ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2020-10-1-14-20
УДК 327(045)

Угрозы терроризма в условиях цифровой трансформации мира и пути защиты от них

В.И. Глотов[a], **Д.М. Михайло**в[b], **В.А. Педанов**[c]
[a] Федеральная служба по финансовому мониторингу, Москва, Россия
[b] Физический институт им. П.Н. Лебедева Российской академии наук, Москва, Россия
[c] Центр международной информационной безопасности и научно-технической политики МГИМО МИД России, Москва, Россия
[a] https://orcid.org/0000-0002-0583-0797; [b] https://orcid.org/0000-0003-0357-7772;
[c] https://orcid.org/0000-0003-2188-117X

АННОТАЦИЯ

В работе исследуются проблемы одной из наиболее значимых на сегодняшний день мировых угроз — терроризма и его важной и трансграничной формы — кибертерроризма. Интерес представляет проведенный авторами анализ информационно-коммуникационных технологий, используемых при осуществлении террористической деятельности и непосредственно для актов кибертерроризма. Приводится ряд актуальных примеров и практических кейсов применения информационно-коммуникационных технологий со стороны террористов. Сделан вывод о необходимости совместного поиска решений в борьбе с террористической угрозой в рамках международного сообщества, предлагаются определенные шаги в этом направлении.

Ключевые слова: кибертерроризм; информационная безопасность; информационно-коммуникационная сфера

Для цитирования: **Глотов В.И., Михайлов Д.М., Педанов В.А. Угрозы терроризма в условиях цифровой трансформации мира и пути защиты от них.** ***Гуманитарные науки. Вестник Финансового университета.*** **2020;10(1):14-20. DOI: 10.26794/2226-7867-2020-10-1-14-20**

ORIGINAL PAPER

Threats of Terrorism in the Context of the Digital Transformation of the World and Ways of Protection Against Them

V.I. Glotov[a], **D.M. Mikhailov**[b], **V.A. Pedanov**[c]
[a] Federal Financial Monitoring Service, Moscow, Russia
[b] Lebedev Institute of Physics of the Russian Academy of Sciences, Moscow, Russia
[c] Centre of International Information Security and Scientific-Technical Policy of the MGIMO-University, Moscow, Russia
[a] https://orcid.org/0000-0002-0583-0797; [b] https://orcid.org/0000-0003-0357-7772;
[c] https://orcid.org/0000-0003-2188-117X

ABSTRACT

This article deals with the problems of one of the most urgent threats in the world today — the problem of terrorism, and its essential and cross-border form — cyberterrorism. It is of growing interest in the analysis of information and communication technologies used in the implementation of terrorist activities and directly for acts of cyberterrorism. We present several relevant examples and practical cases of the use of information and communication technologies by terrorists. The authors concluded that it is necessary to jointly search for solutions to combat the terrorist threat from terrorist organisations within the international community.

Keywords: cyberterrorism; information security; information and communication sphere

For citation: **Glotov V.I., Mikhailov D.M., Pedanov V.A. Threats of terrorism in the context of the digital transformation of the world and ways of protection against them.** ***Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University.*** **2020;10(1):14-20. DOI: 10.26794/2226-7867-2020-10-1-14-20**

Вызовы и угрозы, с которыми столкнулись Россия и все мировое сообщество во втором десятилетии XXI в., в значительной степени связаны со стремительно растущей ролью информационно-коммуникационных технологий (ИКТ). Их широкое распространение на сегодняшний день является не только залогом технологического прогресса и успешного развития общества, но и причиной высокой степени зависимости человечества от безопасности информационно-коммуникационной сферы. Традиционно эту сферу рассматривают через призму единой «триады» — угроз военно-политического, криминального и террористического характера. Благодаря развитию и доступности ИКТ появилось новое явление — кибертерроризм. Термин возник в 80-х гг. прошлого столетия и был предложен Барри Коллином — старшим научным сотрудником Института безопасности и разведки (Institute for Security and Intelligence). Он использовался в контексте тенденции перехода терроризма из физического в виртуальный мир и конвергенции угроз в этих мирах [1]. О применении террористами ИКТ-технологий и различных методик известно с момента возникновения Исламского государства (ИГ/ИГИЛ/ДАИШ).

В последнее время все реже можно найти их страницы в социальных сетях, так как идет активная борьба государственных служб с данными аккаунтами. Это обусловливает переход пользователей в относительно закрытое информационное пространство, существующее в мессенджерах. В начале 2015 г. стало известно, что ИГ разработало 34-страничное руководство по обеспечению безопасности связи. Документ, имеющий в своей основе инструкцию по общим вопросам кибербезопасности, появился на форумах джихадистов. В нем были перечислены и наиболее пригодные для использования приложения, в том числе и Telegram (https://techcrunch.com/2016/01/16/isis-app/).

Это только один мессенджер, которым пользуется ИГИЛ. Представителями преступных организаций используются также WhatsApp, RedPhone, Signal и Wickr. Павел Дуров, основатель Telegram, был подвергнут многочисленным обвинениям в пособничестве ИГИЛ. При этом со стороны Telegram было объявлено о блокировке 600 террористических аккаунтов и постоянном характере такой деятельности. Однако найти аккаунты экстремистского содержания до сих пор возможно, наример: @is2020, @shamtoday_1, @ccs_muslim_lib, @ccs_muascar1, @knida-djihada, @FATIXA_6. При этом наблюдается значительное количество каналов, которые представляют не только русскоязычный контент, но также с изменением цифр (например, @FATIXA_16) ведутся на других языках.

В январе 2016 г. группа Ghost, специализирующаяся на борьбе с терроризмом, обнаружила в Сети мессенджер, созданный боевиками, — Alrawi. Это приложение для Android нельзя скачать в Google Play — оно доступно в так называемых «темных», глубоких разделах Сети. Alrawi пришло на смену приложению Amaq — мессенджеру, предоставляющему доступ к потоку новостей и пропагандистских роликов, в том числе кадрам казней и видео с полей битвы. Но, в отличие от Amaq, Alrawi имеет оконечное (сквозное) шифрование (http://fortune.com/2016/01/13/isis-has-its-own-secure-messaging-app).

Предполагается, что террористические организации могут использовать в узком кругу строго для координации действий террористов руководящего уровня или террористов-смертников разработки на основе открытого исходного кода популярных платформ для общения, например на основе открытого кода Signal.

Привлекает внимание приложение CCS, которое курсирует по просторам Сети и позиционирует себя как «средство общения для братьев и сестер по вере», но на самом деле за ним стоят радикальные исламисты. 1 сентября 2016 г. на канале CCS Links (в настоящее время заблокирован, но функционируют каналы со схожей тематикой: @ccs_muslim_lib, @ccs_muascar1) в мессенджере Telegram началось распространение информации о создании собственного средства для переписки мусульман по всему миру. Разработчики утверждают, что приложение стало результатом двухлетней работы и является своеобразной площадкой для исламских радикалов, где они могут свободно обмениваться информацией. Новое приложение не подразумевает сложного процесса регистрации — достаточно логина и пароля. Никакой привязки к номеру телефона — в отличие от популярных мессенджеров, человек «не засветит» свой телефон при переписке. Кроме того, согласно информации разработчиков, новый мессенджер не хранит переписку и не логгирует IP пользователей.

На данный момент большая часть рекламируемых каналов недоступна для широкого пользователя, однако уже представленная в CCS информация несет пропаганду радикального ислама: в частности, там представлены ссылки на каналы террористов ИГ.

Выделим методики и средства работы в информационном поле со стороны террористической группировки ИГИЛ:

1. **Применение положительных образов**, чтобы привлечь новую аудиторию и создать притягательный образ ИГИЛ. Так, телеканал CNN в 2015 г. опубликовал видеоролик, где говорилось о том, что члены ИГИЛ часто используют фотографии с котятами, смайлы emoji и шоколадную пасту Nutella. Тем самым, считает CNN, вербовщики ИГИЛ привлекают внимание женской аудитории. Такие образы используются, чтобы показать, что жизнь в Исламском государстве ничем не отличается от жизни обычных людей. Данное явление отмечает и британская газета The Independent. В статье, посвященной Twitterаккаунту Islamic State of Cats (@ ISILCats), говорится, что большая часть авторов таких постов называют нарисованных животных mewjahids [мяуджахедами] по аналогии с моджахедами. Подобная проблема вызывает беспокойство Мохаммеда Шарифа, главы мусульманской организации Ramadhan Foundation: «Если мы не будем с этим бороться, то все эти милые публикации в Facebook и Twitter приведут к тому, что будет считаться обычным делом ехать в Ирак и Сирию, чтобы участвовать в военных действиях» (http://goo.gl/Ai26lY).

Анализ ряда новостных сайтов и сообщений в Twitter показывает, что твитты сопровождаются картинками, где боевики общаются с детьми, раздают им еду и оказывают социальную поддержку. К примеру, весной 2014 г. ИГИЛ опубликовал очередное видео, где боевик ИГИЛ — бывший немецкий рэп-исполнитель Дэнис Гусперт играет в снежки и веселится со своими приятелями по экстремистской организации: «Теперь вы можете видеть… Здесь, в Сирии, мы тоже умеем веселиться! Это джихад, джихад строит веселье… и мы тут веселимся с детьми… Давай же, мы приглашаем тебя в джихад!» (http://goo.gl/JRAJkq).

2. **Специальные приложения для платформы Andriod**. ИГИЛ создало свой специальный Twitter — Fajr al-Bashaer, или Dawn of Good Tidings, который помечен как потенциально опасный. Если попытаться его установить, то автоматически запрашивается доступ к персональным данным, а после загрузки отправляются материалы о борьбе ИГИЛ в Сирии и Ираке. Чтобы обойти защиту системы антиспама, после каждого слова и символа ставятся пробелы. Более сотни пользователей загрузили данное приложение на свои Android-телефоны через Google Play Store. Dawn of Good Tidings стало особенно активно использоваться летом 2014 г. Именно в то время ИГИЛ захватило город Мосул на севере Ирака. На данный момент скачивание приложения остановлено.

3. **Анализ целевой аудитории**. Особое внимание создатели медиа-продукции ИГИЛ уделяют изучению характеристик целевой аудитории. Именно это позволяет террористической пропаганде иметь успех и эффективность, а, значит, увеличить и шансы у вербовщиков. Если используется Facebook, то пишут смысловые посты, а если Twitter, то короткие, но информативные записи. В Instagram это в первую очередь ориентация на визуальное восприятие информации и т.д. Чтобы создать иллюзию видеоигры военной тематики, камера прикрепляется к стволу автомата, и с такого ракурса снимается казнь заложников. Подобные игры весьма популярны среди молодых людей и подростков от 16 лет (http://goo.gl/p8Ujs4).

Создано еще одно приложение Huroof, специализирующееся на обучении детей арабскому алфавиту и грамматике. Приложение поражает удобством в пользовании и хорошим методом подачи информации. Фон сделан в спокойных тонах: цветочки и звездочки. На нем всплывают арабские буквы, а в связке к буквам приведены слова военной тематики. Ведется обучение в виде интерактивного игиловского нашида (мусульманское песнопение, традиционно исполняемое мужским вокалом соло или в хоре без сопровождения музыкальных инструментов) (http://goo.gl/6vbnZx).

4. **Технология Twitter Storms (ботнет-атаки)**. Twitter Storm — это специальный термин, которым обозначают компании по рассылке заранее подготовленных массовых постов. Ежедневно тысячи пользователей социальных сетей размещают свои посты с одинаковыми хэштегами, так что они становится популярными в сети.

Также, по словам российского источника, формат Twitter Storm используется для «прощупывания настроений» среди целевой аудитории,

с помощью массовых опросников на различные темы. Например, летом 2014 г. ИГИЛ опубликовал несколько сообщений о том, что хочет вновь создавать халифат во всем мире, а не только на территории Сирии и Ирака. Однако подписчики начали высказывать свое неодобрение, поэтому специалисты ИГИЛ быстро закрыли данную кампанию и сняли с себя ответственность за подобного рода сообщения (http://apparat.cc/network/isis-social-war).

Британская газета The Guardian приводит пример, как террористы проводят опросы в Интернете. Так, в сентябре 2014 г. активный пользователь Twitter Абдульрахман аль-Хамид попросил у своих 4000 подписчиков помочь ему определить самые популярные хэштеги в Великобритании, чтобы продвинуть контент ИГИЛ. В то время шло активное обсуждение возможного отделения Шотландии, поэтому подписчики начали присылать такие хэштеги, как #scotlandindependence, #andymurray, #VoteYes #scotland, #VoteNo (http://goo.gl/iF33gy). Считается, что именно Twitter Storms активно используется для привлечения внимания общественности к посланиям ИГИЛ.

5. **Ориентация на иностранных граждан**. Целью ИГИЛ является вербовка союзников не только с Ближнего Востока, но и из стран западного региона. «Аль-Фуркан» выпускает продукцию не только на арабском языке, но и на русском, французском, английском, турецком, немецком и испанском, что является ярким примером ориентации на западного читателя. Например, данное медиаподразделение осуществляет перевод речей Абу Бакра аль-Багдади (лидера ИГИЛ) на французский, индонезийский, русский, турецкий и английский языки. Так как английский является международным языком, то особое внимание ИГИЛ уделяет соответствующему контенту. Таким образом исламское государство пытается войти в мировое сообщество, создав продукцию, которая понятна каждому человеку (http://goo.gl/ZzEVcW).

6. **Интернет-магазины специализированной продукции с символикой ИГИЛ**. На страницах Facebook и специально созданных сайтах, приложениях продается разнообразная одежда с символикой ИГИЛ. Хотя на данный момент большинство страниц в Facebook, которые занимались подобной деятельностью, заблокированы, создаются новые страницы. Типичными слоганами на одежде являются: Muslim Brotherhood, F**k Israel, Pray for Gaza и Mujahedeen Around The World United We Stand (http://goo.gl/4UeFJv). Например, в Триполи существует магазин с товарами ИГИЛ, где можно увидеть различную продукцию — от одежды до сувениров с характерной символикой (http://goo.gl/vyUUm4).

7. **Использование имиджа лидеров мнений**. Еще одним важнейшим механизмом пропаганды ИГИЛ стало использование образов известных личностей, которые стали членами ИГИЛ. Яркие примеры — рэп-исполнитель Денис Гусперти и британская рок-певица Салли Джонс. Российский пример — актер Вадим Дорофеев. Существуют случаи, когда молодые футболисты тоже присоединялись к террористической организации ИГИЛ.

8. **Использование социальных сетей для набора рекрутов**. Набор новых участников происходит через социальные сети Twitter и Facebook (http://aitmag.ahram.org.eg/News/753.aspx). В основном рекрутеры ориентированы на молодых людей, которые имеют экстремистские взгляды. Процедура довольно проста: сначала идет обсуждение вопросов, связанных с функционированием ИГИЛ, потом — перспектив приема на службу. Цель рекрутера — создать положительный образ организации и помочь будущему участнику добраться до пункта назначения. Варвара Караулова в своем интервью на канале «Россия-1» подробно рассказала о том, как происходила переписка. Согласно данным, которые предоставили европейские органы безопасности, в 2014 г. к джихаду в Сирии присоединились более 700 граждан Франции, 300 — Германии, 250 — Бельгии, 250 — Австралии, 100 — США, 50 — Испании и около 500 — Великобритании. Стоит отметить, что во время общения в Сети тщательно скрываются имена рекрутеров и того, кто должен помочь будущим членам группировки с переездом. Обычно диалог заканчивается такими фразами: «Выдвигайся, и Аллах покажет тебе дорогу», «Ты найдешь этих людей», «Ищи того, кто свяжется с тобой» и т.д. Позже диалог переходит в мессенджеры (http://www.alhaya.ps/arch_page.php?nid=243269).

9. **Логистика и финансовые вопросы.** По сообщению газеты «Аль-Арабия», которая является одной из наиболее авторитетных на Ближнем Востоке, ИГИЛ использует социальные сети для решения своих финансовых вопросов и вопросов логистики. Таким образом, социальные сети

являются не только основой для пропагандирования и рекрутирования. Так, интернет-сайт «Ас-Сакина» ссылается на газету «АльДжазира» и сообщает, что на страницах Facebook члены ИГИЛ осуществляют финансовые операции, при этом личность, которая осуществляет данные процессы, остается неизвестной.

Идеологи террористических формирований постоянно разрабатывают изощренные способы агитации и вербовки в свои ряды новых людей, а технологии предоставляют возможность делать это эффективней (сохранять скрытность, оказывать воздействие на широкую аудиторию).

Помимо обозначенных технологий, террористы также могут использовать различные порталы в так называемом Darknet, где участники обмениваются анонимными сообщениями на закрытых форумах. Например, на портале http://vlr2sz44rxf5wmuu.onion/ — ISIS Red Room.

Приведенные примеры использования цифровых технологий Исламским государством вовсе не означают исключительную возможность воздействия на общество со стороны только этой организации. Так, в странах Юго-Восточной Азии, где ислам имеет широкое распространение, проблема терроризма и, как следствие, кибертерроризма тоже присутствует. В Юго-Восточной Азии действуют такие террористические группы, как Джемаа Исламия (Jemaah Islamiyya (JI), Абу Сайяф (Abu Sayyaf — ASG), Мауте (Исламское государство Ланао) и ряд других, некоторые из них ассоциированы с Исламским государством. Предполагается, что одним из способов заработка подобных организаций является киберпреступность. Функционирующий в составе Исламского государства так называемый Кибер Халифат (Islamic State Hacking Division или United Cyber Caliphate) разворачивает свою деятельность с привлечением, в том числе, и представителей стран Юго-Восточной Азии. Обращает на себя внимание тот факт, что среди объектов успешных атак, проведенных кибер-халифатом, присутствуют малазийские, а также значительное число австралийских. Среди атак, произведенных группировками, объединенными названием Cyber Caliphate, значатся следующие:

• атака на сайт австралийского аэропорта весной 2015 г. (https://www.telegraph.co.uk/news/worldnews/islamic-state/11531794/Australian-airport-website-hacked-by-Islamic-State.html);

• веб-сайт национальной авиакомпании Малайзии Malaysia Airlines. За атакой стояли представители Official Cyber Caliphate, разместившие информацию об этом на самом портале (https://www.securitylab.ru/news/470437.php);

• атака на французский телеканал TV5Monde Live Feed в июле 2015 г., когда в рамках брутфорс-атаки был получен доступ к социальным медиа и размещено сообщение провокационного характера Je Suis ISIS, что после серии терактов во Франции воспринималось как агрессивная угроза обществу (http://www.france24.com/en/20150409-france-tv5monde-is-group-hacking);

• несанкционированный доступ к базе данных Министерства обороны США (август 2015 г.); данные примерно о 1400 военнослужащих были размещены в Интернете в «расстрельном списке», что, безусловно, является элементом информационной войны (https://www.theguardian.com/world/2015/aug/13/isis-hacking-division-releases-details-of-1400-americans-and-urges-attacks);

• в сентябре 2015 г. атаке подверглась переписка секретного характера в Британском правительстве. Скомпрометированные письма касались высших членов кабинета министров. Вторжение было обнаружено Центром правительственной связи Великобритании — GCHQ (https://www.mirror.co.uk/news/uk-news/isis-hackers-intercept-top-secret-6428423);

• 15 апреля 2016 г. хакеры United Cyber Caliphate провели успешную атаку 20 австралийских веб-сайтов в рамках скоординированных действий против австралийского бизнеса. Некоторые из веб-сайтов после атаки перенаправляли пользователя на страницы, содержащие информацию террористического характера;

• в апреле 2017 г. United Cyber Caliphate выпустил «расстрельный список» для одиночных атак, в который вошли 8786 человек (https://www.newsweek.com/isis-linked-cyber-group-releases-kill-list-8786-us-targets-lone-wolf-attacks-578765).

Наибольшее число актов кибертерроризма пришлось на 2015 г., равно как и наибольшая активность террористов, наносящих физический вред. Представляется, что дальнейший спад активности связан с началом Россией антитеррористической операции в Сирии, а также с деятельностью международной коалиции, возглавляемой США. Так, в конце 2015 г. в результате ракетно-бомбового удара был ликвидирован предположительно основатель и один из лидеров Cyber Caliphate — Джунаид Хуссейн, который

являлся видным специалистом по информационной безопасности в рядах ИГИЛ. В ответ на это хакеры Cyber Caliphate в результате массивной брутфорс-атаки взломали более 54 000 Twitter аккаунтов сотрудников ЦРУ и ФБР [2].

Ряд действий, совершаемых террористическими организациями исламского толка, в том числе публикация подробных данных о личном составе противника с целью запугивания или устранения физических лиц, могут быть поставлены в один ряд с действиями националистических экстремистских группировок. Примером может служить веб-портал «Миротворец», на котором размещаются личные данные людей, собранные нелегальным путем (хакинг, фишинг) и средствами разведки по открытым источникам. При этом, вопреки провозглашенной цели создания сайта и широко распространенному мнению, что сайт публикует личные данные лиц, которые причастны к преступлениям против основ национальной безопасности Украины, мира и безопасности ее граждан, 8 октября 2015 г. на портале были опубликованы личные данные российских военнослужащих, проходящих службу в Сирии и ведущих там борьбу с международным терроризмом. Автор украинского сайта «Миротворец» — Георгий Тука. До событий на Украине он два с половиной года жил в Каире и участвовал в «арабской весне», с которой и началась гражданская война в Сирии и становление терроризма на Ближнем Востоке (http://society.lb.ua/war/2015/01/03/291256_georgiy_tuka_dazhe_stal.html).

Факты свидетельствуют о широкой распространенности проблематики кибертерроризма и большом количестве кибератак. В этой связи определение самой природы кибертерроризма, на наш взгляд, является необходимым для комплексной и эффективной борьбы с ним.

Кибертерроризм по своей сущности может быть определен как часть киберпреступности по тому же принципу, по которому террористическая деятельность относится к преступной. Однако при выделении угроз использования информационно-коммуникационных технологий для международной информационной безопасности угрозу кибертерроризма стоит выделять как отдельный вызов международному сообществу, требующий эффективного и адекватного ответа.

Кибертерроризм — это одна из форм терроризма. Сама природа информационно-коммуникационных технологий в значительной мере определяет его международный характер. Это, в свою очередь, требует ряда определенных действий со стороны международного сообщества. Речь идет прежде всего об уполномоченных органах ООН, таких как Совет безопасности ООН, КТК ООН и система международных уголовно-правовых институтов.

Применение передовых технологий в информационно-коммуникационном поле в рамках террористической деятельности может иметь значительные негативные последствия для всего мирового сообщества.

К числу угроз международной информационной безопасности, связанной с применением ИКТ, могут быть отнесены исходящие от киберпреступности, террористических организаций, а также информационные и кибернетические угрозы, исходящие от государств и военных альянсов.

В качестве мер, позволяющих противостоять подобным угрозам, могут быть названы политические, правовые и технические. Технические методики противодействия объединяют использование различных инструментов, в том числе создание единого центра мониторинга угроз кибертерроризма и противодействия им или же сети обмена информацией о подобных угрозах. К техническим инструментам могут быть отнесены технологии обеспечения кибербезопасности, а также конкурентной разведки и мониторинга информационного поля, что позволяет не только отражать атаки в момент их осуществления, но также прогнозировать их заранее и осуществлять защиту.

К политическому направлению относятся инструменты «мягкой силы», общественной дипломатии, а также использование политической площадки ООН и других межгосударственных организаций с целью недопущения использования ИКТ для осуществления враждебных действий и минимизации последствий их применения.

Правовыми инструментами являются акты международно-правового характера, определяющие и закрепляющие общие подходы к обеспечению международной информационной безопасности.

Представляется, что только сбалансированное применение обозначенных инструментов позволит добиться обеспечения международной информационной безопасности и безопасности национального информационно-коммуникационного поля в контексте цифровой трансформации мира.

СПИСОК ИСТОЧНИКОВ/REFERENCES

1. Collin B. The Future of Cyberterrorism. *Crime & Justice International Journal*. 1997;13(2):15–18.
2. Нефёдова М. Хакеры ИГ взломали более 54 000 Twitter-аккаунтов. URL: https://xakep.ru/2015/11/10/cyber-caliphate/.
   Nefedova M. Hackers of IS broke into more than 54,000 Twitter accounts. URL: https://xakep.ru/2015/11/10/cyber-caliphate/. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Владимир Иванович Глотов — кандидат экономических наук, профессор, заместитель директора Федеральной службы по финансовому мониторингу, Москва, Россия
glotov@fedsfm.ru
Дмитрий Михайлович Михайлов — высококвалифицированный старший научный сотрудник, кандидат наук, Физический институт имени П.Н. Лебедева Российской академии наук, Москва, Россия
mikhaylovdm@lebedev.ru
Владимир Александрович Педанов — соискатель степени кандидата наук, Центр международной информационной безопасности и научно-технической политики МГИМО МИД России, Москва, Россия
v.pedanoff@gmail.com

ABOUT THE AUTHORS

Vladimir I. Glotov — Candidate of Economic Sciences, Professor, Deputy Director of the Federal Financial Monitoring Service, Moscow, Russia
glotov@fedsfm.ru
Dmitry M. Mikhailov — Senior Researcher, Candidate of Sciences, Lebedev Institute of Physic of the Russian Academy of Sciences, Moscow, Russia
mikhaylovdm@lebedev.ru
Vladimir A. Pedanov — Postgraduate student, Centre of International Information Security and Scientific-Technical Policy of the MGIMO-University of Ministry of Foreign Affairs of Russia, Moscow, Russia
v.pedanoff@gmail.com

Заявленный вклад авторов:
В.И. Глотов — общенаучное руководство, экспертная оценка исследования.
Д.М. Михайлов — теоретико-обзорная часть исследования.
В.А. Педанов — практически-аналитическая часть исследования.

Authors' declared contribution:
V.I. Glotov — General scientific guidance, expert evaluation of the research.
D.M. Mikhailov — theoretical and review part of the study.
V.A. Peganov — practical-analytical part of the study.

Статья поступила 15.07.2019; принята к публикации 20.10.2019.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article received on 15.07.2019; accepted for publication on 20.10.2019.
The authors read and approved the final version of the manuscript.