.84.018

7. Krasinsky VV, Leonov PYu, Morozov NV. Criminological research of cryptocurrency blockchains in the russian anti-laundering system. *Modern Law.* 2024;(5):75–82. EDN: SWGQID

8. Krasinsky VV, Norkina AN. The use of artificial intelligence in the field of countering money laundering and terrorist financing. *Modern Law.* 2024;(8):88–94. EDN: BRTINO doi: 10.25799/NI.2024.43.93.017

СПИСОК ЛИТЕРАТУРЫ

1. Давитадзе М.Д. Уголовная ответственность за диверсию // Вестник Московского университета МВД России. 2020. № 3. С. 169–173. EDN: SOYWGE doi: 10.24411/2073-0454-2020-10163

2. Лисовский Д.Г., Моисеенко Е.Е. Уголовно-правовая и социальная сущность диверсии // E–Scio. 2022. № 4(67). С. 181–185. EDN: IRAREM

3. Тутуков А.Ю., Татаров Л.А. Правильная квалификация террористического акта и его отграничение от диверсии // Пробелы в российском законодательстве. 2018. № 6. С. 166–170. EDN: YPOQYX

4. Хрусталев М.А. Диверсионно-террористическая война как военно-политический феномен // Международные процессы. 2003. Т. 1, № 2(2). С. 55–67. EDN: OIPOIP

5. Dr. Teichmann F., Park E. Terrorismusfinanzierung durch Kryptowaehrungen // ZRFC. 2018. № 2. doi: 10.37307/j.1867-8394.2018.02.05

6. Красинский В.В. Противодействие финансированию терроризма с использованием криптовалют // Современное право. 2022. № 9. С. 108–115. EDN: LDHFOO doi: 10.25799/NI.2022.58.84.018

7. Красинский В.В, Леонов П.Ю., Морозов Н.В. Применение искусственного интеллекта в сфере противодействия отмыванию денег и финансированию тероризма // Современное право. 2024. № 5. С. 75–82. EDN: SWGQID

8. Красинский В.В., Норкина А.Н. Криминологические исследования блокчейнов криптовалют в российской антиотмывочной системе // Современное право. 2024. № 8. С. 88–94. EDN: BRTINO doi: 10.25799/NI.2024.43.93.017

AUTHOR INFO

Alexander Dzh. Kerimov, Dr. Sci. (Jurisprudence), professor, chief researcher; eLibrary SPIN: 7041-9829;
e-mail: 8017498@mail.ru
***Vladislav V. Krasinsky,** Dr. Sci. (Jurisprudence), associate professor; ORCID: 0000-0001-6354-4644;
eLibrary SPIN: 9577-6810; e-mail: VVkrasinskii@mephi.ru

ОБ АВТОРАХ

Александр Джангирович Керимов, д-р юрид. наук, профессор, главный научный сотрудник;
eLibrary SPIN: 7041-9829; e-mail: 8017498@mail.ru
***Владислав Вячеславович Красинский,** д-р юрид. наук, доцент; ORCID: 0000-0001-6354-4644;
eLibrary SPIN: 9577-6810; e-mail: VVkrasinskii@mephi.ru

* Corresponding author / Автор, ответственный за переписку