

УДК 343.326

DOI: 10.34670/AR.2022.44.88.065

Кибертерроризм как форма компьютерной преступности**Колосова Анна Борисовна**

Следователь Главного следственного управления
ГУ МВД России по Иркутской области,
664003, Российская Федерация, Иркутск, ул. Литвинова, 15;
e-mail: 38@mvd.ru

Старичков Максим Владимирович

Кандидат юридических наук, доцент,
доцент кафедры криминалистики,
Восточно-Сибирский институт МВД Российской Федерации,
664074, Российская Федерация, Иркутск, ул. Лермонтова, 110;
e-mail: 38@mvd.ru

Аннотация

Глобальная сеть «Интернет» открывает большое количество возможностей, таких как простота доступа, независимость от местонахождения, а также высокая скорость обмена информацией и относительная анонимность. Данные преимущества активно используются злоумышленниками для совершения компьютерных преступлений, в том числе и кибертерроризма. Стремительное развитие информационных технологий сопровождается увеличением совершения компьютерных преступлений. Наиболее опасной формой компьютерной преступности является кибертерроризм. В статье рассматривается понятие, особенности и способы совершения кибертерроризма, а также направления развития российского уголовного законодательства, направленного на противодействие кибератакам. Понятие кибертерроризма до сих пор не нашло легального определения и, соответственно, не предусматривается повышенной ответственности за подобные, бесспорно, общественно опасные деяния. В этом направлении первым шагом явилась криминализация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в 2017 г. и нарушений правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ) в 2022 г.

Для цитирования в научных исследованиях

Колосова А.Б., Старичков М.В. Кибертерроризм как форма компьютерной преступности // Вопросы российского и международного права. 2022. Том 12. № 10А. С. 556-562. DOI: 10.34670/AR.2022.44.88.065

Ключевые слова

Кибертерроризм, компьютерная преступность, теракт, компьютерные преступления, кибератака, ответственность, киберпространство.

Введение

Современное общество характеризуется активным внедрением компьютерных технологий практически во все сферы жизни. Управление в бизнесе, оборот денежных средств, даже некоторые юридические процессы теперь могут проходить «дистанционно» [Осодоева, 2021]. В образовании появляются и совершенствуются системы электронных библиотек и электронных дневников, в медицине – электронные картотеки пациентов, различные медицинские онлайн-сервисы и возможность записи через информационно-телекоммуникационные сети на прием к врачу, в культуре – свободный доступ к произведениям искусства. Можно с уверенностью сказать, что информационные технологии стали частью нашей повседневной жизни.

Глобальная сеть «Интернет» открывает большое количество возможностей, таких как простота доступа, независимость от местонахождения, а также высокая скорость обмена информацией и относительная анонимность [Родивилина, Родивилин, Коломинов, 2021]. Данные преимущества активно используются злоумышленниками для совершения компьютерных преступлений, в том числе и кибертерроризма [Осодоева, 2021, 36].

Основная часть

В Уголовном кодексе Российской Федерации отсутствует понятие компьютерного преступления. Другие нормативно-правовые акты также не раскрывают значение данного понятия. Формулировкой понятия компьютерного преступления или по-другому киберпреступления занимаются криминологи и ученые в области уголовного права [Васильев, Демин, 2009, 47].

Юридическая наука выделяет большое количество понятий компьютерных преступлений. Проанализировав мнения ученых и исследователей, сформулируем общее понятие. Компьютерное преступление – это общественно опасное деяние, совершаемое в киберпространстве и посягающее на общественную безопасность, права человека и собственность. При этом необходимым элементом механизма подготовки, совершения и сокрытия преступления является компьютерная информация, выступающая в роли предмета и (или) средства совершения преступления [Гейдаров, 2022].

Под киберпространством (его еще называют виртуальным пространством) понимается создаваемое средствами компьютерной техники информационное пространство, в котором существуют определенного рода объекты или информация, представленная в виде машиночитаемых символов, то есть место, в котором функционируют компьютерные программы и происходит обработка, перемещение и хранение данных [Богачев, Редин, 2012, 791].

Совершение киберпреступлений возможно только с помощью средств компьютерной техники, для функционирования которой необходимо программное обеспечение, находящееся в открытом или ограниченном доступе, а также проводных и беспроводных информационно-телекоммуникационных сетей. В настоящее время большинство компьютерных преступлений совершаются путем удаленного доступа с помощью обычной компьютерной техники, на которой установлено специальное программное обеспечение. При таком доступе злоумышленники могут находиться на значительном расстоянии от объекта посягательства, даже в другой стране, что в свою очередь создает сложности при расследовании данных преступлений.

Кибертерроризм является наиболее опасной формой компьютерных преступлений, так как создает угрозу безопасности всему обществу.

В то же время кибертерроризм является разновидностью терроризма. Понятие терроризма закреплено в ст. 3 Федерального закона от 06.03.2006 № 35-ФЗ «О противодействии терроризму». Под терроризмом понимается идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий.

Вместе с тем, понятие «кибертерроризма» законодательно не закреплено. Обратимся к науке международного права и рассмотрим мнения некоторых ученых. Так, Ю. Бочаров полагает, что кибертерроризм есть не что иное, как определенная разновидность терроризма, направленная на устрашение и иное воздействие на принятие решений различных структур с использованием современных информационно-телекоммуникационных технологий [Бочаров, www].

Д. Деннинг считает, что существует 3 различных понятия: активизм, хакеризм и кибертерроризм. Активизм – это «легитимное» использование киберпространства для пропаганды своих идей, зарабатывания денег и привлечения новых членов. Хакеризм – это хакерские атаки, проводимые для выведения из строя отдельных компьютерных сетей или интернет-сайтов, получения доступа к секретной информации, хищения средств и т.д. Кибертерроризм – это компьютерные атаки, спланированные для нанесения максимального ущерба жизненно важным объектам информационной инфраструктуры [Бочинин, 2015, 62].

К. Лорд и Т. Шарп определяют кибератаку как враждебные действия с использованием компьютеров, электронной информации и/или цифровых сетей с целью манипулирования, хищения, вывода из строя, воспрепятствования доступа, ослабления или уничтожения критически важных систем и средств, а также данных. Кибершпионаж предполагает использование компьютерных или смежных систем для сбора сведений или выполнения определенных операций в киберпространстве или в реальном мире [Лукавский, www].

Кибертерроризм носит международный и межгосударственный характер, поскольку преступники и жертвы в момент совершения теракта могут находиться в разных частях света. Вместе с этим кибертерроризм характеризуется большой степенью скрытности и плохой раскрываемостью, минимальными финансовыми затратами и нанесением глобального материального ущерба [Соколова, 2017, 115].

Кибертерракт основывается на использовании информационной инфраструктуры для создания условий, вызывающих негативные последствия для общества и государства [Хачатрян, 2018, 250]. Кроме того, отличительной особенностью кибертерроризма является открытость, выражающаяся в публичном оглашении условий и требований террориста, а также направленность действий на привлечение внимания средств массовой информации.

Некоторые ученые выделяют следующие способы совершения кибертерракта:

- несанкционированный доступ к различной информации (государственной, коммерческой, банковской и другим видам тайн, персональным данным);
- причинение значительного ущерба элементам информационного пространства (разрушение информационных сетей, порча ресурсов, создание искусственных помех и т. п.);
- захват каналов распространения информации с целью пропаганды террористической деятельности;
- воздействие на программное обеспечение и информацию (воздействие вредоносных

- программ, несанкционированное уничтожение, блокирование, копирование и искажение информации и т. д.);
- захват СМИ для распространения информации в своих корыстных целях, запугивания населения, оглашения своих условий и требований;
 - уничтожение и порча линий связи, переадресация отправлений [Аман, Истлеев, Ахметкалиев, 2018, 25].

По мнению Е.А. Капитоновой [Капитонова, 2015, 33] способы совершения кибертеракта следует разделить на две группы. Первая характеризуется совершением теракта путем непосредственного посягательства на объекты компьютерной сферы и различные информационные сети, т. е. полностью находится вне закона. Во вторую группу входят действия, направленные на распространения информации, вызывающей у населения страх и панику, при этом используются легальные электронные средства массовой информации и социальные сети [Яцкина, 2020].

В свете современных геополитических тенденций на фоне фактически ведущихся информационных войн угрозы кибертерроризма будут только возрастать. Противодействие таким угрозам должно осуществляться не только организационно-техническими, но и правовыми способами, среди которых выступает уголовно-правовая защита [Кобец, 2022]. В последнее время в отечественное уголовное законодательство внесен ряд статей, предусматривающих ответственность за распространение ложной информации, направленной против России – статьи 207.1, 207.2 УК РФ в 2020 г., статьи 207.3, 282.4, 284.2 УК РФ в 2022 г. Не уменьшается необходимость выявлять экстремистские проявления в киберпространстве как идеологическую подпитку терроризма и привлекать экстремистов к уголовной ответственности [Куликов, 2021; Бендзяк, 2022; Болвачев, 2022]. Также эффективным направлением борьбы с кибертерроризмом является подрыв источников его финансирования, в том числе связанных с оборотом криптовалюты [Лемайкина, 2020].

Заключение

Однако понятие кибертерроризма до сих пор не нашло легального определения и, соответственно, не предусматривается повышенной ответственности за подобные, бесспорно, общественно опасные деяния. В этом направлении первым шагом явилась криминализация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в 2017 г. и нарушений правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ) в 2022 г.

Библиография

1. Аман К.П., Истлеев А.Б., Ахметкалиев Н.Г. Кибертерроризм как новая форма терроризма // Информация и образование: границы коммуникаций. 2018. № 10 (18). С. 24-26.
2. Бендзяк С.П. Осуществление оперативно-розыскных мероприятий по выявлению организованных групп экстремистской направленности в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2022. № 1 (21). С. 18-25.
3. Богачев В.Я., Редин В.В. Информационная безопасность как составная часть национальной безопасности Российской Федерации // Стратегия гражданской защиты: проблемы и исследования. 2012. Т. 2. № 2 (3). С. 785-797.
4. Болвачев М.А. Особенности производства лингвистических судебных экспертиз по делам о преступлениях

- экстремистской направленности в социальных сетях // Криминалистика: вчера, сегодня, завтра. 2022. № 2 (22). С. 17-24.
5. Бочаров Ю. Киберпреступность и кибертерроризм. Новая глобальная угроза государственному строю. URL: <http://www.elections-ices.org/russian/publications/region:world/textid:12835/>
 6. Бочинин А.В. Тема терроризма на страницах качественной прессы США (на примере газет «Вашингтон Пост», «Вашингтон Таймс» и «Нью-Йорк Таймс» в период с 2010 по 2014 гг.): дис. ... канд. филол. наук. М., 2015. 296 с.
 7. Бураева Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма // Пробелы в российском законодательстве. 2017. № 3. С. 35-37.
 8. Васильев А.А., Демин К.Е. Электронные носители данных как источники получения криминалистически значимой информации. М., 2009. 198 с.
 9. Гейдаров Г.М.О. Правовые основы борьбы с киберпреступностью // Охрана, безопасность, связь. 2022. № 7-2. С. 123-127.
 10. Капитонова Е.А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2 (34). С. 29-41.
 11. Кобец П.Н. Совершенствование противодействия современным вызовам и угрозам в сфере информационной безопасности Российской Федерации, исходящих от международных террористических организаций // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2022. № 2 (101). С. 51-64.
 12. Куликов А.Г. К вопросу совершенствования оперативно-розыскной деятельности по противодействию экстремизму в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2021. № 2 (18). С. 64-71.
 13. Лемайкина С.В. Актуальные вопросы противодействия киберпреступлениям // Криминалистика: вчера, сегодня, завтра. 2020. № 4 (16). С. 54-59.
 14. Лукавский С. Некоторые аспекты кибертерроризма. URL: <https://www.geopolitica.ru/article/nekotorye-aspekty-kiberterrorizma/>
 15. Осодоева Н.В. К вопросу об установлении личности допрашиваемого лица при производстве допроса свидетелей посредством видео-конференц-связи в уголовном судопроизводстве // Криминалистика: вчера, сегодня, завтра. 2021. № 1 (17). С. 217-224.
 16. Родивилина В.А., Родивилин И.П., Коломинов В.В. Проблемы противодействия использованию анонимности в сети Интернет в преступных целях // Криминалистика: вчера, сегодня, завтра. 2021. № 4 (20). С. 68-76.
 17. Соколова О.А. Кибертерроризм: понятие и меры борьбы // Вестник молодых ученых и специалистов Самарского государственного университета. 2017. № 1 (10). С. 114-116.
 18. Хачатрян А.Г. Кибертерроризм в современном мире // Актуальные проблемы правового, социального и политического развития России. Саратов: Саратовский источник, 2018. С. 248-252.
 19. Яцкина И.А. Криминалистическая сущность преступлений, связанных с пропагандой экстремизма, и особенности проведения различных следственных действий в процессе их расследования // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 209-217.
 20. Короткова О.В. Особенности исследовательского подхода к вопросам обеспечения безопасности бизнеса в РФ // Человек. Социум. Общество. 2022. № 12. С. 139 – 142.
 21. Короткова О.В. Особенности обеспечения экономической безопасности предпринимательской деятельности в эпоху цифровых технологий // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 7 (71). С. 53 – 59.
 22. Короткова О.В. Особенности научного подхода в сфере обеспечения безопасности бизнеса // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2022. № 7. С. 20 – 23.
 23. Зудаева В.В., Фидель Е.С., Балдынова А.А. Современные подходы к определению понятия «киберпреступность» в мировом сообществе // International Law Journal. 2021. Т. 4. № 1. С. 74 – 79.

Cyberterrorism as a form of computer crime

Anna B. Kolosova

Investigator of the Main Investigative Department
of the Main Directorate of the Ministry of Internal Affairs
of the Russian Federation in the Irkutsk Region,
664003, 15, Litvinova str., Irkutsk, Russian Federation;
e-mail: 38@mvd.ru

Maksim V. Starichkov

PhD in Law, Associate Professor,
Associate Professor of the Department of Forensic Science,
East Siberian Institute of the Ministry of Internal Affairs
of the Russian Federation,
664074, 110, Lermontova str., Irkutsk, Russian Federation;
e-mail: 38@mvd.ru

Abstract

The global network «Internet» opens up a large number of opportunities, such as ease of access, independence from location, as well as high speed of information exchange and relative anonymity. These advantages are actively used by attackers to commit computer crimes, including cyberterrorism. The rapid development of information technology is accompanied by an increase in the commission of computer crimes. The most dangerous form of computer crime is cyberterrorism. The article discusses the concept, features and methods of committing cyberterrorism, as well as the direction of development of Russian criminal legislation aimed at counteracting cyber-attacks. The concept of cyberterrorism has not yet found a legal definition and, accordingly, there is no increased responsibility for such, no doubt, socially dangerous acts. In this direction, the first step was the criminalization of unlawful impact on the critical information infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation) in 2017 and violations of the rules for centralized management of technical means to counter threats to the stability, security and integrity of the functioning of the information and telecommunications network on the territory of the Russian Federation « Internet» and public communication networks (Article 274.2 of the Criminal Code of the Russian Federation) in 2022.

For citation

Kolosova A.B., Starichkov M.V. (2022) Kiberterrorizm kak forma komp'yuternoï prestupnosti [Cyberterrorism as a form of computer crime]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 12 (10A), pp. 556-562. DOI: 10.34670/AR.2022.44.88.065

Keywords

Cyberterrorism, computer crime, terrorist attack, computer crime, cyber-attack, responsibility, cyberspace.

References

1. Aman K.P., Istleev A.B., Akhmetkaliev N.G. (2018) Kiberterrorizm kak novaya forma terrorizma [Cyberterrorism as a new form of terrorism]. *Informatsiya i obrazovanie: granitsy kommunikatsii* [Information and education: boundaries of communications], 10 (18), pp. 24-26.
2. Bendzyak S.P. (2022) Osushchestvlenie operativno-rozysknykh meropriyatiï po vyyavleniyu organizovannykh grupp ekstremistskoi napravlenosti v seti Internet [Implementation of operational-search measures to identify organized groups of extremist orientation on the Internet]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 1 (21), pp. 18-25.
3. Bocharov Yu. *Kiberprestupnost' i kiberterrorizm. Novaya global'naya ugroza gosudarstvennomu stroyu* [Cybercrime and cyberterrorism. A new global threat to the state system]. Available at: <http://www.elections-ices.org/russian/publications/region:world/textid:12835/> [Accessed 12/12/2022]

4. Bochinin A.V. (2015) *Tema terrorizma na stranitsakh kachestvennoi pressy SShA (na primere gazet «Washington Post», «Washington Times» i «N'yu-York Times» v period s 2010 po 2014 gg.)*. Doct. Dis. [The theme of terrorism on the pages of the US quality press (on the example of the newspapers The Washington Post, The Washington Times and The New York Times in the period from 2010 to 2014)]. Doct. Dis.]. Moscow.
5. Bogachev V.Ya., Redin V.V. (2012) *Informatsionnaya bezopasnost' kak sostavnaya chast' natsional'noi bezopasnosti Rossiiskoi Federatsii* [Information security as an integral part of the national security of the Russian Federation]. *Strategiya grazhdanskoj zashchity: problemy i issledovaniya* [Civil Protection Strategy: Problems and Research], 2, 2 (3), pp. 785-797.
6. Bolvachev M.A. (2022) *Osobennosti proizvodstva lingvisticheskikh sudebnykh ekspertiz po delam o prestupleniyakh ekstremistskoi napravlenosti v sotsial'nykh setyakh* [Features of the production of linguistic forensic examinations in cases of extremist crimes in social networks]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 2 (22), pp. 17-24.
7. Buraeva L.A. (2017) *Kiberterrorizm kak novaya i naibolee opasnaya forma terrorizma* [Cyberterrorism as a new and most dangerous form of terrorism]. *Probely v rossiiskom zakonodatel'stve* [Gaps in Russian legislation], 3, pp. 35-37.
8. Geidarov G.M.O. (2022) *Pravovye osnovy bor'by s kiberprestupnost'yu* [Legal basis for combating cybercrime]. *Okhrana, bezopasnost', svyaz'* [Protection, security, communication], 7-2, pp. 123-127.
9. Kapitonova E.A. (2015) *Osobennosti kiberterrorizma kak novoi raznovidnosti terroristicheskogo akta* [Features of cyberterrorism as a new type of terrorist act]. *Izvestiya vysshikh uchebnykh zavedenii. Povolzhskii region. Obshchestvennyye nauki* [News of higher educational institutions. Volga region. Social Science], 2 (34), pp. 29-41.
10. Khachatryan A.G. (2018) *Kiberterrorizm v sovremennom mire* [Cyberterrorism in the modern world]. In: *Aktual'nye problemy pravovogo, sotsial'nogo i politicheskogo razvitiya Rossii* [Actual problems of legal, social and political development of Russia]. Saratov: Saratovskii istochnik Publ.
11. Kobets P.N. (2022) *Sovershenstvovanie protivodeistviya sovremennym vyzovam i ugrozam v sfere informatsionnoi bezopasnosti Rossiiskoi Federatsii, iskhodyashchikh ot mezhdunarodnykh terroristicheskikh organizatsii* [Improving the counteraction to modern challenges and threats in the field of information security of the Russian Federation emanating from international terrorist organizations]. *Vestnik Vostochno-Sibirskogo instituta Ministerstva vnutrennikh del Rossii* [Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia], 2 (101), pp. 51-64.
12. Kulikov A.G. (2021) *K voprosu sovershenstvovaniya operativno-rozysknoi deyatel'nosti po protivodeistviyu ekstremizmu v seti Internet* [On the issue of improving operational-search activities to counter extremism on the Internet]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 2 (18), pp. 64-71.
13. Lemaikina S.V. (2020) *Aktual'nye voprosy protivodeistviya kiberprestupleniyam* [Actual issues of combating cybercrime]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 4 (16), pp. 54-59.
14. Lukavskii S. *Nekotorye aspekty kiberterrorizma* [Some aspects of cyberterrorism]. Available at: <https://www.geopolitica.ru/article/nekotorye-aspekty-kiberterrorizma/> [Accessed 12/12/2022]
15. Osodoeva N.V. (2021) *K voprosu ob ustanovlenii lichnosti doprashivaemogo litsa pri proizvodstve doprosa svidetelei posredstvom video-konferents-svyazi v ugovnom sudoproizvodstve* [On the issue of establishing the identity of the interrogated person during the interrogation of witnesses through videoconferencing in criminal proceedings]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 1 (17), pp. 217-224.
16. Rodivilina V.A., Rodivilin I.P., Kolominov V.V. (2021) *Problemy protivodeistviya ispol'zovaniyu anonimnosti v seti Internet v prestupnykh tselyakh* [Problems of countering the use of anonymity on the Internet for criminal purposes]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 4 (20), pp. 68-76.
17. Sokolova O.A. (2017) *Kiberterrorizm: ponyatie i mery bor'by* [Cyberterrorism: concept and measures of struggle]. *Vestnik molodykh uchenykh i spetsialistov Samarskogo gosudarstvennogo universiteta* [Bulletin of young scientists and specialists of the Samara State University], 1 (10), pp. 114-116.
18. Vasil'ev A.A., Demin K.E. (2009) *Elektronnyye nositeli dannykh kak istochniki polucheniya kriminalisticheskoi informatsii* [Electronic data carriers as sources of obtaining forensically significant information]. Moscow.
19. Yatskina I.A. (2020) *Kriminalisticheskaya sushchnost' prestuplenii, svyazannykh s propagandoi ekstremizma, i osobennosti provedeniya razlichnykh sledstvennykh deistvii v protsesse ikh rassledovaniya* [Forensic Essence of Crimes Related to Propaganda of Extremism and Features of Conducting Various Investigative Actions in the Process of Their Investigation]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: yesterday, today, tomorrow], 2 (14), pp. 209-217.
20. Korotkova O.V. *Features of the research approach to the issues of business security in the Russian Federation* // *Man. Society. Society*. 2022. No. 12. pp. 139 – 142.
21. Korotkova O.V. *Features of ensuring economic security of entrepreneurial activity in the era of digital technologies* // *Bulletin of the O.E. Kutafin University (MSU)*. 2020. № 7 (71). Pp. 53-59.
22. Korotkova O.V. *Features of the scientific approach in the field of business security* // *Modern science: actual problems of theory and practice. Series: Economics and Law*. 2022. No. 7. pp. 20-23.
23. Zudaeva V.V., Fidel E.S., Baldynova A.A. *Modern approaches to the definition of the concept of "cybercrime" in the world community* // *International Law Journal*. 2021. Vol. 4. No. 1. pp. 74-79.