RUDN Journal of Political Science. ISSN 2313-1438 (print), ISSN 2313-1446 (online)
Вестник Российского университета дружбы народов. Серия: ПОЛИТОЛОГИЯ
2022 Vol. 24 No. 3 408–418
http://journals.rudn.ru/political-science

DOI: 10.22363/2313-1438-2022-24-3-408-418

Научная статья / Research article

Даркнет и политическое

М.В. Яковлев

Московский государственный университет имени М.В. Ломоносова, Москва, Российская Федерация

maxvuz@mail.ru

Аннотация. Даркнет становится все более заметной структурной единицей в политической сфере и вместе с тем пока остается малоизученным участком киберпространства. Поэтому в исследовании ставится цель определить концептуальную призму для его рассмотрения и его актуальное значение в измерении политического. При помощи сравнительно-исторического метода выявляются причины и время политического рождения Даркнета, посредством системного и контент-анализа характеризуются его ресурсы и политическая роль, на основе положений Р. Геля, М. Кастельса, К. Шмитта и др. систематизируются и уточняются понятия власти и политики в Сети. Делается вывод о том, что основным фактором политизации и трансформации Даркнета стала экспансия государств (в особенности автократий) в интернет-пространстве. Давление систем власти и доминирования, нацеленных на поддержание в киберпространстве суверенитета и контроля, вызвало «цифровое сопротивление» программистов и пользователей, стремящихся к свободному обмену данными и конфиденциальности, а также гражданских активистов, желающих избежать преследования за инакомыслие, что обусловило обновление архитектуры и функционала Даркнета, его превращение в альтернативное пространство информационного взаимодействия и базу для наращивания оппозиционного потенциала. Возможностями новой сети для своих целей воспользовался и криминалитет. Основным результатом исследования является тезис о том, что Даркнет трансформируется в особую социально-техническую систему, находящуюся вне сферы международного и государственного права, где все взаимодействия осуществляются только посредством частных соглашений между клиентами, где на основе криптовалют сформирована альтернативная мировая платежная система.

Ключевые слова: власть, Даркнет, киберпространство, политическое, хактивизм, цифровое сопротивление

Для цитирования: *Яковлев М.В.* Даркнет и политическое // Вестник Российского университета дружбы народов. Серия: Политология. 2022. Т. 24. №3. С. 408–418. https://doi.org/10.22363/2313-1438-2022-24-3-408-418

Благодарности: Исследование выполнено при поддержке Междисциплинарной научно-образовательной школы Московского университета «Сохранение мирового культурно-исторического наследия».

Darknet and the Political

Maksim V. Yakovlev

Lomonosov Moscow State University, Moscow, Russian Federation

maxvuz@mail.ru

Abstract. The Darknet is becoming an increasingly visible structural unit in the political sphere and at the same time remains a little-studied area of cyberspace. Therefore, the article aims to determine the conceptual prism for its consideration and its actual significance in the measurement of the political. With the help of comparative historical analysis, the study reveals the causes and time of the political birth of the Darknet, characterizes its resources and political role through system and content analysis, systematizes and clarifies the concepts of power and politics in the Network based on the provisions of R. Gel, M. Castels, K. Schmitt, etc. The author names the expansion of states (especially autocracies) in the digital space as the main factor in the politicization and transformation of the Darknet. The pressure of power and dominance systems aimed at maintaining sovereignty and control in cyberspace caused "digital resistance" of programmers and users seeking free data exchange and confidentiality, as well as civil activists who strived to avoid prosecution for dissent, which led to the renewed architecture and functionality of the Darknet, its transformation into an alternative space of informational interaction and a database to build up the opposition potential. Criminals also took advantage of the opportunities of the new network for their own purposes. The main result of the research is the thesis that the Darknet is being transformed into a special socio-technical system that is outside the sphere of international and state law, where all interactions are carried out exclusively through private agreements between clients, with an alternative world payment system based on cryptocurrencies.

Keywords: cyberspace, Darknet, "digital opposition", political, power, hacktivism

For citation: Yakovlev, M.V. (2022). Darknet and the political. *RUDN Journal of Political Science,* 24(3), 408–418. (In Russian). https://doi.org/10.22363/2313-1438-2022-24-3-408-418

Acknowledgements: The study is supported by the Interdisciplinary Scientific and Educational School of Moscow University "Preservation of the world cultural and historical heritage".

Введение

Даркнет («Темная сеть», Dark web) стал большим участком кибепространства, где скрытно группируются и набирают мощь разного рода силы, которые осуществляют экспансию в открытом сегменте интернета и пытаются повлиять на повестку дня и процесс принятия политико-государственных решений. Наиболее известными примерами служат действия LulzSec, Anonymous и других сетевых групп. Ресурсы Даркнета используют и правительства многих стран для оказания политического давления и ведения кибервойн. Эти обстоятельства довольно давно привлекают большое внимание ученых по всему миру. В последнее время они попали в поле зрения и отечественных исследователей: на сегодняшний день в базе данных Elibrary содержится более 160 касающихся Даркнета научных публикаций

на русском языке [Александров, Сафронов 2021; Арчаков, Баньковский, Зенченко 2021; Жмуров 2020]. Подавляющее их большинство выдержано в негативном ключе, посвящено проблемам безопасности государства, а также юридическим аспектам использования данных и уголовным преступлениям.

Обзор материалов показывает изрядную неразбериху с определением Даркнета (его путают с «Глубоким интернетом», ошибочно называют сайтом и т.д.). Также имеется большое количество заблуждений о структуре и характере этой сети.

Цель и методы

В связи с недостатком точных и достоверных знаний о текущем статусе Даркнета в политике ставится цель определить концептуальную рамку для его аналитического рассмотрения и выявить его актуальное место и перспективы в политической деятельности.

Для достижения цели проводится сравнительно-исторический анализ, который позволяет определить причины и время политического рождения Даркнета; для общей характеристики его функционирования в политическом измерении и для выявления его политического значения как структурной единицы делаются контент-анализ его ресурсов и системный анализ; уточняется понятийно-категориальный аппарат исследования.

Даркнет как структурная единица киберпространства

В сугубо технической интерпретации Даркнет — это общее название для одноранговых (P2P) компьютерных сетей (даркнетов), располагающих собственными псевдодоменами верхнего уровня (onion, i2p, freenet и др.), доступ в которые возможен (если они, конечно, не полностью изолированы) только посредством особого программного обеспечения, специальной авторизации, нестандартных протоколов и портов [Mansfield-Devine 2009].

Как следует из приведенного определения, Даркнет имеет две специфики. Во-первых, его узлы равны друг другу, каждый из них одновременно может являться и клиентом, и сервером, при этом выделенные серверы часто отсутствуют. Во-вторых, его сетевой протокол основан на многократном независимом шифровании и маршрутизации по нескольким случайно выбранным узлам (прокси-серверам), что позволяет скрыть («затемнить») личность пользователей, местоположение узлов и контента, в отличие от Видимой сети. Именно так выстроена архитектура анонимной прокси-сети с анонимизированным соединением TOR (имеет одноименный браузер и развивается некоммерческой организацией с тем же названием). Другими наиболее известными примерами являются I2P (проект «Невидимый Интернет») и Freenet. Эти аппаратно-программные конфигурации располагаются в третьем секторе Всемирной сети (как TOR), после Видимой сети (Surface web — часть, контент которой находится в общем доступе и обрабатывается поисковыми машинами) и Глубокой сети (Deep web — сегмент, содержание которого закрыто и не индексируется поисковиками) [Devine, Egger-

Sider 2021; Hamilton 2003], или поверх Всемирной сети (как I2P). Хотя некоторые авторы полагают, что Даркнет входит в состав Глубокой сети, однако это не совсем верно, так как для подключения к Глубокой сети не требуются специальные программные средства, чего нельзя сказать о Даркнете.

Таким образом, предикат «Dark» («Темная»), который напугал общественность и мистифицировал эту сеть (точнее, группу сетей под общим названием), на поверку оказывается не определением правового статуса ее информационного содержания и клиентов, а является ее метафорической технической характеристикой.

В одной из первопроходческих работ по Даркнету определяются три базовых положения его функционирования: доступность любого объекта для широкого распространения, возможность свободного копирования любого объекта, высокоскоростное соединение [Biddle, England, Peinado, Willman 2002]. Очевидно, что речь здесь идет о файлообменниках, отделенных от сетей общего доступа. Действительно, даркнеты был задуманы и построены именно таковыми в 1970-е гг.

Политизация Даркнета

Задачу обособленного файлового обмена даркнеты выполняли на протяжении 1980-х и начала 1990-х гг. — в период бурного саморазвития интернета, архитектуру которого создавали главным образом независимые добровольцы-программисты и продвинутые пользователи, руководствовавшиеся принципами свободы, открытого исходного кода, бескорыстного обмена знаниями, технического совершенствования для общественного прогресса, что обстоятельно описано в литературе [Кастельс 2004: 22-50].

С начала 2000-х гг. значение Даркнета начинает меняться. Причину этого можно определить с помощью сравнительно-исторического метода, который демонстрирует связь между трансформацией Даркнета (увеличением его политического потенциала) и расширением государственного контроля и слежки в Видимой сети. Так, по мере роста интернет-экспансии государства, даркнеты превращаются в наполненные разнообразными ресурсами зашифрованные участки киберпространства, функционирующие на основе полной конфиденциальности. Сравнительно-исторический метод помогает определить время полноценного вхождения Даркнета в политическую реальность — около 2010 г. Точная дата обсуждается, однако именно в 2010 г. политические активисты «Арабской весны» начали массово и постоянно использовать TOR для общения по социально значимым вопросам, протестной самоорганизации, а также безопасного информирования с целью содействовать демократизации и для увеличения степени влияния общественности на консолидированные автократии.

К 2012 г. на арене мировой политики в качестве самостоятельного актора прочно утвердилось использующее Даркнет международное движение хактивистов, которое объединяет политически активных хакеров, с конца 1990-х гг. распространяющих свои идеи и послания и привлекающих единомышленников посредством взлома веб-сайтов, DDoS-атак, кражи информации для последующего ее обнародования, путем организации саботажа, забастовок, бой-

котов во Всемирной сети и т. д. Подтверждением этого стало включение одной из групп Anonymous в список ста наиболее влиятельных людей года по версии журнала Time. Так, хактивисты Anonymous обрушили сайты Федерального бюро расследований США, Администрации Президента США, Министерства юстиции США и ряда звукозаписывающих компаний в рамках акции против закрытия ресурса MegaUpload.com, совершили DDoS-атаку на портал Европарламента в знак протеста против после вступления правительства Польши в Торговое соглашение по борьбе с контрафактом в 2012 г. Тогда же широкую известность приобрела политически мотивированная деятельность LulzSec, которая атаковала интернет-ресурсы Сената США, ЦРУ, Агентства по раскрытию тяжких преступлений и борьбе с организованной преступностью Великобритании и др. В 2013 г. интерес к Даркнету резко возрос в связи с разоблачением Э. Сноуденом массовой слежки за гражданами: информация об американской системе шпионажа PRISM была передана в редакции The Guardian и Washington Post через сеть TOR. Последняя, кстати, была создана исследовательскими подразделениями Министерства обороны США и получает существенное финансирование от Государственного департамента США.

Итак, давление государств, естественным образом стремящихся к поддержанию своих систем доминирования в киберпространстве (в первую очередь в национальных доменных зонах), на привыкшее мыслить себя свободным и независимым интернет-сообщество породило в последнем сильное недовольство, быстро переросшее в сопротивление. В соответствии с общественным запросом инфраструктура и база даркнетов стремительно эволюционировали, они на очень высоком уровне начали предоставлять собственную DNS (систему доменных имен) для конфиденциального размещения контента и создания зеркал сайтов. Так, в I2P появились возможности расположить любые интернет-службы (чаты, блоги, форумы, IP-телефония, IP-телевидение, электронную почту, файловый хостинг, потоковые сервисы и др.), создать платформу (открытую или приватную), построить другие одноранговые сети (файлообменники BitTorrent, eDonkey и др.). В свою очередь, TOR позволил анонимно посещать сайты, в том числе заблокированные, вести блоги, обмениваться данными в Видимой сети, а его скрытый функционал дал возможность, как и в I2P, создавать собственные интернет-ресурсы, сохраняя втайне их местоположение и их владельцев. На его базе сегодня работают Electronic Frontier Foundation (Фонд электронных рубежей — американская некоммерческая организация по защите прав пользователей в интернете), Strongbox (служба приема компромата издания The New Yorker), MafiaLeaks (база данных об итальянской мафии), Indymedia (информационная сеть альтерглобалистов), ProPublica (сайт независимой журналистики расследований) и др. Эти сервисы используют как внесистемные силы, так и государство и системные медиа.

Отдельно стоит отметить форумы наподобие DWF, Raid, Dread, Nulled, 4chan (стал известен после атаки на Капитолий сторонников конспирологически настроенных активистов Qanon в 2020 г.), служащие площадками для политически активных пользователей и хактивистов.

В наши дни политическое значение Даркнета повышается, он становится все более значительным феноменом политической реальности. Так, группирующиеся на его базе хактивисты Anonymous вывели из строя сайты «ТАСС», «Известия», «Коммерсант», Forbes, «РБК» 28 февраля 2022 г. в ходе кибервойны, объявленной российской системе власти, и др. По словам вице-премьера, министра цифровой трансформации Украины, правительство этой страны посредством Telegram организовало «более 660 хакерских атак против российских и белорусских предприятий и учреждений», которые были выполнены анонимными добровольцами-хактивистами[1]. Сам Telegram, точнее появившийся в 2019 проект Telegram open network, включающий в себя основанную на блокчейне одноранговую сеть и оснащенную прокси и анонимайзером платформу, становится влиятельным и заметным ресурсом Даркнета. С ним связано движение Digital Resistance («Цифровое сопротивление»), созданное П. Дуровым 16 апреля 2018 г. в ответ на блокировку мессенджера в России для защиты «цифровых свобод и прогресса по всему миру»[2].

Одним из важнейших факторов развития Даркнета как действительно важного социально-политического явления является обращение криптовалюты. Последняя предстает одним из наиболее существенных вызовов для современного государства, чей суверенитет во многом держится на монопольном праве денежной эмиссии.

Контент-анализ сайтов современного Даркнета [Moore, Rid 2016; Tzanetakis 2017] позволяет опровергнуть широко распространенное мнение о его преимущественно криминальной направленности. Исследования определенно указывают, что темы оружия, наркотиков, компьютерных взломов не являются определяющими и первостепенными в Даркнете. Например, рассмотрение 13 600 страниц в TOR показало, что 52 % контента можно классифицировать как легальный, согласно законодательствам Великобритании и США. Удельный вес сайтов, на которых продаются наркотики и оружие, составил соответственно 4 и 0,3 %. Около трети ресурсов — это сервисы по обмену файлами. Содержание другой трети сайтов — это данные, изъятые из закрытых баз. 12 % сайтов связаны с финансовыми махинациями[3]. Другое исследование демонстрирует в общих чертах схожие результаты. Из проанализированной выборки в 2 723 сайтов сети TOR 43 % их оказались законными, среди оставшихся 15 % связаны с торговлей и потреблением наркотиков 12 % — с финансами, 7 % — с прочими нарушениями, 1,5 % — с оружием [Moore, Rid 2016; Tzanetakis 2017]. Хотя две этих работы различаются и по объему генеральной совокупности (в первой рассматриваются все найденные

[1] На Украине заявили об организации 660 хакерских атак против компаний России и Белоруссии. URL: https://tass.ru/mezhdunarodnaya-panorama/14488235 (дата обращения: 02.05.2022).

[2] «Цифровое сопротивление» Павла Дурова. URL: https://www.iguides.ru/main/other/tsifrovoe_soprotivlenie_pavla_durova/ (дата обращения: 02.05.2022).

[3] Deeplight: shining a light on the Dark Web. An Intelliagg report. 2016. URL: http:// onyxcomms.com/wp-content/uploads/2017/01/intelliagg-deeplight-report.pdf+&cd=1&hl=ru&ct=clnk&gl=ru (accessed: 11.04.2022).

и функционирующие интернет-страницы, во второй — лишь часть сайтов), и по поставленным задачам, однако обе они рассеивают предрассудки и позволяют заключить о том, что Даркнет не является исключительно кибер-гетто.

Эскиз теоретического разъяснения

Аналитическое рассмотрение Даркнета в политическом измерении требует особой концептуальной призмы. Ряд базовых аспектов теоретического исследования политического измерения Даркнета заложили М. Кастельс и некоторые другие авторы, которые сформулировали несколько основоположений о власти и контрвласти в сетевом обществе. Во-первых, современные конфликты представляют собой борьбу среди связанных сетью акторов, привлекающих и мобилизующих сторонников с помощью мультимедийного общения. Во-вторых, изменение доминирования власти и сопротивление этому доминированию в современных условиях основаны на «сетевой конструкции и сетевых стратегиях нападения и защиты». В-третьих, сопротивление власти осуществляется посредством аналогичных механизмов, что и установление самой власти в сети, а именно при помощи «программы сетей» (точнее, путем введения новых команд и новых кодов) и «переключения между сетями». При этом наиболее радикальная стратегия предполагает полную замену основополагающих принципов сети («ядра программного кода») [Кастельс 2016: 66-68].

Р. Гель предложил оригинальную и применимую к Даркнету (и вообще ко всем политическим институтам и процессам в Сети) трактовку власти как системы наблюдения, слежения, алгоритмического регулирования и ограничения архитектуры (структуры сети, состоящей из аппаратных и программных компонентов) [Gehl 2016].

Дж. Аркилла и Д. Ронфельдт ввели в оборот концепт нополитика, который обозначает стратегию, охватывающую киберпространство и все информационные системы (включая медиа) [Arquilla, Ronfeldt 1999], направленную на установление и/или поддержание гегемонии.

Применение этих положений для обобщения эмпирических фактов (политических событий), связанных с функционированием Даркнета, позволяет прийти к следующим результатам.

Длительное время (1980–1990-е гг.) интернет создавался добровольцами-программистами и продвинутыми пользователями как свободная среда технико-технологических новаций и творческого обмена данными без ограничений, надзора, принуждения. Внедрение государственного надзора и контроля в эту среду вызвало недовольство среди большого числа тех, кто непосредственно участвовал в ее формировании в соответствии со своими интересами и ценностями. Дальнейшее введение ограничений и давление на интернет-сообщество по всему миру усилило это недовольство и породило сопротивление, которое в силу своей интенсивности обрело политическую окраску. Вспомним, что согласно К. Шмитту политическое возникает в случае конфликтного разделения на группы «друг/враг» и выраженного острого противостояния по какому-либо общественно значимому вопросу [Шмитт 2016:

301, 305, 312]. Впоследствии связанные сетью несогласные объединились в «цифровое сопротивление» и ушли в современное подполье — Даркнет. В ходе их противостояния с государством как системой власти и доминирования (и состоящими в союзе с ним корпорациями, извлекающими прибыль из монопольного производства и распространения информацинно-технологической и медиапродукции) сформировались сетевые группы наподобие Anonymous и LulzSec, использующие базу и средства Даркнета для реализации сетевой защиты и продвижения своих интересов, подпитываемые идеями криптоанархизма, инфоанархизма и других концепций анархизма. Со стороны государств последовали ответы в виде преследований хакеров-активистов, блокировок ресурсов, замедлений трафика, построения мощных файрволов (программно-аппаратных комплексов, обеспечивающих фильтрацию и блокировку интернет-трафика), ограничивающих нормативных правовых актов и т.п. Одновременно с этим государства в рамках ноополитики начали мощную информационную кампанию, в которой под лозунгом борьбы за безопасность осуществляется постепенная смена основополагающих принципов Сети, а именно — замещение некогда преобладавших установок на добровольность, бескорыстное участие, свободный доступ к общественно ценной и значимой информации (включая научные тексты, произведения литературы, музыки, живописи и пр.), открытый исходный код и т.д. ориентацией на аутентификацию, шифрование, платный доступ к контенту. Эту пропагандистскую кампанию активно поддержали корпорации (медиаконгломераты), в коммерческих интересах продвигающие законодательство о защите прав на создание и использование разного рода произведений (Copyright).

Выводы

На основе изложенного можно заключить, что первопричиной политизации и трансформации Даркнета стала естественная устремленность государств к суверенному контролю над киберпространством. Экспансия систем власти и доминирования в интернете обусловила реакцию его пользователей, придерживающихся установок на конфиденциальность, свободный доступ, открытость социально значимых данных и исходного кода, побудила программистов к созданию собственного «цифрового бастиона» в виде Даркнета, а также инициировала «цифровое сопротивление» хактивистов и сочувствующих. Побочным эффектом этого процесса стало внедрение в Даркнет криминального элемента.

Вряд ли будет преувеличением утверждение о том, что в настоящее время в рамках Даркнета последовательно выстраивается порядок, в котором государство и корпорации не играют заметной роли (что их весьма беспокоит, так как подрывает суверенитет первых и угрожает монопольному положению вторых в деле извлечения прибыли из информационной деятельности). Возможно, мы наблюдаем за становлением абсолютно новой социальной и технической системы (в которой пользователи Даркнета — социальная часть, а сам Даркнет — техническая), находящейся вне сферы международного и государственного права, в которой все отношения осуществляются добровольно и посредством частных соглашений, где на основе криптовалют сформирована альтернативная

мировая платежная система и пользователи пребывают не в гражданском состоянии, а в естественном (выражаясь в терминах И. Канта и Дж. Локка).

С одной стороны, развитие Даркнета является серьезным вызовом для современных систем власти (особенно автократических) и корпораций, подрывающим их суверенитет и монопольное положение. При этом следует помнить, что сами государства используют Даркнет для ведения кибервойн как посредством кибервойск, так и через наемников. С другой стороны, Даркнет позволяет пользователям и заинтересованным группам действовать свободно, независимо, конфиденциально, участвовать в общественно-политических переговорах и массовых собраниях даже в тех случаях, когда таковые фактически запрещены.

Сейчас становится все более ясной траектория развития Даркнета как интенсивно формирующейся независимой международной среды для тайного и приватного общения, в том числе по имеющим государственную и политическую важность вопросам. На его базе не только наращивается потенциал сопротивления государствам как системам власти и доминирования, но и может наметиться своеобразная (виртуальная) альтернатива им в будущем.

Поступила в редакцию / Received: 11.03.2022
Доработана после рецензирования / Revised: 10.06.2022
Принята к публикации / Accepted: 15.06.2022

Библиографический список

Александров А.Г., Сафронов А.А. Использование сети Даркнет при подготовке и совершении преступлений // Вестник Санкт-Петербургского университета МВД России. 2021. № 1. С. 156–160.

Арчаков В.Ю., Баньковский А.Л., Зенченко Е.В. Даркнет в контексте рисков национальной безопасности // Право.by. 2021. № 6. С. 5–10.

Бартлетт Дж. Подпольный интернет: темная сторона мировой паутины. М.: Эксмо, 2017. 352 с.

Билтон Н. Киберпреступник № 1. История создателя подпольной сетевой империи. М.: Эксмо, 2017.

Бронников И.А. Самоорганизация граждан в эпоху цифровых коммуникаций // Контуры глобальных трансформаций: политика, экономика, право. 2020. № 2. Т. 13. С. 269–285.

Жмуров Д.В. Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1. С. 89–98.

Кастельс М. Власть коммуникации. М.: Изд. Дом Высшей школы экономики, 2016.

Кастельс М. Галактика Интернет: Размышление об Интернете, бизнесе и обществе. Екатеринбург: У-фактория, 2004. 328 с.

Пучков О.А. Мотивация действий хакеров в современной цифровой среде: междисциплинарный подход // Проблемы современного педагогического образования. 2020. Т. 67, № 3. С. 306–309.

Тормошева В.С. Политическая активность аудитории Постмодерна: коммуникативный аспект // Via in Tempore. История. Политология. 2020. № 3. Т. 47. С. 647–657.

Чернышев Р.С., Рашкован А.А. Киберпространство — новая сфера военных действий в международных отношениях // Этносоциум и межнациональная культура. 2021. № 3. С. 134–159.

Шмитт К. Понятие политического. СПб.: Наука, 2016.
Acar H., Pekcandanoglu M. Analysis of Russia's cyber security and cyber espionage policies // Turkish Journal of Russian Studies. 2020. No. 3. P. 167–189.
Anjum A., Kaur Ch., Kondapalli S., Hussain M. A Mysterious and Darkside of The Darknet: A Qualitative Study // Webology. 2021. Vol 18, no 4. P. 285–294
Arquilla J., Ronfeldt D. The Emergence of Noopolitik. Toward An American Information Strategy. RAND Corporarion, 1999.
Bachrach P., Baratz M.S. The two faces of power // American political science review. 1962. No. 56. P. 947–952.
Biddle P., England P., Peinado M., Willman B. The Darknet and the Future of Content Distribution // Microsoft Corporation. The Wyndham City Center Washington DC: ACM Workshop on Digital Rights Management, 2002.
Devine J., Egger-Sider F. Beyond Google: The invisible web in the academic library // The Journal of Academic Librarianship. 2021. Vol. 30, no 4. P. 265–269.
Gayard L. Darknet: Geopolitics and Uses. Hoboken, NJ: John Wiley & Sons, 2018.
Gehl R.W. Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network // New Media and Society. 2016. Vol. 18, no. 7. P. 1219–1235.
Hamilton N. The mechanics of a Deep Net Metasearch Engine // Proceedings of the 12th International World Wide Web Conference. Budapest, 2003.
Mansfield-Devine S. Darknets // Computer Fraud & Security. 2009. Vol. 12. P. 4–6.
Moore D., Rid T. Cryptopolitik and the Darknet // Survival. 2016. Vol. 57, no. 1. P. 7–38.
Tzanetakis M. The Darknet's anonymity dilemma // Encore. The Annual Magazine on Internet and Society Research. 2017. P. 118–125.
Wood J. The Darknet: A Digital Copyright Revolution // XVI Rich. J.L. & Tech. 2010. Vol. 14. URL: http://jolt.richmond.edu/v16i4/article14.pdf (accessed: 11.04.2022 г.).
Zakariye M.O., Jamaluddin I. An Overview of Darknet, Rise and Challenges and Its Assumptions // International Journal of Computer Science and Information Technology. 2020. Vol. 8. Issue 3. P. 110–116.

References

Acar, H., & Pekcandanoglu, M. (2020). Analysis of Russia's cyber security and cyber espionage policies. *Turkish journal of Russian studies*, (3), 167–189.
Alexandrov, A.G., & Safronov, A.A. (2021). Use of Darknet to prepare and commit crimes. *Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia*, 1(89), 156–160. (In Russian).
Anjum, A., Kaur, Ch., Kondapalli, S., & Hussain, M. (2021). A Mysterious and Darkside of The Darknet: A Qualitative Study. *Webology*, 18(4), 285–294.
Archakov, V. Yu., Makarov, O.S., & Bankowski, A.L. (2021). Darknet in the context of national security risks. *Pravo.by*, (6), 5–10. (In Russian).
Arquilla, J., & Ronfeldt, D. (1999). *The Emergence of Noopolitik. Toward An American Information Strategy.* RAND Corporation.
Bachrach, P. & Baratz, M.S. (1962). The two faces of power. *American political science review,* 56, 947–952.
Bartlett, J. (2017). *Underground Internet: the dark side of the World Wide Web*. Moscow: Eksmo. (In Russian). [Bartlett, J. (2014). *The Dark Net: Inside the Digital Underworld.* William Heinemann Publishing.]
Biddle, P., England, P., Peinado, M., & Willman, B. (2002). *The Darknet and the Future of Content Distribution.* Microsoft Corporation. The Wyndham City Center Washington DC: ACM Workshop on Digital Rights Management.

Bilton, N. (2017). *Cybercriminal No. 1. The history of the creator of the underground network empire*. Moscow: Eksmo. [Bilton, N. (2017). *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road*]

Bronnikov, I.A. (2020). Self-organization of Citizens in the Age of Digital Communications. *Outlines of global transformations: politics, economics, law.* 13(2), 269–285. https://doi.org/10.23932/2542-0240-2020-13-2-14 (In Russian).

Castells, M. (2004). *The Internet Galaxy: Reflection on the Internet, Business and Society*. Yekaterinburg: U-factoriya. (In Russian). [Castells, M. (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society.* https://doi.org/10.2307/40252194]

Castells, M. (2016). *Communication Power*. Moscow: HSE Publising House. (In Russian). [Castells, M. (2009). *Communication Power*. Oxford University Press]

Chernyshev, R.S., & Rashkovan, A.A. (2021). Cyberspace — a new sphere of military operations in international relations. *Ethnosocium and interethnic culture*, 3, 134–159. (In Russian).

Devine, J., & Egger-Sider, F. (2021). Beyond Google: The invisible web in the academic library. *The Journal of Academic Librarianship*, 30(4), 265–269.

Gayard, L. (2018). *Darknet: Geopolitics and Uses*. Hoboken, NJ: John Wiley & Sons.

Gehl, R.W. (2016). Power/freedom on the Dark Web: A digital ethnography of the Dark Web social network. *New Media and Society*, 18(7), 1219–1235.

Hamilton, N. (2003). The Mechanics of a Deep Net Metasearch Engine. *Proceedings of the IADIS International Conference on e-Society*, 1034–1036.

Mansfield-Devine, S. (2009). Darknets. *Computer Fraud & Security*, 12, 4–6.

Moore, D. & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 57(1), 7–38.

Puchkov, O.A. (2020). Motivation of hackers' actions in the modern digital environment: an interdisciplinary approach. *Problems of modern pedagogical education*, 67(3), 306–309. (In Russian).

Schmitt, C. (2016). *The concept of the political*. St. Petersburg: Nauka. (In Russian). [Schmitt, C. (1932). *The concept of the political*]

Tormosheva, V.S. (2020). Political activity of the postmodern audience: the communicative aspect. *Via in Tempore. History and Political Science*, 47(3), 647–657. (In Russian).

Tzanetakis, M. (2017). The Darknet's anonymity dilemma. *Encore. The Annual Magazine on Internet and Society Research,*118-125.

Wood, J. (2010). The Darknet: A Digital Copyright Revolution. *XVI Rich. J.L. & Tech. 14*. URL: http://jolt.richmond.edu/v16i4/article14.pdf (accessed: 04.05.2022).

Zakariye, M.O., & Jamaluddin, I. (2020). An Overview of Darknet, Rise and Challenges and Its Assumptions. *International Journal of Computer Science and Information Technology*, 8(3), 110–116.

Zhmurov, D.V. (2020). Darknet as an elusive sphere of legal regulation. *Siberian Criminal Process and Criminalistic Readings*, (1), 89–98. (In Russian).

Сведения об авторе:

Яковлев Максим Владимирович — доктор политических наук, профессор кафедры философии политики и права философского факультета Московского государственного университета имени М.В. Ломоносова (e-mail: maxvuz@mail.ru) (ORCID: 0000-0002-0127-5642)

About the author:

Maksim V. Yakovlev — Doctor of Political Science, Professor of the Department of Philosophy of Politics and Law, Lomonosov Moscow State University (e-mail: maxvuz@mail.ru) (ORCID: 0000-0002-0127-5642)