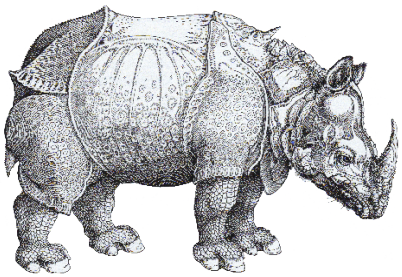
Non multa, sed multum



ИНДЕКС БЕЗОПАСНОСТИ №17 (43) I 2022

НАУЧНЫЕ ЗАПИСКИ

Леонид Цуканов

ВЗЛЕТЫ И ПАДЕНИЯ *КИБЕРХАЛИФАТА*: АЛЬ-КАИДА* И ИГИЛ* В ЦИФРОВОМ ПРОСТРАНСТВЕ

ПИРПРЕСС

МОСКВА, 2022

Главный редактор: В.А. Орлов

Редактор: Е.Г. Чобанян

Цуканов Леонид Вячеславович. Взлеты и падения *Киберхалифата*: Аль-Каида* и ИГИЛ* в цифровом пространстве / Ред. Е.Г. Чобанян. М.: ПИР-Пресс, 2022. – 39 с. – (*Индекс Безопасности* – Научные записки).

ISBN 978-5-6048679-2-1

Одной из ключевых угроз для безопасности России по-прежнему остается международный терроризм. Однако, по мере продолжающейся цифровизации мира, вместе с традиционными формами распространение получает кибертерроризм, который может нанести гораздо больший ущерб мировой архитектуре безопасности, чему во многом способствует быстрое развитие информационно-коммуникационных технологий. Цель данной научной записки – проанализировать деятельность Аль-Каида* и ИГИЛ*, как двух наиболее активных сторонников концепции *цифрового джихада*, в киберпространстве.

* Перечисленные в работе организации являются террористическими, их деятельность запрещена на территории РФ. В соответствии с положениями федерального закона N 35-ФЗ «о противодействии терроризму», данная научная записка не является пропагандистской, представленная в ней информация носит ознакомительный характер.

Данная научная записка и другие материалы научной серии размещены на сайте: http://pircenter.org/articles

Данная записка выпущена в рамках *Евстафьевской серии* (см. стр. 39).

ISBN 978-5-6048679-2-1
9 785604 867921

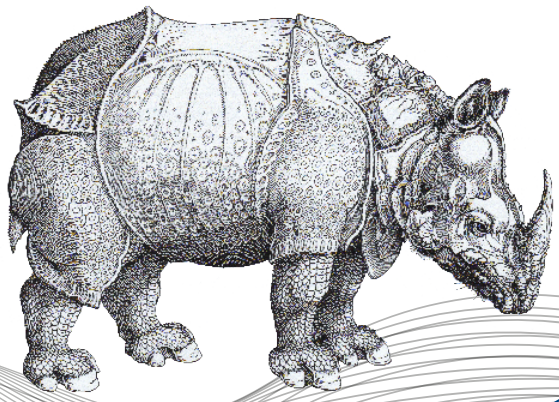
Автор

ЦУКАНОВ Леонид Вячеславович

Эксперт РСМД, постоянный автор ПИР-Центра. Колумнист журнала *Эксперт*. Номинант Международной премии Насера Бин Хамада аль-Халифы в сфере молодежного творчества по треку *наука* (Бахрейн, 2021 г.), участник II российско-египетского форума по вопросам сотрудничества в области искусственного интеллекта и кибербезопасности (Египет, 2021 г.). Выпускник XX Международной школы ПИР-Центра по проблемам глобальной безопасности (2020). Прошел курсы повышения квалификации по проблемам региональной безопасности на Ближнем Востоке (Tel-Aviv University) и кибербезопасности (УрФУ им. Б.Н. Ельцина, Arab Academy for Science, Technology & Maritime Transport), а также по вопросам исследования проблем терроризма (Universiteit Leiden, Allameh Tabataba'i University). Владеет русским, английским, китайским, арабским и персидским языками, а также ивритом.

Экспертиза: современные вызовы и угрозы международной безопасности, вопросы безопасности на Ближнем Востоке, кибербезопасность (с углубленной специализацией на киберсистемах государств Ближнего Востока), противодействие терроризму.

Эл.почта: leon.tsukanov@mail.ru



Оглавление

Главное

- Теоретическое осмысление феномена кибертерроризма продолжается по сей день и пополняется дополнительными вводными и категориями – в первую очередь, из-за освоения джихадистами новых аспектов деятельности в цифровом пространстве.

- Выработанным пропагандистским клише о допустимости *цифрового джихада* достаточно трудно противодействовать, поскольку они формулируются с опорой на труды *отверженных* проповедников или с заведомым искажением сути первоисточника. За счет этого достигается высокая гибкость и живучесть продвигаемых радикалами концептов.

- И Аль-Каида*, и ИГИЛ* прошли схожий путь в развитии цифровой составляющей своей деятельности, однако лидеры ИГИЛ* подошли к вопросу более системно, ввиду чего концепция *цифрового джихада* стала прочно ассоциироваться именно с этой группировкой. С другой стороны, несмотря на завоеванное преимущество, ИГИЛ* довольно быстро утратило лидирующие позиции ввиду системных проблем, что обусловило комплексную стагнацию их киберсистемы.

- К началу пандемии COVID-19 обе группировки минимизировали наступательную цифровую деятельность. Вместо этого на передний план вышла пропагандистская составляющая деятельности. Идея же создания *цифровых отрядов* в пандемию осталась в категории долгосрочных планов из-за нехватки ресурсов.

- Все наиболее вероятные варианты развития событий имеют точку соприкосновения: первое время джихадисты не будут предпринимать масштабных наступательных действий в киберпространстве, *прощупывая* возможности вероятного противника.

Взлеты и падения *Киберхалифата*: Аль-Каида* и ИГИЛ* в цифровом пространстве

Леонид Цуканов

ВВЕДЕНИЕ

В соответствии с положениями Стратегии национальной безопасности РФ 2021 г., одной из приоритетных задач государства остается обеспечение надлежащего уровня защиты от внутренних и внешних угроз, а также поддержание коллективных усилий в области реагирования на вызовы безопасности[1]. При этом одной из ключевых угроз, с точки зрения России, по-прежнему остается международный терроризм. Однако, по мере продолжающейся цифровизации мира, вместе с традиционными формами распространение получает кибертерроризм, который может нанести гораздо больший ущерб мировой архитектуре безопасности, чему во многом способствует быстрое развитие информационно-коммуникационных технологий. Учитывая, что РФ напрямую вовлечена в борьбу с исламистской угрозой (включая ее проявления в цифровом пространстве), данная тема представляет интерес как с академической, так и с практической точки зрения. Кроме того, дополнительное внимание к теме привлекает резкая активизация усилий радикалов от ислама по вербовке хакеров на фоне череды острых региональных кризисов, что требует от мирового сообщества дополнительной оценки грядущих рисков.

Подробный расклад актуализирует ряд вопросов. Как менялся подход к трактовке понятий *кибертерроризм* и *цифровой джихад* с течением времени? Каким образом Аль-Каида* и ИГИЛ* (как два наиболее активных сторонника концепции *цифрового джихада*) обосновывают деятельность в киберпространстве с точки зрения религиозных норм? Каковы перспективы перехода радикалов от ислама к наступательным действиям в киберпространстве с учетом накопленного ими опыта?

Рассматриваемая проблематика представлена в современном научном поле внушительным количеством исследований и характеризуется высокой степенью дискуссионности ввиду

[1] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Президент России. 02.07.2021. URL: http://www.kremlin.ru/acts/bank/47046/page/1 (дата обращения: 12.06.2022).

разнообразия методологических подходов. Вместе с тем российские и зарубежные эксперты сходятся во мнении, что кибертерроризм перешел в группу первоочередных угроз и требует комплексного осмысления. Как правило, на передний план выдвигаются вопросы, связанные со спецификой трактовки понятия[2], обзором усилий радикалов от ислама в области развития киберпотенциала[3], разработкой механизмов противодействия проблеме на глобальном и региональном уровнях[4], а также оценкой влияния цифрового фактора на развитие систем безопасности[5]. Кроме того, поскольку джихадисты выстраивают свою пропаганду с опорой на элементы исламской идентичности, тема традиционно получает освещение в трудах и выступлениях авторитетных отечественных[6] и зарубежных[7] исламоведов.

С другой стороны, большинство работ, посвященных исследованию феномена *цифрового джихада* и его места в деятельности международных террористических группировок, сводятся, в первую очередь, к анализу отдельных акций или инициатив радикалов от ислама в киберпространстве. Более того, практически отсутствуют работы, посвященные специфике функционирования глобального исламистского подполья в условиях пандемии COVID-19 (а имеющиеся уделяют недостаточное внимание цифровому фактору деятельности). Данное исследование позволяет в определенной степени устранить имеющийся пробел.

Источниковой основой исследования стали отчеты международных организаций, ведущих экспертных центров, специализирующихся на вопросах кибербезопасности и международной безопасности как таковой; выдержки из свя-

Кибертерроризм перешел в группу первоочередных угроз и требует комплексного осмысления

[2] Weimann G. Lone Wolves in Cyberspace // Journal of Terrorism Research. 22.09.2012. URL: https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.405/ (accessed: 16.05.2022).
[3] Combating Cyber-Jihad // RUSI. 20.09.2006. URL: https://rusi.org/publication/combating-cyber-jihad (accessed: 10.05.2022); Liang C. Understanding and Countering Islamic State Propaganda // GCSP. 01.02.2015. URL https://www.gcsp.ch/publications/cyber-jihad (accessed: 12.05.2022); Mamaev A. Cyber Caliphate: What Apps Are the Islamic State Using? // RIAC. 25.05.2018. URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/cyber-caliphate-what-apps-are-the-islamic-state-using/ (accessed: 12.05.2022).
[4] Smith T. The Specter of Cyber in the Service of the Islamic State // American Intelligence Journal – 2017. – №1. – P. 54-58.
[5] Hoffman A., Schweitzer Y. Cyber Jihad in the Service of the Islamic State (ISIS) // INSS. 18.04.2015. URL: https://inss.org.il/wp-content/uploads/systemfiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf (accessed: 13.05.2022).
[6] См., напр.: Силантьев Р.А. Современное технологии на службе у террористов и контртеррористов // Материалы Всероссийской научно-практической конференции (с международным участием) VII «Расулевские чтения: ислам в истории и современной жизни России». Под ред. И.И. Аносова. – 2018 – С. 146–155; Sykianen L.R. The Islamic Concept of Caliphate: basic principles and a contemporary interpretation – Islamology – 2017. – №1. – P.61–70; Сюкияйнен Л.Р. Современная исламская правовая мысль о Халифате и гражданском государстве с исламской ориентацией – Северо-Кавказский юридический вестник. – 2016. – №2. – С. 7–19; Яхьяев М. Я., Яхьяев А. М. Феномен джихада в исламе //Исламоведение. – 2020. – Т. 11. – №. 4 (46). – С. 81–94 и др.
[7] См., напр.: حديث الذكريات مع الإمام محمد سعيد رمضان البوطي (Воспоминания о беседах с имамом Мухаммадом Саидом Рамаданом Аль-Бути) // Imam Al-Bouti Martyr (YouTube). 30.10.2017. URL: https://www.youtube.com/watch?v=hPp65f3Xaz8 (accessed: 19.05.2022).

щенных текстов (Коран); фетвы и выступления мусульманских богословов; материалы информационно-новостных ресурсов. Были применены такие методы как системный анализ, ивент-анализ, моделирование и прогнозирование.

КИБЕРТЕРРОРИЗМ: ОСМЫСЛЕНИЕ УГРОЗЫ

Следует начать с того, что понятие *кибертерроризм* (из которого в дальнейшем был выведен более узкий термин *цифровой джихад*), введенное в научный дискурс дискурс в конце 1980-х – начале 1990-х гг., долгое время являлось теоретическим. Термин переосмысливал понятие *терроризм*, до этого использовавшееся в документах Государственного департамента США (*Преднамеренная, политически мотивированная атака, приведшая к насилию против некомбатантов со стороны субнациональных группировок или подпольно действующих агентов*), с большим акцентом на цифровую составляющую террористической деятельности[8]. При этом цифровая инфраструктура рассматривалась одновременно и как цель, и как средство атаки.

Активизации радикалов от ислама в цифровом пространстве поспособствовало начало *гонки кибервооружений* на Ближнем Востоке

Однако вплоть до второй половины 2000-х гг. эксперты не позиционировали кибертерроризм как отдельную угрозу, считая его лишь агрессивной формой киберпреступности и включая в понятие не только деятельность террористических группировок, но и *хактивизм* (например, акции палестинских хакеров)[9]. Кроме того, сами радикалы от ислама не вели централизованной деятельности в киберпространстве, ограничиваясь фишингом и кражей денежных средств (т. н. *E-Jihad*)[10]. По этой причине многие авторитетные специалисты по проблемам терроризма (например, Л. Ричардсон) выступали против использования нового термина[11].

Активизации радикалов от ислама в цифровом пространстве поспособствовало начало *гонки кибервооружений* на Ближнем Востоке. Атака вируса Stuxnet[12] на программное обеспечение

[8] Hoffman A., Schweitzer Y. Cyber Jihad in the Service of the Islamic State (ISIS) // INSS. 18.04.2015. URL: https://inss.org.il/wp-content/uploads/systemfiles/adkan18_1ENG%20(5)_Hoffman-Schweitzer.pdf (accessed: 13.05.2022).

[9] См., напр.: Stohl M. Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? // Crime, law and social change. – 2006. – №. 4. – pp. 225, 227, 233; Combating Cyber-Jihad // RUSI. 20.09.2006. URL: https://rusi.org/publication/combating-cyber-jihad (accessed: 10.05.2022)

[10] Teasuro L. The Role Al Qaeda Plays in Cyberterrorism // Small Wars Journal. 08.12.2018. URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (accessed: 19.05.2022).

[11] См., напр.: Richardson L.: Illusions of Terrorism // Carnegie Council for Ethics in International Affairs (YouTube). 27.10.2011. URL: https://www.youtube.com/watch?v=EBBJN2r7pt4 (accessed: 17.05.2022).

[12] Stuxnet – универсальный автономный инструмент промышленного шпионажа, предназначенный для получения доступа к операционной системе, отвечающей за обработку, сбор данных и оперативное диспетчерское управление промышленными объектами. В отличие от большинства аналогичных вирусов, основным применением Stuxnet может стать не хищение данных, а повреждение промышленных автоматизированных систем. См.: Stuxnet 'hit' Iran nuclear plans

промышленных объектов Ирана (2010 г.)[13] продемонстрировала кумулятивный эффект (в первую очередь, психологический[14]), который можно достичь с использованием цифровых технологий, что отразилось на приоритетах джихадистских организаций – в частности, о намерении развивать собственный киберпотенциал объявила Аль-Каида*[15]. В этот же период в экспертных работах впервые появился термин *цифровой джихад* (*противозаконные атаки или угрозы атак на компьютеры, сети и хранимую в них информацию для устрашения или принуждения правительства или граждан к какому-либо действию в политических или общественных целях*)[16], что привело к возобновлению академических дискуссий. Тем не менее, большинство экспертов по-прежнему настаивали, что шансы джихадистов нанести серьезный урон в киберпространстве остаются ничтожными – ввиду слабого понимания специфики кибермира[17].

Тем не менее цифровая угроза со стороны радикалов от ислама с течением времени неуклонно росла. Джихадисты использовали все более сложные программы (включая службы обмена зашифрованными сообщениями) и инструменты, а также усиливали влияние на международное хакерское сообщество (что наиболее полно проявилось в 2014–2017 гг.), ввиду чего игнорировать растущие возможности международных террористических группировок в киберпространстве уже не представлялось возможным. Это, в свою очередь, обусловило новый всплеск интереса к теме со стороны экспертного сообщества – так, помимо уже традиционных сюжетов, широкое освещение в научных работах получили феномен использования радикалами от ислама социальных сетей и мессенджеров для оперативной координации атак и их последующего освещения (*Джихад* 2.0 или *Медиаджихад*[18]),

Боевики террористической организации *ИГИЛ**

Источник: www.ria.ru

// BBC. 22.11.2010. URL: https://www.bbc.com/news/technology-11809827 (accessed: 14.05.2022).

[13] Stuxnet 'hit' Iran nuclear plans // BBC. 22.11.2010. URL: https://www.bbc.com/news/technology-11809827 (accessed: 14.05.2022).

[14] Например, эксперты сравнивали психологический эффект от использования Stuxnet с первыми взрывами атомных бомб. См.: Benedict K. Stuxnet and the Bomb // The Bulletin of the Atomic Scientists. 15.06.2012. URL: http://thebulletin.org/webedition/columnists/kennette-benedict/stuxnet-and-the-bomb (accessed: 15.05.2022).

[15] Teasuro L. The Role Al Qaeda Plays in Cyberterrorism // Small Wars Journal. 08.12.2018. URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (accessed: 19.05.2022).

[16] Также в некоторых работах – «киберджихад»; здесь и далее по тексту термины будут иметь идентичное значение. См.: Weimann G. Lone Wolves in Cyberspace // Journal of Terrorism Research. 22.09.2012. URL: https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.405/ (accessed: 16.05.2022).

[17] Al-Qaeda lacks expertise for cyberwar, expert tells MPs // BBC. 14.03.2013. URL: https://www.bbc.com/news/uk-politics-21769078 (accessed: 15.05.2022).

[18] См., напр.: Social Media Jihad 2 0: Inside ISIS' Global Recruitment and Incitement

а также оценки перспектив более широкого использования инструментов разведки по открытым источникам (OSINT)[19].

Как результат, к началу 2020-х гг. тема кибертерроризма не только не утратила актуальности, но и продолжает дополняться новыми вводными за счет дифференциации деятельности радикалов от ислама и освоения последними смежных измерений цифрового пространства.

ДЖИХАД И КИБЕРПРОСТРАНСТВО: ВЗГЛЯД РАДИКАЛОВ ОТ ИСЛАМА

Исследуя эволюцию подходов двух группировок к ведению борьбы в киберпространстве, необходимо сказать о специфике обоснования радикалами от ислама подобной деятельности – тем более, что модели пропаганды обеих группировок в данном случае имеют множество точек пересечения.

Первое, на что необходимо обратить внимание – кажущийся обширным духовный базис. По оценкам экспертов, проповеди и *фетвы*[20] джихадистов содержат ссылки на работы более чем сотни религиозных деятелей разных эпох. Подобный подход призван подчеркнуть приверженность группировки идеологии *истинного ислама* в трактовке раннего периода мусульманства, а также сгладить в пропаганде негативные черты политически ориентированного такфиризма[21]. При этом в вопросах оценки действий в цифровом мире радикалы от ислама предпочитают апеллировать к трудам современников (поскольку это облегчает проведение прямых параллелей) – Халида аль-Рашида, Насира аль-Фахда, Сулеймана бин Насир аль-Ульвана, Хамуда бин Укла аль-Шуайби, Омара бин Ахмед аль-Хазими и Али бин Хидр аль-Худиара. Также встречаются ссылки на работы идеологов Аль-Каиды* – Абу Мухаммада аль-Макдиси и Абдула Кадира бин Абдул Азиза[22].

Campaign // The Atlantic Council (Official YouTube Channel). 27.03.2017. URL: https://www.youtube.com/watch?v=CNg6mLkXcYM (accessed: 10.05.2022).

[19] См., напр.: Charania. S. Social Media's Potential in Intelligence Collection // American Intelligence Journal – 2016 – №33(2) – P. 94–100; Pastor-Galindo J. et al. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends // IEEE Access. – 2020. – Т8. – №1. – pp. 20,22.

[20] В случае с обозначенными джихадистскими группировками слово «фетва» намеренно взято в кавычки, поскольку, по мнению большинства исламоведов, радикалы не имеют права на издание подобных документов. См., напр.: ذكريات مع الإمام محمد سعيد رمضان البوطي (Воспоминания о беседах с имамом Мухаммадом Саидом Рамаданом Аль-Бути) // Imam Al-Bouti Martyr (YouTube). 30.10.2017. URL: https://www.youtube.com/watch?v=hPp65f3Xaz8 (accessed: 19.05.2022).

[21] Силантьев Р.А. Современное технологии на службе у террористов и контртеррористов // Материалы Всероссийской научно-практической конференции (с международным участием) VII «Расулевские чтения: ислам в истории и современной жизни России». Под ред. И.И. Аносова. – 2018 – сс. 148–149.

[22] Справедливо для обеих группировок. Несмотря на то, что после разрыва между ИГИЛ* и Аль-Каидой* в 2014 г., труды аль-Макдиси и бин Абдул Азиза стали гораздо реже упоминаться в проповедях ИГИЛ*, отрывки из них долгое время публиковались в журналах «Дабик» и «Румийя», издаваемых группировкой. См.: Хассан Х. «Исламское государство»*: идеологические корни и политический контекст межконфессиональной вражды // Центр Карнеги. 27.12.2016. URL: https://

Кроме того, довольно часто в работах радикалов можно встретить апеллирование к принципу *аль-дарурат тубих аль-махзурат* (*запретное превращается в дозволенное при острой необходимости*). Так, использование средств и методов ведения войны в цифровом пространстве (в т.ч. нанесение массированного кибердудара) при наличии у *отступников*[23] аналогичных технологий не только не порицается, но и рассматривается как мера, продиктованная обстоятельствами. Для подкрепления этой идеи радикальные пропагандисты довольно часто используют примеры из исламской истории – предания о Сафийи Бинт Абдель Мутталиб и Халиде ибн аль-Валиде[24].

Большое значение имеет принцип сюжетных параллелей. Например, говоря о киберпространстве, радикалы от ислама приводят сюжет о противостоянии с племенем Бану Надир (Коран 59:2)[25] – как пример эффективности тактики выжженной земли (в широком смысле – удара с повышенным психологическим эффектом): среди прочего, сюжет используется для замещения менее растиражированных в исламском мире конструктов *Цифровая Хиросима* и *Цифровой Перл-Харбор*. Дополнительно следует указать, что образ противостояния с Бану Надир является довольно популярным среди джихадистских проповедников и ранее использовался, например, для обоснования допустимости разработки и использования оружия массового уничтожения (ОМУ). Также довольно часто можно встретить ссылки на *Аят меча* (Коран 9:5)[26], который приводится для обоснования дозволенности цифровых атак на критическую инфраструктуру. Несмотря на то, что перечисленные выше сюжеты не принято рассматривать в отрыве от исторического контекста (на что неоднократно указывали авторитетные исламоведы[27]), джихадисты намеренно идут на допущение и используют их для повышения эффективности вербовочной и антиправительственной деятельности.

Кроме того, радикалы от ислама стремятся обратить в свою пользу неточности, имеющиеся в авторитетных источниках.

Радикалы от ислама стремятся обратить в свою пользу неточности, имеющиеся в авторитетных источниках

carnegie.ru/2016/12/27/ru-pub-66552 (дата обращения: 19.05.2022).

[23] В зависимости от ситуации, под «отступниками» могли пониматься как немусульмане в целом, так и отдельные государства (в т.ч. мусульманские), в отношении которых выдвигается обвинение в неверии (такфир). См.: Liang C. Understanding and Countering Islamic State Propaganda // GCSP. 01.02.2015. URL https://www.gcsp.ch/publications/cyber-jihad (accessed: 12.05.2022).

[24] Sykianen L.R. The Islamic Concept of Caliphate: basic principles and a contemporary interpretation – Islamology – 2017. – №1. – pp. 65, 68, 69.

[25] Аль-Хашр (Сбор), 2-й аят из 24 // Коран онлайн. URL: https://quran-online.ru/59:2 (дата обращения: 19.05.2022).

[26] Особый акцент делается, в частности, на пассаж «[...] убивайте многобожников, где бы вы их ни обнаружили, берите их в плен, осаждайте их и устраивайте для них любую засаду». См.: Ат-Тауба (Покаяние), 5-й аят из 129 // Коран онлайн. URL: https://quran-online.ru/9:5 (дата обращения: 19.05.2022).

[27] См., напр.: Сюкияйнен Л.Р. Современная исламская правовая мысль о Халифате и гражданском государстве с исламской ориентацией – Северо-Кавказский юридический вестник. – 2016. – №2. – С. 11.

Ярким примером служат спекуляции вокруг положений Энциклопедии исламской юриспруденции, считающейся одним из наиболее авторитетных источников исламского права. В частности, проповедники ИГИЛ* указывают, что в Энциклопедии термин *джихад* тождественен понятию *война с неверными* (т.е. *джихад меча*[28]), ввиду чего иные формы борьбы (включая *джихад языка*[29] и *джихад познания*[30]) являются малоэффективными[31]. Подобное видение проецируется и на киберпространство, что лишь способствует продвижению концепции киберджихада в массы. Разумеется, представители авторитетных духовных центров исламского мира ведут борьбу с пропагандой джихадистов и на регулярной основе издают фетвы с критикой деятельности глобального исламистского подполья[32], однако террористам, тем не менее, удается купировать это влияние: в первую очередь, за счет постоянного обновления собственных пропагандистских материалов – в т.ч. обосновывающих избранную агрессивную модель поведения в киберпространстве. В результате борьба с пропагандой радикалов неизбежно приобретает реактивный характер.

Боевики ИГИЛ* в Алеппо, Сирия, 2014 г.

Источник: www.rbc.ru

[28] «Джихад меча» (газават) – священная война, вооруженная борьба с неверными. См.: Яхьяев М. Я., Яхьяев А. М. Феномен джихада в исламе //Исламоведение. – 2020. – Т. 11. – №. 4 (46). – С. 83.

[29] «Джихад языка» – призыв к другим совершенствоваться, становиться лучше, то есть обращение к другим людям с «повелением одобряемого и запрещением порицаемого». См.: Яхьяев М. Я., Яхьяев А. М. Феномен джихада в исламе //Исламоведение. – 2020. – Т. 11. – №. 4 (46). – С. 84.

[30] «Джихад познания» – борьба посредством распространения истинных знаний об исламе. См.: Яхьяев М. Я., Яхьяев А. М. Феномен джихада в исламе //Исламоведение. – 2020. – Т. 11. – №. 4 (46). – С. 84.

[31] Сюкияйнен Л.Р. Современная исламская правовая мысль о Халифате и гражданском государстве с исламской ориентацией – Северо-Кавказский юридический вестник. – 2016. – №2. – С. 14.

[32] См., напр.: لماذا رفك الزال رمز داع؟ (Почему Аль-Азхар не поддержал ИГИЛ*?) // Al-Araby Al-Jadeed. 24.04.2019. URL: https://www.alaraby.co.uk/لماذا-رفك-الزال-رمز-داع؟ (accessed: 18.05.2022).

АЛЬ-КАИДА* И ИГИЛ*: АДАПТАЦИЯ К ЦИФРОВОМУ МИРУ

Несмотря на то, что модели обоснования деятельности в киберпространстве у Аль-Каиды* и ИГИЛ*, в целом, совпадают, на практике цифровые начинания двух группировок реализовывалась по различным схемам. Рассмотрим в деталях каждую из них.

Аль-Каида*

Данная группировка, созданная в 1988 г., сегодня является одной из наиболее известных и непримиримых международных террористических организаций[33], а также первой радикальной группировкой, которая высоко оценила значение киберфактора. Ее адаптация к цифровым реалиям началась едва ли не одновременно с расширением Всемирной паутины во второй половине 1990-х гг. При этом основной акцент делался на пропагандистскую и вербовочную работу, в то время как проведение *ударных* акций (кибератаки) было определено как приоритет более низкого порядка[34]. Исключение было сделано для фишинговых акций, которые, среди прочего, служили дополнительным источником доходов группировки в начале 2000-х гг.[35].

Основатель Аль-Каиды* Усама бен Ладен в 1998 г.

Источник: www.lenta.ru

Важность работы с цифровым измерением неоднократно подчеркивали и лидеры Аль-Каиды*. Так, например, основатель группировки Усама бен Ладен писал, что широкомасштабное распространение джихадистской идеологии посредством Интернета, а также привлечение на радикальные веб-ресурсы значительного количества молодых людей, является одним из важных шагов на пути мирового джихада[36]. Впоследствии эту идею транслировал и его преемник, Айман аз-Завахири[37]. Не удивительно, что одним из ключевых инструментов

[33] Официально признана в США террористической только в 1998 г., после взрывов посольств США в столицах Кении и Танзании. В России признана террористической организацией в 2003 г. См.: East African Embassy Bombings // FBI. 07.08.1998. URL: https://www.fbi.gov/history/famous-cases/east-african-embassy-bombings (accessed: 06.06.2022); Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством РФ террористическими // ФСБ России. 22.04.2022. URL: http://fsb.ru/fsb/npd/terror.htm (дата обращения: 07.06.2022).

[34] Teasuro L. The Role Al Qaeda Plays in Cyberterrorism // Small Wars Journal. 08.12.2018. URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (accessed: 19.05.2022).

[35] Ibidem.

[36] Jihadist use of social media: how to prevent terrorism and preserve innovation // The United States Government Publishing Office. 06.12.2011. URL: https://www.govinfo.gov/content/pkg/CHRG-112hhrg74647/html/CHRG-112hhrg74647.htm (accessed: 13.06.2022).

[37] Online Jihadist Propaganda - 2021 in review // Europol. 24.05.2022. URL: https://www.europol.europa.eu/publications-events/publications/online-jihadist-propaganda-2021-in-review (accessed: 12.06.2022).

Аль-Каида* стала первой террористической группировкой, которая попыталась наладить контакты с международным хакерским сообществом и привлечь компьютерных специалистов для распространения радикальных идей

достижения, поставленных высшим руководством группировки целей стало созданное в 2001 г. медиакрыло *Ас-Сахаб*[38], специализировавшееся на производстве аудио и видеоконтента для джихадистов[39].

Также Аль-Каида* стала первой террористической группировкой, которая попыталась наладить контакты с международным хакерским сообществом и привлечь компьютерных специалистов для распространения радикальных идей. Первые подтвержденные совместные акции относятся к 2006 г. (хотя некоторые эксперты склонны отсчитывать историю кибероперaций Аль-Каиды* с 2001 г.[40]), когда радикалами, причисляющими себя к *цифровым солдатам Аль-Каиды**, была нарушена работа пяти сайтов с антиисламистским контентом[41]. Годом позже джихадисты попытались расширить плацдарм *цифрового наступления* и реализовать масштабную DDoS-атаку в отношении ряда западных веб-порталов, однако, ввиду низкой скоординированности действий, атака была сравнительно легко остановлена, и вплоть до 2011 г. радикалы от ислама практически никак не проявляли себя в цифровом поле[42].

Начало *гонки кибервооружений* на Ближнем Востоке, о которой говорилось ранее, подстегнуло джихадистов к наращиванию активности в цифровом пространстве. Уже через несколько недель после заявления об обнаружении вируса Duqu[43] на форуме *Шумух аль-Ислам* (крупнейший исламистский форум и главная пропагандистская площадка Аль-Каиды*) были размещены призывы создать хакерский коллектив, который бы сосредоточился на поиске уязвимости в системах диспетчерского управления и сбора данных (SCADA) – аналогичных тем, что составляют основы управления

[38] Ас-Сахаб – официальное медиакрыло Аль-Каиды*, отвечающее за создание пропагандистских материалов, включая проповеди, воззвания и документальные фильмы. В 2008 г. включено в состав «компьютерного департамента» Комитета по медиа группировки. См.: Exploiting Disorder: al-Qaeda and the Islamic State // International Crisis Group. 14.03.2016. URL: https://www.crisisgroup.org/global/exploiting-disorder-al-qaeda-and-islamic-state (accessed: 10.06.2022).

[39] Ibidem.

[40] Речь об атаке на веб-сервисы Национального управления океанических и атмосферных исследований США (NOAA) в октябре 2001 г., которую приписывают себе члены хакерской группировки «Al-Qaeda Alliance Online» (AAO). Причастность AAO к инциденту опровергается правоохранительными органами США. См.: Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program // National Oceanic and Atmospheric Administration. 26.08.2016. URL: https://www.oig.doc.gov/OIGPublications/OIG-16-043-A.pdf (accessed: 10.06.2022).

[41] Серии атак подверглись, в частности, сайты Ватикана и газеты «Jyllands-Posten». См.: Rollins J., Wilson C. Terrorist Capabilities for Cyberattack: Overview and Policy Issues // Congressional Research Service. 22.01.2007. URL: https://sgp.fas.org/crs/terror/RL33123.pdf (accessed: 10.06.2022).

[42] За исключением угроз нанести «сокрушительный удар в киберпространстве» (таких заявлений Аль-Каида*, в среднем, делала до полутора десятков ежегодно), за которыми, как правило, не следовали реальные действия. См.: Teasuro L. The Role Al Qaeda Plays in Cyberterrorism // Small Wars Journal. 08.12.2018. URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (accessed: 19.05.2022).

[43] Duqu (также ~DQ) – троянская программа, используемая для целенаправленных атак на крупные компании и промышленные предприятия. Считается продолжением сетевого червя Stuxnet. См.: Целевые атаки типа Duqu 2.0 // Лаборатория Касперского. 10.06.2015. URL: https://www.kaspersky.ru/resource-center/threats/duqu-2 (дата обращения: 10.06.2022).

критической инфраструктуры США, Франции и Великобритании[44]. Помимо этого, радикалы от ислама в разное время рассматривали другие варианты цифровых акций: удаленный захват американских БПЛА, *смертельные удары*[45] по цифровой инфраструктуре западных электростанций и НПЗ, диверсии на АЭС и т.д.[46] Однако, как показали дальнейшие события, ни одна из анонсированных акций не была реализована на практике.

Новая попытка Аль-Каиды* усилить свои позиции в киберпространстве, создать некое подобие *цифрового исламистского фронта*, пришлась уже на вторую половину 2010-х гг. – и, по сути, являлась реакцией на агрессивную пропагандистскую кампанию ИГИЛ*[47]. Так, в январе 2015 г. на ресурсах Аль-Каиды* появились сообщения о создании *цифрового батальона* группировки, к которому «присоединились наиболее мотивированные и непримиримые хакеры»[48]. Новое подразделение возглавил Яхья аль-Немр, ранее входивший в ближайшее окружение Аймана аз-Завахири. И, хотя к серьезным преобразованиям организационной структуры группировки это не привело (*цифровой батальон* не был включен ни в одну из ветвей управления и существовал, фактически, независимо), связи между Аль-Каидой* и хакерским сообществом укрепились, в результате чего возникла небольшая *прослойка* лояльных джихадистам специалистов. Можно выделить три хакерские группировки, которые чаще всего взаимодействовали с аль-Немром и его структурой. Это *Al-Qaeda Alliance Online* (порча веб-сайтов, кибератаки), *Youni Tsoulis* (создание джихадистских веб-форумов, разработка учебных пособий по киберджихаду) и *Al-Qaeda Electronic* (доксинг, DDoS-атаки), суммарное число подтвержденных акций трех группировок, проведенных от имени Аль-Каиды*, превышает пять десятков случаев[49].

[44] Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad' // ABC News. 23.05.2012. URL: https://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875 (accessed: 20.05.2022).

[45] Подразумеваются те виды кибератак, которые могут нанести глубокий урон компьютерной технике и вывести ее из строя, – например, нарушив работу микросхем BIOS на материнской плате, как в случае с вирусом Win95/CIH («Чернобыль»). См.: VIRUS.WIN9X.CIH // Kaspersky Threats. 20.11.2002. URL: https://threats.kaspersky.com/ru/threat/Virus.Win9x.CIH/ (accessed: 29.05.2022).

[46] Chen T. Cyberterrorism after Stuxnet // Strategic Studies Institute, US Army War College. – 2014 – pp. 17, 20, 22, 31, 35.

[47] Пропагандисты ИГИЛ*, среди прочего, критиковали членов и руководителей Аль-Каиды* за «преступное бездействие» и недостаточное использование наступательных средств для борьбы за провозглашенные идеалы. См.: Anderson G., Bronk C. Encounter Battle: Engaging ISIL in Cyberspace // The Cyber Defense Review. – 2017. – Vol.2, №1 – P. 95.

[48] Cyber-Terrorism Activities Report №16 // International Institute for Counter-Terrorism. 20.03.2016. URL: https://www.ict.org.il/UserFiles/ICT-Cyber-Review-16.pdf (accessed: 12.06.2022).

[49] Ejazi F. Performance of Virtual Terrorism in Cyber Space //Media and Terrorism in the 21st Century. – IGI Global, 2022. – pp. 227–229, 231, 233.

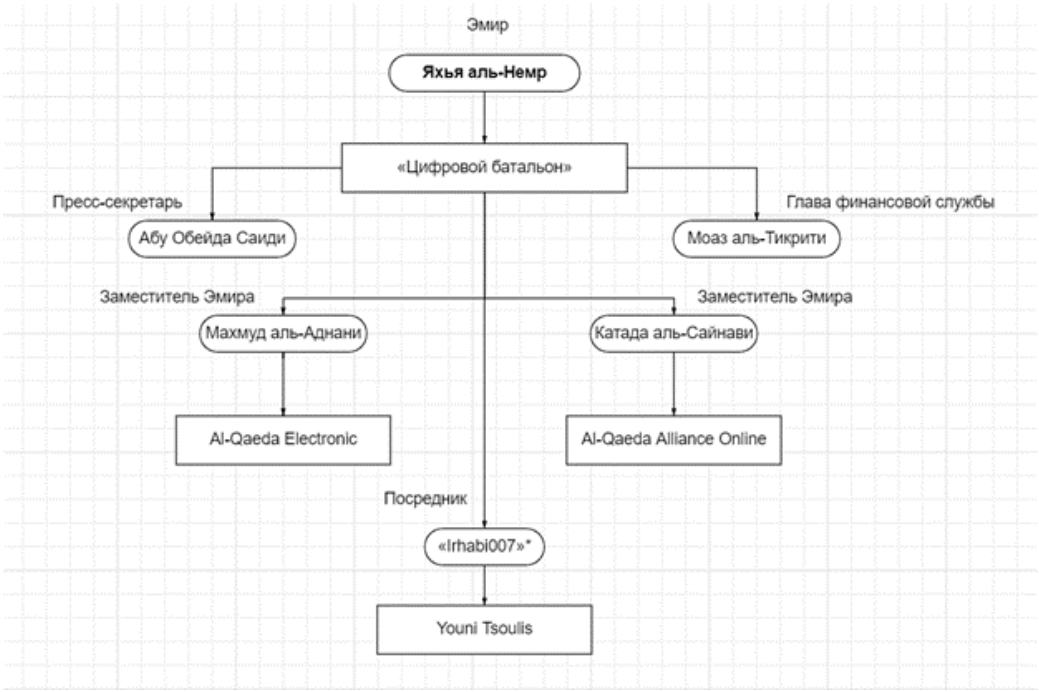


Схема *Цифрового батальона* Аль-Каиды* на момент его учреждения (первая половина 2015 г.), с указанием аффилированных группировок

Источник: Teasuro L. The Role Al Qaeda Plays in Cyberterrorism

Впрочем, считать структуру аль-Немра полноценной боевой единицей, ориентированной на ведение джихада в киберпространстве, не стоит – в первую очередь, ввиду специфики восприятия хакерской деятельности высшими функционерами Аль-Каиды*. Поскольку хакеры традиционно воспринимались руководством группировки лишь как *сочувствующие* радикалам, поддержка их деятельности не являлась для джихадистов первоочередной (на что косвенно указывает некоторая обособленность *цифрового батальона* от других структур и слабое освещение его деятельности медиакрылом Ас-*Сахаб*). Кроме того, несмотря на попытки джихадистов (и, в первую очередь, радикальных хакеров) выстроить образ *цифровых мстителей* и создать видимость перманентной угрозы в киберпространстве, реальные показатели их деятельности были далеки от пропагандируемых. Согласно данным правоохранительных органов, более 90% атак лояльных Аль-Каиде* хакерских группировок окончились провалом, что было обусловлено низким уровнем подготовки хакеров и отсутствием у них необходимых инструментов обхода цифровой защиты[50].

Наиболее крупной успешной акцией в киберпространстве (из числа заявленных радикалами), является совместная с *Тунисской Киберармией* (ТСА)[51] операция против

[50] Soesanto S. Cyber Terrorism. Why it exists, why it doesn't, and why it will // Real Instituto Elcano. 17.04.2020. URL: https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/ (accessed: 05.06.2022); Timeline of Cyber Incidents Involving Financial Institutions // Carnegie Endowment for International Peace. 10.07.2021. URL: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline (accessed: 12.06.2022).

[51] Тунисская киберармия (Tunisia Cyber Army, TCA) – группа арабских хакеров, причисляющих себя к тунисским патриотам и специализирующихся на краже банковских данных. Период наибольшей активности: 2012–2017 гг. См.: Tunisian Cyber Army Spree of Attacks on Financial Sites // Data breaches. 03.05.2013. URL: https://www.databreaches.net/tunisian-cyber-army-spree-of-attacks-on-finan-

цифровой системы США в 2013 г.[52]. По заявлениям джихадистов, им удалось обнаружить уязвимости в защите ряда веб-сайтов, принадлежавших правительственным учреждениям США, банкам и транснациональным корпорациям, что в дальнейшем позволило украсть более 1, млн строк конфиденциальных данных (логины, пароли, паспортные данные и пр.)[53].

Усредненная динамика кибератак Аль-Каиды* и лояльных ей хакерских группировок, с 2001 г. по первую половину 2022 г.

Источник: составлено автором

Тем не менее, расследование, проведенное Национальным центром интеграции кибербезопасности и связи (структурное подразделение Министерства внутренней безопасности США) по итогам атаки, показало, что, вопреки заявлениям джихадистов, операция была реализована без их участия, а *почерк* атаки является узнаваемым, и за ним легко определяется ТСА[54].

Впоследствии деятельность Аль-Каиды* в киберпространстве не отличалась значительным размахом. Приписываемые радикалам от ислама хаотичные атаки (последние относительно успешные датируются 2017 г.) не наносили существенного урона цифровой инфраструктуре и практически не освещались в СМИ, что, вероятно, сформировало у руководства группировки разочарованность концепцией киберджихада. На этом фоне проекты вроде *цифрового батальона* были заморожены и выведены из публичного пространства[55], а сами джихадисты вновь сосредоточились на пропагандистской и вербовочной работе.

ИГИЛ*

Несмотря на то, что данная группировка долгое время

cial-sites/ (accessed: 04.06.2022).

[52] «Цифровой батальон» аль-Немра отсчитывал свою историю именно от этой операции (поскольку в ней, по заявлениям радикалов, были задействованы все ключевые фигуры сообщества), хотя официально структура сложилась только в 2015 г. См.: Electronic al-Qaeda Army claims to have hacked US government websites // Russia Today. 11.03.2013. URL: http://www.rt.com/usa/hacked-us-government-websites-112/ (accessed: 10.06.2022); تنظيم القاعدة الإلكتروني يعلن قيام تنظيم القاعدة في اليمن (Al-Qaeda announces al-Qaeda Electronic) // Al-Khabar. 21.01.2015. URL: http://www.alkhabar.ma/تنظيم-القاعدة-في-اليمن-تنظيم-القاعدة-الإلكتروني.html (accessed: 12.06.2022).

[53] Timeline of Cyber Incidents Involving Financial Institutions // Carnegie Endowment for International Peace. 10.07.2021. URL: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline (accessed: 12.06.2022).

[54] Tunisia Cyber Army // US Department of Homeland Security, National Cybersecurity and Communications Integration Center. 27.03.2013. URL: http://dropbox.curry.com/ShowNotesArchive/2013/04/NA-503-2013-04-11/Assets/Cyber%20War$/AQECA.pdf (accessed: 11.06.2022).

[55] В дальнейшем многие сторонники «цифрового батальона» примкнули к киберсообществу «Jaysh al-Malahim al-Electroni», разделяющему ценности Аль-Каиды*, но не аффилированному с ней.

являлась частью структур Аль-Каиды* (и, как следствие, вела работу в цифровом пространстве, опираясь на принятую в ней стратегию), с началом самостоятельной борьбы (в 2014 г.) ее высшие функционеры полностью пересмотрели подход, учтя многие ошибки предшественников. В первую очередь, группировка отошла от принципа *интернет – площадка пропаганды*, укоренившегося среди членов Аль-Каиды*, и, фактически, сделала физическое и цифровое измерения равнозначными. Не последнюю роль в этом сыграла позиция лидера ИГИЛ* Абу Бакра аль-Багдади. В своих проповедях он неоднократно подчеркивал, что цифровое пространство является полноценным полем борьбы, и должно быть использовано для консолидации джихадистов по всему миру, а не только для распространения идей[56].

Кроме того, ключевым отличием модели позиционирования ИГИЛ* от других джихадистских группировок в киберпространстве стала некоторая институционализация собственной деятельности. В частности, функционеры группировки разделили понятие *деятельность в цифровом пространстве* на четыре взаимодополняющих *потока*, управление которыми было закреплено за отдельными институтами и дополнительно контролировалось *Кабинетом* (ближайшим окружением) лидера группировки[57]:

- деятельность с целью обогащения (управление финансовыми потоками[58]);
- деятельность с целью устрашения (организация кибератак и иных акций в цифровом пространстве);
- деятельность с целью укрепления позиций (разведка по открытым источникам[59], координация действий);
- деятельность с целью вербовки (агитационно-вербовочная работа, медиа-сопровождение, создание потенциально вирусного цифрового контента[60] и пр.).

[56] См., напр.: Baghdadi vs. Zawahri: battle for global jihad // Al-Monitor. 25.11.2014. URL: https://www.al-monitor.com/originals/2014/11/battle-global-jihad-bin-laden-legacy.html (accessed: 05.06.2022).
[57] Smith T. The Specter of Cyber in the Service of the Islamic State // American Intelligence Journal – 2017. – №1. – p. 56.
[58] Сюда относится в т.ч. майнинг криптовалют, начатый группировкой в 2016 г. См.: Global Disruption of Three Terror Finance Cyber-Enabled Campaigns // The United States Department of Justice. 13.08.2020. URL: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns (accessed:10.06.2022).
[59] Данная тема была впервые поднята радикалами в Еженедельном информационном бюллетене ИГИЛ* «Аль-Наба», посвященном атакам на посольство Ирака в Кабуле, Афганистан (30 июля 2017 г.). В заметке атака была охарактеризована как «акция высокого качества». Также в статье указывалось, что все данные, необходимые для осуществления теракта, джихадисты получили с помощью инструментов разведки открытых данных. Также в статье присутствовал призыв к другим боевикам перенимать опыт подобных атак и реализовывать их в других регионах. См.: Pastor-Galindo J. et al. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends // IEEE Access. – 2020. – Vol.8. – №1. – pp. 11, 13.
[60] Примером такого контента являются музыкальные клипы «Скоро, очень скоро кровь прольется морем», «Звон мечей» и др., распространяемые радикалами в социальных сетях и мессенджерах в 2015 – 2017 г. См.: «Исламское государство»* пригрозило России терактами // Lenta.ru. 12.11.2015. URL: https://lenta.ru/news/2015/11/12/video/ (дата обращения: 10.06.2022).

В этот же период отмечается активизация хакерских группировок, лояльных джихадистам, и их оформление в полноценную структуру ИГИЛ*[61]. Так, уже во второй половине 2014 г. был создан *Объединенный киберхалифат* (UCC), в состав которого вошли четыре подразделения хакеров (*Призрачный Халифат*, *Киберармия Халифата*, *группа электронной безопасности* и *Армия сыновей Халифата*) и две формально независимых группировки (*Исламская киберармия* и *Рабитат* Аль-Ансар)[62]. Возглавил объединенные силы радикальный хакер Абу Хуссейн аль-Британи[63].

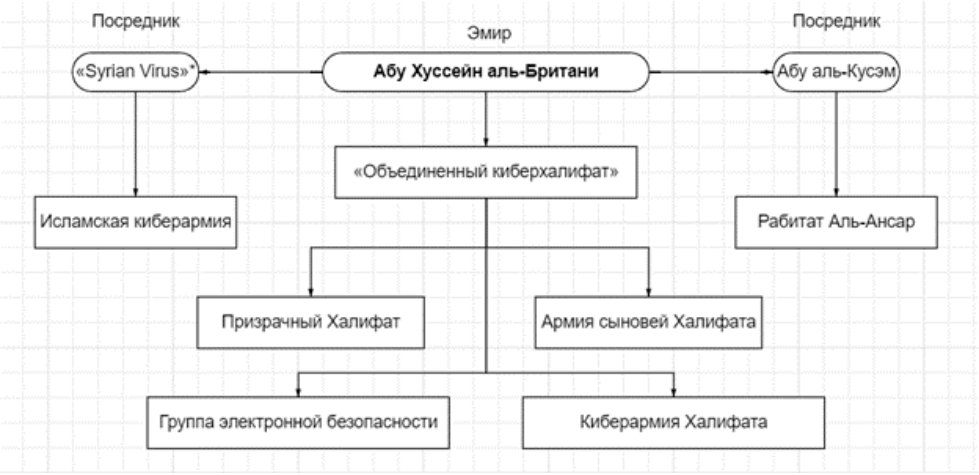


Схема *Объединенного киберхалифата* (UCC) ИГИЛ* на момент его создания (вторая половина 2014 г.), с указанием аффилированных группировок

Источник: Nance M. Hacking ISIS: How to Destroy the Cyber Jihad // Simon and Schuster – 2017 – с. 248, 271–273, 277, 290, 301.

Следует отметить, что члены UCC специализировались не только на проведении наступательных операций (порча веб-сайтов, доксинг и пр.), но и участвовали в защите личных данных радикалов. В частности, под эгидой *Объединенного киберхалифата* был утвержден список веб-приложений и программ, разрешенных к использованию на передовой и в тылу группировки[64], что несколько усложнило слежку за джихадистами со стороны спецслужб. Как результат, к концу 2015 г. ИГИЛ* удалось создать довольно развитую (по сравнению с другими группировками) систему кибербезопасности, а также сформировать посредством пропаганды убежденность в приближении *Эры цифрового джихада*[65].

С другой стороны, период активности *Цифрового халифата* был относительно коротким – менее 3 лет. Уже во второй половине 2017 г. интенсивность действий джихадистов

[61] В отличие от Аль-Каиды*, ИГИЛ* осуществило полноценную интеграцию хакерских отрядов, что позволило более эффективно осуществлять оперативное целеполагание и реализовать большее число успешных кибератак (в соотношении с заявленными).
[62] Hamid N. The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain // Combating Terrorism Centre. 05.04.2018. URL: https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/ (accessed: 17.05.2022).
[63] Абу Хуссейн аль-Британи (Джунаид Хусейн) – британский хакер и пропагандист, основатель международной хакерской группировки «Объединенный киберхалифат». Ликвидирован в августе 2015 г. См.: Hamid N. The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain // Combating Terrorism Centre. 05.04.2018. URL: https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/ (accessed: 17.05.2022).
[64] Mamaev A. Cyber Caliphate: What Apps Are the Islamic State Using? // RIAC. 25.05.2018. URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/cyber-caliphate-what-apps-are-the-islamic-state-using/ (accessed: 12.05.2022).
[65] Glenn C. Timeline: the Rise, Spread, and Fall of the Islamic State // Wilson Centre. 28.10.2019. URL: https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state (accessed: 13.05.2022).

Динамика успешных кибератак, выполненных группировками, входившими в *Объединенный киберхалифат* в 2014–2019 гг.

Источник: составлено автором

в киберпространстве начала стремительно снижаться[66]. Более того, поражение ИГИЛ* в битве при Багхуз-Фавкани (март 2019 г.) и последовавший за этим уход высших функционеров группировки в подполье спровоцировал раскол в рядах UCC, ввиду чего из структуры вышли два подразделения (*Рабитат Аль-Ансар* и *Призрачный Халифат*)[67]. Потеря наиболее боеспособных объединений обернулась провалом ряда операций и нанесло ИГИЛ* дополнительный имиджевый урон.

После ликвидации аль-Багдади в октябре 2019 г. и провозглашения *халифом* Абу Ибрагима аль-Хашими аль-Курайши, группировка вновь пересмотрела подход к деятельности в киберпространстве. В частности, в рамках *доктрины аль-Курайши*[68] было объявлено об активизации пропагандистской и вербовочной деятельности, призванной восстановить позиции ИГИЛ*, в то время как наступательный аспект (кибератаки) был минимизирован. Кроме того, роспуску подверглись структуры UCC, а их членам было рекомендовано перейти к тактике индивидуальной борьбы[69]. Такое решение (обусловленное в т.ч. конфликтом аль-Курайши с преемником основателя UCC Абу Хуссейна аль-Британи[70]) ускорило процесс ослабления лояльного джихадистам хакерского сообщества: лидеры ИГИЛ* уже не могли осуществлять оперативное целеполагание, и хакеры сами выбирали направление удара. Ввиду низкой скоординированности подобные атаки не решали

[66] Также представители экспертного сообщества отмечали малоопытность хакеров ИГИЛ*, поскольку группировка использовала общедоступные хакерские инструменты (зачастую, не требующие специализированных знаний), а ее атаки не скомпрометировали государственные структуры. См.: Alexander A. Clifford B. Doxing and Defacements: Examining the Islamic State's Hacking Capabilities // Combating Terrorism Centre. 05.04.2019. URL: https://ctc.usma.edu/doxing-defacements-examining-islamic-states-hacking-capabilities/ (accessed: 17.05.2022).

[67] Milton D. Structure of a State: Captured Documents and the Islamic State's Organizational Structure // Combating Terrorism Centre. 28.06.2021. URL: https://ctc.usma.edu/structure-of-a-state-captured-documents-and-the-islamic-states-organizational-structure/ (accessed: 13.05.2022).

[68] «Доктрина аль-Курайши» – стратегия поведения ИГИЛ* в условиях «затянувшегося отступления», разработанная высшими функционерами группировки и сформулированная в формате послания второго «халифа» сторонникам после присяги на верность в январе 2020 г. Название взято в кавычки ввиду того, что Стратегия не была официально издана. См., напр.: Ingram J., Mohammed O. The Head of ISIS Is a Hypocrite and a Traitor // Foreign Policy. 19.11.2020. URL: https://foreignpolicy.com/2020/11/19/isis-islamic-state-leader-hypocrite-traitor-mawla-quraishi/ (accessed: 15.05.2022).

[69] Ingram J., Mohammed O. The Head of ISIS Is a Hypocrite and a Traitor // Foreign Policy. 19.11.2020. URL: https://foreignpolicy.com/2020/11/19/isis-islamic-state-leader-hypocrite-traitor-mawla-quraishi/ (accessed: 15.05.2022).

[70] Имя преемника аль-Британи не афишировалось. Согласно источникам, его место занял один из его заместителей, также взявший нисбу аль-Британи. См.: Hamid N. The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain // Combating Terrorism Centre. 05.04.2018. URL: https://ctc.usma.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/ (accessed: 17.05.2022).

поставленной задачи и, как следствие, не получали широкого освещения в СМИ, что создало убежденность в ликвидации хакерского движения исламистов. Как итог, уже к концу 2020 г. ИГИЛ*, по степени представленности в цифровом пространстве, вернулось к уровню конца 2013 г.

Обе радикальные группировки, несмотря на разницу стратегий, прошли схожий путь в развитии цифровой составляющей своей деятельности. И несмотря на то, что ИГИЛ* имело некоторые преимущества перед Аль-Каидой* (в первую очередь, имело возможность использовать эффективные тактики и отказаться от неэффективных, а также получило доступ к более совершенным инструментам борьбы), и даже смогло выйти на ведущие позиции (как ключевой источник цифровой угрозы исламистского характера), преодолеть системные проблемы (реактивный подход к развитию киберструктур, низкий уровень квалификации хакеров, проблемы целеполагания) по итогу не удалось.

Серьезные стратегические просчеты, а также чрезмерная ставка на фактор страха, привели к быстрому снижению наступательного потенциала радикалов от ислама в киберпространстве. Кроме того, ужесточившееся соперничество двух группировок за *идеологическое главенство* среди исламистов не только сделало невозможной кооперацию между ними, но и усложнило работу джихадистов с радикальными хакерами. В результате к концу 2010-х гг. мы можем наблюдать стагнацию цифровых структур обеих группировок и фактическое прекращение ими активной борьбы в киберпространстве.

Абу Бакр аль-Багдади во время своего единственного публичного появления в мечети Мосула вскоре после провозглашения его *халифом,* 5 июля 2014 г.

www.rbc.ru

КИБЕРХАЛИФАТ И ПАНДЕМИЯ COVID-19

С началом пандемии COVID-19[71] нагрузка на цифровые системы, обусловленная повсеместным переходом на удаленный режим работы, многократно увеличилась, сделав их более уязвимыми к атакам извне. Кроме того, выросло среднее время присутствия пользователей в социальных сетях и в Интернете в целом. В свою очередь, это привело к тому, что концепт киберджихада был в очередной раз переосмыслен глобальным исламистским подпольем.

Пандемия COVID-19 привело к тому, что концепт киберджихада был в очередной раз переосмыслен глобальным исламистским подпольем

Аль-Каида*

Неудача с *ударными акциями* в киберпространстве привела к тому, что группировка вернулась к традиционной для нее тактике работы – правда, с некоторыми корректировками. Так, Интернет стал позиционироваться не только как площадку для пропаганды, но и как *пространство консолидации мусульман новой эпохи*. И пандемия COVID-19 только ускорила начатые радикалами преобразования. Можно выделить несколько трендов, характерных для этого периода.

В первую очередь, изменения коснулись идеологической базы деятельности группировки. Так, концепция *Великого исламского халифата*, лежащая в основе *исторической миссии* Аль-Каиды*, была частично экстраполирована на цифровое пространство. Уже в первые месяцы пандемии на пропагандистских ресурсах радикалов вышло несколько видеообращений, в которых высокие представители группировки заявили о намерении принять роль *защитников мусульман* в цифровом пространстве и бороться с *тлетворной пропагандой крестоносцев*[72]. Разумеется, строительство *цифрового халифата* потребовало расширения пропагандистской сети радикалов, а также ее адаптации под новые условия ведения работы, что впоследствии и обусловило увеличение числа формальных и неформальных площадок пропаганды у группировки.

Также, ввиду массового перехода в онлайн, за первый год пандемии ощутимо выросли объемы использования членами Аль-Каиды* различных легальных коммуникационных платформ: Telegram на 30%, RocketChat – на 44%, ChirpWire – более чем на 78%; значительным остается присутствие радикалов от ислама в Twitter и YouTube (показатели изменились менее чем на 1%), в то время как присутствие в Facebook** и Instagram** (где до 2019 г. можно было найти *официальные* аккаунты

[71] В данной работе отправной точкой пандемии COVID-19 считается 30.01.2020 г., когда Всемирная организация здравоохранения объявила эту вспышку чрезвычайной ситуацией в области общественного здравоохранения, имеющей международное значение.

[72] Online Jihadist Propaganda - 2021 in review // Europol. 24.05.2022. URL: https://www.europol.europa.eu/publications-events/publications/online-jihadist-propaganda-2021-in-review (accessed: 12.06.2022).

группировки) упало более чем на 20%[73]. Кроме того, джихадисты продолжили курс на увеличение числа собственных независимых веб-сайтов и мобильных приложений, управляемых сторонниками группировки или сочувствующими им лицами.

Усредненные показатели использования социальных медиа сторонниками Аль-Каиды* (в тыс. чел.) до пандемии и к концу первого ее года

Источник: составлено автором

Крупнейшей акцией Аль-Каиды* на данном направлении стал запуск флагманского портала *Sadaislam* в сентябре 2021 г., на котором публикуются пропагандистские и образовательные материалы группировки, а также новости из различных регионов, где действуют боевики[74]. Среди прочего внимание было уделено и развитию уже существующих площадок – в частности, радикальное информационное агентство *Thabat*, входящее в ядро пропагандистских ресурсов Аль-Каиды*, в первой половине 2021 г. запустило специализированное приложение для мобильных устройств, а также расширило возможности базового веб-клиента[75].

Другой заметной тенденцией стало повышенное внимание джихадистов к обеспечению собственной киберзащиты. В частности, за последний год было создано несколько постоянно функционирующих образовательных ресурсов и закрытых чатов (в первую очередь в ChirpWire и Telegram), в которых публиковались инструкции по корректировке собственного *цифрового следа*, повышению безопасности личных данных и пр.[76]. Факт появления подобных ресурсов (а также повышения качества публикуемых по теме материалов в целом) свидетельствует о некотором прогрессе в развитии цифровых компетенций у джихадистов.

Несмотря на то, что вербовочно-пропагандистская деятельность вновь стала *приоритетом* №1, полностью от наступательных акций в киберпространстве Аль-Каида* не

[73] Fraiwan M. Identification of markers and artificial intelligence-based classification of radical Twitter data // Applied Computing and Informatics – 2022. – №1. – P. 1–13; Bouko C. et al. Discourse patterns used by extremist Salafists on Facebook**: identifying potential triggers to cognitive biases in radicalized content // Critical Discourse Studies. – 2022. – Vol. 19. – №. 3. – P. 252; Mehran W. et al. Humour in jihadi rhetoric: comparative analysis of ISIS, Al-Qaeda, TTP, and the Taliban // Behavioral Sciences of Terrorism and Political Aggression. – 2022. – pp. 11-12, 14.

[74] Online Jihadist Propaganda - 2021 in review // Europol. 24.05.2022. URL: https://www.europol.europa.eu/publications-events/publications/online-jihadist-propaganda-2021-in-review (accessed: 12.06.2022).

[75] Lyammouri R., Nsabia H. The Digital Transformations of Al-Qaeda and Islamic State in the Battle Against Online Propaganda // Global network on Extremism and Technology. 19.05.2022. URL: https://gnet-research.org/2021/05/19/the-digital-transformations-of-al-qaeda-and-islamic-state-in-the-battle-against-online-propaganda/ (accessed: 13.12.2022).

[76] Zegart A. Threats Never Sleep: We still haven't done enough to prevent another 9/11 // Hoover Digest. – 2022. – №. 1. – P. 140.

отказалась, и в настоящий момент продолжает вести точечную работу с хакерским сообществом. Так, начиная с середины 2021 г., джихадисты неоднократно публиковали на своих ресурсах воззвания к компьютерным специалистам, мотивируя их присоединиться к новому этапу борьбы. Основным проводником этой идеи можно считать сетевое сообщество *Jaysh al-Malahim al-Electroni* (*Электронная боевая армия*), являющееся идейным наследником *цифрового батальона* Аль-Каиды* – именно представители данной группы занимались распространением *воззваний* среди лояльных хакеров, а также вели переговоры с претендентами[77]. Примечательно, что призывы к хакерам публиковались в аккаунтах группировки наряду с техническими должностями (разработчик Интернет-ботов, менеджер платформ, администратор веб-сервиса и пр.), что позволяет говорить о попытках радикалов от ислама восполнить дефицит квалифицированных кадров и вновь перейти к наступательным действиям.

Следует подчеркнуть, что свою роль в активизации усилий Аль-Каиды* сыграло недавнее обострение украинского кризиса. В настоящий момент, радикалы от ислама рассматривают происходящие события как возможность воспользоваться разногласиями внутри христианского мира и нанести *неожиданный и сокрушительный удар*. И, хотя большинство экспертов склонны относиться к угрозам джихадистов скептически, недооценивать данный риск не стоит.

ИГИЛ*

Как уже отмечалось выше, к началу глобальной пандемии цифровые структуры группировки оказались в состоянии стагнации, а тактика *индивидуального цифрового террора*, принятая в этот же период, не оправдала себя: уже к концу 2021 г. доля успешных кибератак со стороны ИГИЛ* стала мизерной, и группировка, как и Аль-Каида*, переключилась на развитие экосистемы вербовочных, пропагандистских и образовательных платформ[78]. Более того, ликвидация *Второго Халифа* аль-Курайши в феврале 2022 г. вынудила ИГИЛ* начать выборы нового лидера, что привело к возникновению *переходного периода* длительностью в несколько месяцев – и, как следствие, к заморозке запланированных операций.

[77] См., напр.: Listening to what our enemies say // Center for Security Policy. 14.09.2021. URL: https://centerforsecuritypolicy.org/listening-to-what-our-enemies-say/ (accessed: 10.06.2022).

[78] Радикалами было создано порядка 15 агитационных и 8 образовательных платформ, 3 мобильных приложения, запущено несколько чатов по проблемам кибербезопасности, восстановлены приложения, ориентированные на детскую и подростковую аудиторию. См.: Islamic State evolves 'emoji' tactics to peddle propaganda online // Publico. 10.02.2022. URL: https://www.politico.eu/article/islamic-state-disinformation-social-media/ (accessed: 11.06.2022); Online Jihadist Propaganda - 2021 in review // Europol. 24.05.2022. URL: https://www.europol.europa.eu/publications-events/publications/online-jihadist-propaganda-2021-in-review (accessed: 12.06.2022).

По данным СМИ, ссылавшихся на источники в иракских органах безопасности, на пост *халифа* претендовало четверо кандидатов. Это, в первую очередь, Абу Хадиджа, занимавший пост *губернатора* иракских территорий в период господства ИГИЛ* в Ираке и вместе с главой «военного совета» группировки Абу Сулейманом ан-Насиром руководивший джихадистами в битве за Мосул в 2016–2017 гг., и Абу Муслим, курировавший работу законспирированных ячеек в Сирии на территориях, занятых правительственными войсками. Кроме того, в числе возможных преемников называли некоего Абу Салиха, являвшегося доверенным лицом аль-Багдади и аль-Курайши[79], и Абу Ясира[80] – влиятельного полевого командира, участвовавшего во всех ключевых битвах иракской кампании[81].

Несмотря на то, что переданные иракской стороной данные, с высокой долей вероятности, являлись фейком, распространенным боевиками с целью дискредитации источника (особенно с учетом того, что в представленном списке фигурировали ликвидированные джихадисты) или выявления возможных утечек, они несли в себе важный посыл для мирового сообщества. В первую очередь, имел значение состав кандидатов на пост лидера ИГИЛ*. Так несмотря на то, что претенденты являлись представителями разных *структур* группировки (финансовой, оборонной, пропагандистской), их объединяла приверженность идеям *первого халифа*. Таким образом, радикалы от ислама давали понять, что возможный преемник аль-Курайши откажется от курса, которому группировка следовала в 2020–2021 гг., и сосредоточится на наращивании активности – как это было при аль-Багдади.

Эта гипотеза получила подтверждение в марте 2022 г., когда на пропагандистских ресурсах ИГИЛ* было опубликовано аудиообращение *Кабинета*, в котором прозвучало имя нового лидера джихадистов. Им стал Абу аль-Хасан аль-Хашими аль-Курайши – опытный боевик и соратник первых двух *халифов* ИГИЛ*[82]. А через несколько дней по тем же информационным

Радикалы от ислама рассматривают происходящие события на Украине как возможность воспользоваться разногласиями внутри христианского мира и нанести удар

[79] Вероятнее всего, имеется в виду Абу Салих аль-Афри (Муваффак Мустафа Мохаммед аль-Кармуш) – высокопоставленный член ИГИЛ*, курировавший финансовые операции группировки. Учитывая, что аль-Афри был ликвидирован в ноябре 2015 г., не исключено, что под псевдонимом выступает другой джихадист из его ближайшего окружения.

[80] Абу Ясир (Джаббар Салман Али Фархан аль-Иссави) был ликвидирован в январе 2021 г. Вероятно, как в случае с аль-Афри, под его именем фигурирует другой функционер группировки.

[81] Islamic State likely to pick battle-hardened Iraqi as next leader: officials, analysts // Reuters. 09.02.2022. URL: https://www.reuters.com/world/middle-east/islamic-state-likely-pick-battle-hardened-iraqi-next-leader-officials-analysts-2022-02-09/ (accessed: 17.05.2022).

[82] Тень «Халифата»: куда новый лидер поведет террористов // Журнал «Эксперт». 09.05.2022. URL: https://expert.ru/expert/2022/19/ten-khalifata-kuda-noviy-lider-povedet-terroristov/ (дата обращения: 10.06.2022); Также на некоторых новостных ресурсах появлялась информация, что третий «халиф» является братом аль-Багдади, однако позже эта версия была признана несостоятельной и опровергнута. См.: Exclusive: New Islamic State leader is brother of slain caliph Baghdadi - sources // Reuters. 11.03.2022. URL: https://www.reuters.com/world/middle-east/exclusive-new-islamic-state-leader-is-brother-slain-caliph-baghdadi-sources-2022-03-11/ (accessed: 13.06.2022).

каналам было дополнительно распространено выступление официального спикера группировки Абу Хамзы аль-Курейши, в котором подробно рассказывалось о ближайших целях группировки[83]. Среди прочего, аль-Курейши подчеркнул, что новый лидер пришел, чтобы «возродить Халифат в его былом величии» – иными словами, вернуть группировку к стратегии развития, существовавшей в эпоху *первого халифа* аль-Багдади.

Под *возрождением Халифата* функционеры ИГИЛ*, вероятнее всего, понимают восстановление позиций группировки в Сирии и Ираке, однако, принимая во внимание стоящие перед джихадистами трудности (иссякание финансовых потоков, недостаток квалифицированных командиров, разногласия между отдельными *вилайатами* и т.д.), радикалы, вероятнее всего, будут искать способ заявить о себе по-другому – и создание *проекции халифата* в цифровом пространстве в данном случае выглядит довольно очевидным решением.

Как мы можем видеть, и для Аль-Каиды*, и для ИГИЛ* киберпространство по ряду причин вновь превращается в удобное поле для реализации идеологических мегапроектов (в первую очередь, для построения халифата, о чем заявляют в своих пропагандистских материалах обе группировки). Во-первых, концепция *Цифровой халифат* 2.0 не потребует от группировок значительного физического присутствия в регионе интереса[84] (поскольку проект будет существовать виртуально), а также создаст постоянную напряженность не только на Ближнем Востоке (по причине существования системных проблем в организации киберзащиты у большинства государств региона[85]), но и за его пределами. Во-вторых, уход в цифровое пространство, вероятно, позволит радикалам от ислама вернуться к прежним объемам агитационно-вербовочной работы, чему во многом поспособствует увеличение доли деплатформенных площадок. Существует довольно большое количество спорных тем, связанных с киберпространством, на критике которых джихадисты могут строить новую кампанию – развитие мусульманскими странами систем обращения с криптовалютами (что противоречит правилам исламского банкинга[86]), расшире-

[83] В ходе выступления Абу Хамза аль-Курейши, в частности, обратился к хакерскому сообществу, призвав его «присоединиться к праведной борьбе под началом нового Халифа», а также отомстить за гибель ключевых персон группировки от рук отступников. См.: ISIS announces campaign to avenge the death of its former leader and spokesman // The Mair Amit Intelligence and Terrorism Information Center. 19.04.2022. URL: https://www.terrorism-info.org.il/en/isis-announces-campaign-to-avenge-the-death-of-its-former-leader-and-spokesman/ (accessed: 14.06.2022).

[84] В случае с данной работой таковым является, в первую очередь, регион Ближнего Востока и Северной Африки (БВСА). Хоть интересы радикалов от ислама прослеживаются и в других частях мира (например, в Южной Азии), именно регион БВСА традиционно является основной ареной «обкатки» киберсредств джихадистов.

[85] Выявлено на основе анализа отчетов «Global Cybersecurity Index» (GCI), издаваемых МСЭ. См.: Global Cybersecurity Index // ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed: 17.05.2022).

[86] Нарушается принцип «мусавама» (равной цены): поскольку курс цифровой валюты характеризуется нестабильностью и не гарантирует полное покрытие издержек со стороны продавца в случае резкого ценового скачка. См.: Is trading in crypto units

ние запущенного Facebook** проекта *Metaverse*[87] на исламские страны и т.д. В этой связи начало очередной волны *цифрового джихада* будет восприниматься уже не как последствие поражения группировки, а как ее адаптация к современным условиям борьбы.

Кроме того, можно наблюдать, что террористы вновь вернулись к идее создания *цифровых отрядов*, которые могли бы быть на постоянной основе вовлечены в процесс борьбы и, в зависимости от ситуации, выступать либо как основная ударная единица, либо как вспомогательные силы. В целом, подобная риторика укладывается в долгосрочные планы ведущих исламистских группировок о *цифровом реванше*.

Террористы ИГИЛ* из пропагандистского видео группировки

Источник: www.hstoday.us

halal? // Khaleej Times. 11.02.2018. URL: https://www.khaleejtimes.com/business/is-trading-in-crypto-units-halal (accessed: 15.05.2022). При этом сами джихадисты активно добывают и используют криптовалюту.

[87] По замечаниям ряда богословов, развитие системы метавселенных ставит под сомнение идею о главенстве Аллаха над всеми мирами (Коран 1:2, 28:30, 7:54). Кроме того, концепция создания цифровых аватаров также порицается традиционалистами. См., напр.: Is the Metaverse the New Online Frontier for Halal Brands? // Muslim Network. 11.08.2021. URL: https://www.muslimadnetwork.com/2021/08/11/metaverse-for-halal-brands/ (accessed: 12.06.2022).

ЗАКЛЮЧЕНИЕ

Таким образом, опора на доступные данные позволяет нам говорить о продолжающемся *переходном* периоде в развитии цифровых структур Аль-Каиды* и ИГИЛ*, в рамках которого, с одной стороны, существенно снижается реальная вовлеченность джихадистов в борьбу, а, с другой, происходит сосредоточение обеих группировок на развитии собственного агитационно-вербовочного аппарата. Что касается наступательного аспекта цифровой деятельности, то неудачный опыт включения в кибервойну за счет форсированного развития собственных структур в 2015–2017 гг. заставил радикалов от ислама на какое-то время отказаться от наращивания наступления и практически полностью воздержаться от освещения этого направления в пропаганде (даже в период пандемии COVID-19, когда уязвимость мировой цифровой архитектуры повысилась). По этой причине вопрос возвращения международных террористических организаций к тактике *цифрового джихада* в обозримой перспективе по-прежнему остается дискуссионным – в том числе по причине отсутствия достаточного количества достоверной информации о приоритетах радикалов от ислама на данном этапе, уровне их реальных компетенций и степени влиятельности в среде хакеров.

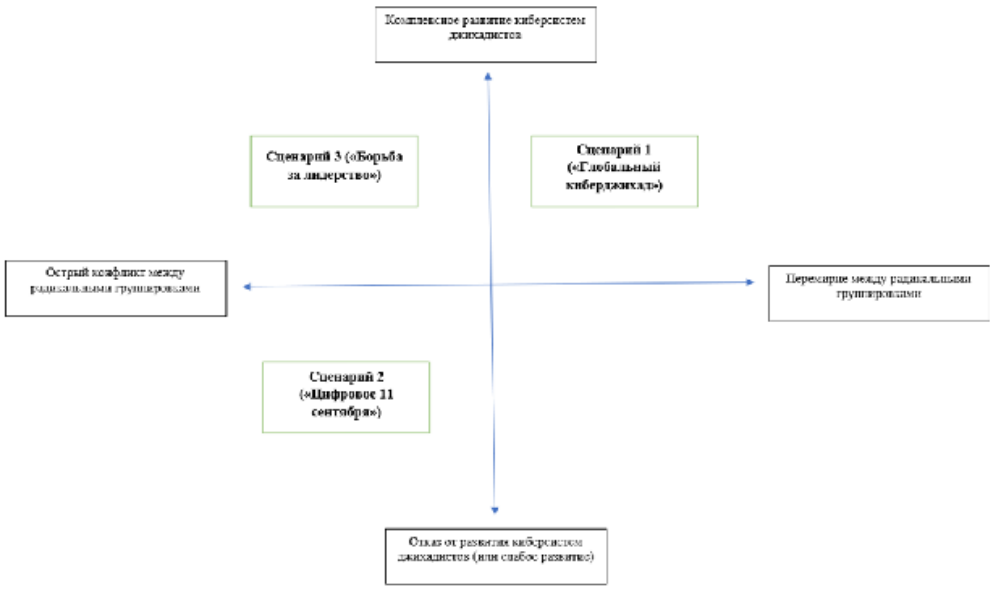
С другой стороны, именно агитационная деятельность в цифровом пространстве, на которую сегодня делают ставку джихадисты, постепенно закладывает идейную основу *Киберхалифата* (*как эфемерного цифрового союза борцов-праведников*[88], *не имеющего границ и, как следствие, априори не способного быть разрушенным*), вокруг которой в дальнейшем могут быть *собраны* и другие направления борьбы (в числе которых и цифровой террор). Однако ключевым препятствием для радикалов от ислама в данном случае является факт, что и Аль-Каида*, и ИГИЛ* претендуют на статус единоличного *защитника* интересов *праведников* и не готовы делить лидерство с конкурентами – а это, в свою очередь, может привести к новому витку соперничества между двумя организациями.

Как бы то ни было, на основании ряда косвенных признаков можно построить первичный прогноз относительно дальнейшего развития ситуации. При анализе необходимо учитывать два ключевых маркера – стратегию трансформации цифровых структур (как формальных, так и неформальных) радикалов от ислама (курс на усложнение или упрощение имеющихся элементов) и формат взаимодействия друг с другом в рамках глобального исламистского подполья (в зависимости от ситуации может подразумевать как сближение, так и конфронтацию).

[88] Слово *праведник* в данном случае написано курсивом по той же причине, что и слово *фетва* ранее.

Основываясь на перечисленном ранее, можно вывести несколько вариантов развития ситуации.

Так, первый сценарий предполагает, что джихадистские группировки уже в краткосрочной перспективе развернут активную деятельность в киберпространстве, мобилизовав для этих целей всех лояльных себе хакеров и вновь провозгласив наступление *эры цифрового джихада*. Не исключено, что для большего эффекта лидеры Аль-Каиды* и ИГИЛ* на какое-то время попытаются свести к минимуму затянувшийся конфликт между группировками (по крайней мере, его публичную составляющую), чтобы сформировать у мирового сообщества убежденность в преодолении исламистами внутреннего кризиса и актуализации угрозы *Цифрового 11 сентября*. С другой стороны, несмотря на общность идей (а также некоторое снижение конфронтации в последний год), уровень недоверия между двумя группировками по-прежнему запредельно высок. По этой причине повышение киберпотенциала одной из них (пусть и обращенного *острием* вовне) станет серьезным фактором разобщения, поскольку создаст постоянную угрозу для других джихадистских объединений и, с высокой долей вероятности, обострит соперничество между ними. Вероятность реализации данного сценария – *средняя*.



Сценарный крест: основные варианты дальнейшего развития ситуации

Источник: составлено автором

Второй, более категоричный, сценарий предполагает, что джихадисты попытаются реализовать цифровой удар без предварительного наращивания потенциала и сближения с конкурентами, делая ставку исключительно на эффект неожиданности. В этом случае целью для атаки, с высокой долей вероятности, станет объект критической инфраструктуры (например, АЭС), что позволит максимизировать психологический эффект от операции и обеспечит широкое информационное сопровождение. *Цифровой джихад* (в виде разовой атаки) в данном случае будет позиционироваться как сигнал о возвращении джихадистов в глобальное противостояние, а также как исполнение ранее прозвучавших угроз. Однако, с учетом деградации цифровых структур радикалов от ислама, им вряд ли удастся достичь

поставленной цели. Более того, за столь агрессивным выпадом гарантированно последует массированная контратака со стороны ведущих кибердержав (а также противостоящих террористам хакерских группировок), которую цифровые структуры джихадистов не выдержат. Таким образом, *цифровой джихад* будет остановлен уже на начальном этапе. В данном случае предполагаемые потери многократно превышают приобретения, ввиду чего вероятность реализации сценария – *низкая*.

Третий (и *наиболее вероятный*) сценарий подразумевает, что джихадисты в относительно короткий (до двух лет) промежуток времени восстановят киберструктуры, существовавшие в 2015–2017 гг., а также усилят их рядом вспомогательных элементов (например, звеном из хакеров-одиночек). Не исключено также, что в данном случае будет существовать разделение специализации хакеров на наступательную и оборонительную, для обеспечения большей устойчивости формируемых институтов. Однако, в отличие от первого сценария, упор будет сделан не на ведение глобальной борьбы, а на достижение лидерства среди исламистов. Соответственно, первой задачей группировок станет дискредитация и последующее низвержение оппонента (один из вариантов которого – лишение его поддержки хакерского сообщества и, как результат, передовым методам цифровой борьбы). В дальнейшем же, по мере укрепления позиций победившей группировки, начнется постепенное расширение цифрового фронта – с последующим переходом противостояния на глобальный уровень.

Так или иначе, все три сценария имеют точку пересечения: первое время джихадисты не будут предпринимать масштабных наступательных действий в киберпространстве, а сосредоточатся на незначительных целях (веб-сайты СМИ, закрытые базы данных и пр.), маскируясь под киберпреступные группировки. Такой подход позволит, с одной стороны, избежать раннего обнаружения, а, с другой стороны, оценить сильные и слабые стороны цифровой обороны противника. ■

** Перечисленные в работе организации являются террористическими, их деятельность запрещена на территории РФ. В соответствии с положениями федерального закона N 35-ФЗ «о противодействии терроризму», статья не является пропагандистской, представленная в ней информация носит ознакомительный характер.*

*** Перечисленные социальные платформы принадлежат компании «Meta», признанной экстремистской организацией и запрещенной в РФ.*

ГЛОССАРИЙ

Аль-дарурат тубих аль-махзурат (*Запрещенное становится дозволенным в случае крайней необходимости*) – один из основополагающих принципов исламского права. Как правило, *крайняя необходимость* (*дарурат*) наступает, когда одна из пяти ценностей по шариату (жизнь, вера, ум, совесть, имущество) оказывается под угрозой разрушения или уничтожения.

Ас-Сахаб – официальное медиакрыло Аль-Каиды*, отвечающее за создание пропагандистских материалов, включая проповеди, воззвания и документальные фильмы. В 2008 г. включено в состав *компьютерного департамента* Комитета по медиа группировки.

Джихад меча **(также газават)** – священная война, вооруженная борьба с неверными.

Джихад познания – борьба посредством распространения истинных знаний об исламе.

Джихад языка – призыв к другим совершенствоваться, становиться лучше, то есть обращение к другим людям с *повелением одобряемого и запрещением порицаемого*.

Доксинг – поиск и публикация персональной или конфиденциальной информации о человеке без его согласия. Относится к нарушению сетевого этикета и часто запрещен внутренними правилами интернет-сообществ.

Доктрина аль-Курайши – стратегия поведения ИГИЛ* в условиях *затянувшегося отступления*, разработанная высшими функционерами группировки и сформулированная в формате послания второго *халифа* сторонникам после присяги на верность в январе 2020 г. Название взято в кавычки ввиду того, что Стратегия не была официально издана.

Метавселенная (также Metaverse) – постоянно действующее виртуальное пространство, в котором люди могут взаимодействовать друг с другом и с цифровыми объектами через свои аватары, с помощью технологий виртуальной реальности.

Мусавама – принцип исламского банкинга (*принцип равной цены*). Осуществление купли-продажи в результате рыночного торга между продавцом и покупателем. В данном случае продающий не определяет реальную стоимость своего товара, а цена устанавливается по ходу торга между продавцом и

покупателем в результате их договоренности.

Нисба – составная часть арабского (мусульманского) имени обозначающее этническую, религиозную, политическую, социальную принадлежность человека, место его рождения или проживания и др.

Объединенный киберхалифат **(United Cyber Caliphate, UCC)** – формирование в структуре ИГИЛ*, созданное компьютерным специалистом Абу Хуссейном аль-Британи (*см. краткий справочник по персонам, Абу Хуссейн аль-Британи*) и включающее в себя несколько радикальных хакерских команд.

Разведка по открытым источникам (Open Source Intelligence, OSINT) – разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из открытых источников, а также ее анализ.

Система диспетчерского управления и сбора данных (Supervisory Control And Data Acquisition, SCADA) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления.

Такфир – обвинение в неверии (куфре). Человек, которому вынесен такфир, считается неверным (кафиром).

Такфиризм – радикальная исламистская идеология, основой которой является обвинение в неверии мусульман (*см. такфир*).

Тунисская киберармия (Tunisia Cyber Army, TCA) – группа арабских хакеров, причисляющих себя к тунисским патриотам и специализирующихся на краже банковских данных. Период наибольшей активности: 2012–2017 гг.

Фетва – в исламе решение по какому-либо вопросу, выносимое муфтием, факихом или алимом, основываемое на принципах ислама и на прецедентах мусульманской юридической практики.

Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Цифровая Хиросима **(также возможны варианты *Цифровой Перл-Харбор*, *Цифровое 11 сентября*)** – термин, используемый для обозначения сокрушительного удара в киберпространстве,

наносящего впоследствии, в том числе, серьезный психологический урон.

Цифровой батальон* Аль-Каиды – тактический альянс хакерских команд, разделяющих ценности джихадистов, возглавляемый Яхьей аль-Немром (*см. краткий справочник по персонам, Яхья аль-Немр*). Впоследствии частично трансформировался в неформальное сетевое движение *Jaysh al-Malahim al-Electroni*, разделяющее ценности Аль-Каиды*, но не аффилированное с ней.

DDoS-атака – хакерская атака на вычислительную систему с целью довести ее до отказа. Создание таких условий, при которых пользователи системы не смогут получить доступ к предоставляемым системным ресурсам, либо этот доступ будет затруднен.

Duqu (~DQ) – троянская программа, используемая для целенаправленных атак на крупные компании и промышленные предприятия. Считается продолжением сетевого червя Stuxnet (*см. Stuxnet*).

Stuxnet – универсальный автономный инструмент промышленного шпионажа, предназначенный для получения доступа к операционной системе, отвечающей за обработку, сбор данных и оперативное диспетчерское управление промышленными объектами. В отличие от большинства аналогичных вирусов, основным применением Stuxnet может стать не хищение данных, а повреждение промышленных автоматизированных систем.

Win95/CIH (*Чернобыль*) – резидентный вирус, работающий под операционной системой Windows 95/98/ME. В годовщину Чернобыльской аварии вирус активизировался и уничтожал данные на жестких дисках инфицированных компьютеров. На некоторых компьютерах также было испорчено содержимое микросхем BIOS.

КРАТКИЙ СПРАВОЧНИК ПО ПЕРСОНАМ[89]

Абдул Кадир бин Абдул Азиз – радикальный исламист, богослов. Наравне с аль-Макдиси (*см. Абу Мухаммад аль-Макдиси*) считается важной фигурой в пропаганде Аль-Каиды* и частично ИГИЛ*.

Абу аль-Кусем (*настоящее имя неизвестно*) – иракский (предположительно) хакер, являвшийся ключевым посредником UCC (*См. глоссарий, Объединенный киберхалифат*) при работе с группировкой *Рабитат аль-Ансар*. Подтвержденные сведения о ликвидации отсутствуют.

Абу аль-Хасан аль-Хашими аль-Курайши – третий *халиф* ИГИЛ* (с 2022 г.).

Абу Бакр аль-Багдади (Ибрахим Аввад Ибрахим Али аль-Бадри; Абу Дуа) – радикальный исламист, богослов, лидер ИГИЛ*, первый *халиф* группировки. До обособления ИГИЛ* в самостоятельную группировку (2003–2013) являлся одной из ключевых функционеров Аль-Каиды* в Ираке. Ликвидирован в 2019 г.

Абу Ибрагим аль-Хашими аль-Курайши – международный террорист, второй *халиф* ИГИЛ* (2019–2022), ранее – приближенное лицо Абу Бакра аль-Багдади (*см. Абу Бакр аль-Багдади*). До избрания на пост лидера группировки носил прозвище *эмир войны*, подчеркивающее его высокий статус и роль в *военном совете* группировки. Ликвидирован в 2022 г.

Абу Муслим (*настоящее имя неизвестно*) – полевой командир ИГИЛ*, военный советник. Курировал работу законспирированных ячеек в Сирии на территориях, занятых правительственными войсками. Подтвержденные сведения о ликвидации отсутствуют. Также, за счет совпадения имен, его можно спутать с Абу Муслимом ат-Туркмани (Фадиль Ахмад Абдалла аль-Хияли), одним из *теневых лидеров* джихадистов в Ираке, отвечавшим за кадровую политику на занятых территориях и ликвидированным в 2015 г.

[89] Перечисленные в данном разделе персоны являются сторонниками или идеологами террористических и радикальных организаций, чья деятельность запрещена на территории РФ, а также членами преступных и околорадикальных хакерских сообществ. В соответствии с положениями федерального закона N 35-ФЗ «о противодействии терроризму», представленные материалы не являются пропагандистскими, представленная информация носит ознакомительный характер и направлена на систематизацию находящихся в открытых источниках данных и, как следствие, более комплексное осмысление содержания данной работы.

Абу Мухаммад аль-Макдиси (Иссам Мухаммад Тахир аль-Баркауи) — иорданский алим палестинского происхождения, идеолог салафитского джихадизма, одна из ключевых фигур в пропаганде Аль-Каиды*. Критиковал ИГИЛ* за обособление от Аль-Каиды*, однако в то же время призывал к заключению перемирия между двумя группировками и формированию единого фронта против *крестоносцев*. Неоднократно арестовывался властями Иордании.

Абу Обейда Саиди (настоящее имя неизвестно) – иракский (предположительно) террорист, помощник Яхьи аль-Немра (*см. Яхья аль-Немр*), пресс-секретарь *Цифрового батальона* Аль-Каиды* (*см. глоссарий, Цифровой батальон*). Подтвержденные сведения о ликвидации отсутствуют.

Абу Салих аль-Афри (Муваффак Мустафа Мохаммед аль-Кармуш) – высокопоставленный член ИГИЛ*, курировавший финансовые операции группировки в 2013–2015 гг. Ликвидирован в 2015 г.

Абу Сулейман ан-Насир (Абу Сулейман ан-Насир Лидиниллах) – иракский террорист, один из ключевых функционеров ИГИЛ*, старший военный советник. С 2014 г. занимал должность главы *Военного совета* группировки, участвовал в разработке ключевых операций иракской и сирийской кампаний. Подтвержденные сведения о ликвидации отсутствуют.

Абу Хадиджа (*настоящее имя неизвестно*) – губернатор одной из территорий ИГИЛ* в Ираке. Доверенное лицо Абу Муслима ат-Туркмани (*см. Абу Муслим*). Подтвержденные сведения о ликвидации отсутствуют.

Абу Хамза аль-Курейши – международный террорист, официальный представитель и пресс-секретарь ИГИЛ* (с 2019 г.). Как правило, полное представление звучит как «шейх-мухаджир Абу Хамза аль-Курейши».

Абу Хуссейн аль-Британи (Джунаид Хусейн) – британский хакер и пропагандист, основатель международной хакерской группировки *Объединенный киберхалифат* (*См. глоссарий, Объединенный киберхалифат*). Ликвидирован в 2015 г.

Абу Ясир (Джаббар Салман Али Фархан аль-Иссави) – полевой командир ИГИЛ*, участвовавший во всех ключевых операциях иракской кампании, а также контролировавший рекрутинг на территории Ирака. Ликвидирован в 2021 г.

Айман аз-Завахири (Айман Мухаммад Рабии аз-Завахири) –

международный террорист, второй лидер (эмир) Аль-Каиды*. Ранее – личный врач Усамы бен Ладена (*см. Усама бен Ладен*). Также известен как богослов-такфирист.

Али бин Хидр аль-Худиар – радикальный богослов, идеолог салафитского джихадизма. Один из наиболее активных сторонников концепции глобального халифата.

Катада аль-Сайнави (настоящее имя неизвестно) – террорист (национальная принадлежность не установлена), заместитель Яхьи аль-Немра (*см. Яхъя аль-Немр*). Отвечал за связи с группировкой *Al-Qaeda Alliance Online*. Подтвержденные сведения о ликвидации отсутствуют.

Махмуд аль-Аднани (настоящее имя неизвестно) – террорист (национальная принадлежность не установлена), заместитель Яхьи аль-Немра (*см. Яхъя аль-Немр*). Отвечал за связи с группировкой *Al-Qaeda Electronic*. Подтвержденные сведения о ликвидации отсутствуют.

Моаз аль-Тикрити (настоящее имя неизвестно) – иракский (предположительно) террорист, помощник Яхьи аль-Немра (*см. Яхъя аль-Немр*), глава финансовой службы *Цифрового батальона* Аль-Каиды* (*см. глоссарий, «Цифровой батальон»*). Подтвержденные сведения о ликвидации отсутствуют.

Насир аль-Фахд – исламский ученый-салафит, родом из Саудовской Аравии. Стал известен благодаря скандальным проповедям, в рамках которых оправдывал джихадизм и применение ОМУ против США, Израиля и других *крестоносцев*, а также против *отступников* из числа мусульман. Арестован саудовскими властями в 2003 г.

Омар бин Ахмед аль-Хазими – саудовский богослов, основоположник экстремистского направления ваххабизма (хазимизм). Какое-то время являлся одним из ключевых идеологов ИГИЛ* (до развенчания его идей по инициативе старшего религиоведа группировки Турки аль-Бинали в 2013 г.). Арестован саудовскими властями в 2015 г.

Сулейман бин Насир аль-Ульван – саудовский проповедник радикального толка. В своих проповедях поддерживал действия Аль-Каиды*, призывал к вооруженному восстанию против династии Саудитов с последующим превращением Саудовской Аравии в плацдарм для *экспорта джихада*. Неоднократно подвергся критике ведущих богословов Саудовской Аравии за свои враждебные высказывания. Арестован саудовскими властями в 2015 г.

Усама бен Ладен (Усама бен Мухаммед бен Авад бен Ладен) – международный террорист, основатель и первый лидер (эмир) Аль-Каиды*. Один из наиболее одиозных джихадистов и ключевая цель американской *Войны против терроризма* (2001–2011 г.). Ликвидирован в 2011 г.

Халид аль-Рашид – саудовский богослов, активный сторонник джихадизма. Разделял идеи Абдул Кадира бин Абдул Азиз (*см. Абдул Кадир бин Абдул Азиз*) и Абу Мухаммада аль-Макдиси (*см. Абу Мухаммад аль-Макдиси*). Арестован саудовскими властями в 2015 г.

Хамуд бин Укла аль-Шуайби (Абу Абдуллах Хамуд Бин Абдуллах Бин Укла Бин Мухаммад Бин Али Бин Укла Аш-Шуайби Аль-Халиди из Аль-Джинаах, из племени Бани Халид) – саудовский богослов. Один из крупнейших и наиболее авторитетных сторонников джихадизма среди суннитских ученых, поддерживал и одобрял деятельность исламистов в Афганистане и на Ближнем Востоке. Известен, в первую очередь, тем, что вынес такфир (обвинение в неверии) королю Саудовской Аравии. Арестован саудовскими властями в 1995 г.

Яхья аль-Немр – иракский специалист в области компьютерной безопасности, основатель и руководитель (эмир) *Цифрового батальона* Аль-Каиды* (*см. глоссарий, Цифровой батальон*). Подтвержденные сведения о ликвидации отсутствуют.

Irhabi007 (настоящее имя неизвестно) – пакистанский (предположительно) хакер, посредник *Цифрового батальона* Аль-Каиды* (*см. глоссарий, Цифровой батальон*) при работе с независимой группировкой пакистанских хакеров *Youni Tsoulis*. Подтвержденные сведения о ликвидации отсутствуют.

Syrian Virus (настоящее имя неизвестно) – сирийский хакер, являвшийся ключевым посредником UCC (*См. глоссарий, Объединенный киберхалифат*) при работе с группировкой *Исламская киберармия*. Подтвержденные сведения о ликвидации отсутствуют.

Индекс Безопасности – Научные записки

№17 (43), 2022

Леонид Цуканов

Взлеты и падения *Киберхалифата*:
Аль-Каида* и ИГИЛ*
в цифровом пространстве

Главный редактор: В.А. Орлов

Редактор: Е.Г. Чобанян

Дизайн и компьютерная верстка: Е.Г. Чобанян

В оформлении доклада используется фрагмент гравюры Альбрехта Дюрера *Носорог*

Работа над данной научной запиской
завершена 14 сентября 2022 г.

ИНДЕКС БЕЗОПАСНОСТИ

Индекс Безопасности – Научные записки – доклады, аналитические статьи, комментарии и интервью, которые отражают позиции российских и зарубежных экспертов по актуальным вызовам глобальной безопасности и политики России в этой сфере.

Задача серии – дать понятный анализ проблем международной безопасности и предложить для них конкретные и реалистичные решения. Серия пришла на смену журналу *Индекс Безопасности*, издаваемому ПИР-Центром в 1994 – 2016 гг.

Авторы и редакторы серии будут рады комментариям, вопросам и предложениям, которые читатели могут направить на электронную почту inform@pircenter.org.

НОВЫЕ ТЕХНОЛОГИИ И ИНТЕРЕСЫ РОССИИ

Данная научная записка выполнена в рамках проекта *Новые технологии и интересы России*, который является частью программы *Глобальная и региональная безопасность: новые идеи для России* и нацелен на изучение влияния новых технологии на мировую архитектуру безопасности, трансформации вызовов военной и невоенной безопасности России, а также поиск решений, позволяющих минимизировать потенциальные угрозы через широкое обсуждение и международное регулирование.

ЕВСТАФЬЕВСКАЯ СЕРИЯ

Данная записка выпущена в рамках *Евстафьевской серии.* Это серия научно-исследовательских и научно-практических публикаций молодых, начинающих авторов из России и различных государств мира в области международной безопасности - прежде всего, аспирантов и магистрантов. Для многих это их первая или одна из первых полноформатных научных публикаций, с обязательным внешним рецензированием и предварительным обсуждением проекта на научно-образовательных семинарах в ПИР-Центре или в аналогичных форматах.

Ежегодно 15 ноября комиссия *Евстафьевской серии* присуждает молодому специалисту, чья научная записка признается лучшей, премию имени Г.М. Евстафьева.

Геннадий Михайлович Евстафьев (1938 – 2013) - выдающийся советский, российский специалист в области нераспространения ОМУ и глобальной безопасности. Последние десять лет жизни Г.М. Евстафьев посвятил ПИР-Центру, где работал в должности старшего вице-президента и уделял большое внимание творческому, научному росту молодежи, считая это своей важнейшей миссией и важнейшей миссией ПИР-Центра.

Галерея памяти Геннадия Евстафьева: https://pircenter.org/experts/194-gennady-evstafiev.

Премия имени Г.М. Евстафьева была учреждена в 2021 году. Лауреаты премии:

- 2021 - С.Д. Семенов.