DOI 10.35775/PSI.2022.83.7.029
УДК 327.7

И.А. КИШУЕВА
аспирант кафедры зарубежного регионоведения
и внешней политики РГГУ,
Россия, г. Москва

РАЗВЕДКА С ОТКРЫТЫМ КОДОМ КАК ИНСТРУМЕНТ ЦИФРОВОГО ВЗАИМОДЕЙСТВИЯ В ДИНАМИКЕ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

Предметом настоящей статьи является разведка с открытым кодом (англ.: OSINT (Open-Source Intelligence)), применяемая в качестве набора инструментов политической коммуникации в меняющемся ландшафте международных отношений. Материально методическая база исследования включает широкий спектр данных и верифицированных источников для формирования всестороннего представления о механизме реализации, сопутствующих рисках дифференцированных правительственных систем и релевантности, технологий разведки с открытым кодом текущим задачам межгосударственного взаимодействия.

В данной работе последовательно конкретизируется предметная структура цифровых технологий на основе, разработанной корпорацией RAND, графической репрезентации элементов методологического цикла OSINT. Системный анализ отражает корреляцию институциональных образований, задействованных в механизме аккумуляции и фильтрации данных. Практические примеры, приводимые в исследовании, иллюстрируют положительные и нежелательные тенденции, в ходе развития технологий цифровой разведки с открытым кодом. Концептуальный анализ западного и восточного подходов к регуляции сферы цифровой коммуникации позволяет идентифицировать области расхождения элементов, детерминирующих структуру международных отношений. В результате исследования предоставлена актуальная характеристика OSINT в текущей международной повестке; выработаны направления по смягчению рисков и эффективному использованию технологий цифровой разведки отрытых данных.

Ключевые слова: *OSINT, цифровая коммуникация, международные отношения, многостороннее управление, цифровой конституционализм.*

Введение. С вовлечением множества заинтересованных сторон в межгосударственное взаимодействие ООН и Совета Европы, парадигма

международных отношений уверенно движется к горизонтальной системе управления. Развитие коммуникационных технологий последних десятилетий, играет ключевую роль в направлении этого процесса. Технологии гражданской интеракции стали инструментом утверждения власти существующих МНПО, как фундаментальных институтов общественного контроля, требующих слияния и синхронизации форм государственного управления.

Тематические форумы все чаще становятся посреднической площадкой для реализации политических целей и взаимодействия с аудиторией, с последующей ретрансляцией в глобальной сети. Благодаря скоростному росту технологий, позволяющим находить, создавать и распространять информацию и формировать реальность, экспоненциально увеличивается количество и качество исследований, на основе открытых данных. Организации по всему миру объединяют профессионалов в смежных областях и развивают технологии разведки с открытым кодом (далее по тексту – OSINT). В условиях проницаемости информационных границ, OSINT используется как модифицируемый инструмент межправительственного взаимодействия.

В исходном понимании OSINT определяется как обособленный инструмент государственной информационной операции, призванный сократить издержки традиционной разведки. Инструкция Справочника НАТО по разведке из открытых источников, датируемая 2002-м годом гласит, что «при систематическом применении продукты OSINT могут снизить потребность в секретных ресурсах для сбора разведданных, ограничивая запросы информации только теми вопросами, на которые нельзя ответить из открытых источников» [30].

В процессе освоения правительственной прерогативы на эксклюзивный доступ к разведданным, преимуществом таких систем становится высокий уровень аутентификации, с одновременным охватом различных источников информации в формируемой посредствам ИКТ аудитории. Что привело к эволюции инструмента и его функционала.

Закон США о национальной обороне от 2006 года определяет OSINT как «разведывательные данные, полученные из общедоступной информации, которые собираются, используются и своевременно распространяются среди соответствующей аудитории с целью удовлетворения конкретных требований разведки» [8].

Исследователь Бенеш Либор констатирует революционность технологий последних десятилетий в соответствии с критериями научных революций Томаса Куна и определяет OSINT как «часть огромного массива данных, который ежедневно распространяется и передается, может считаться актуальной, своевременной и полезной для аналитика» [14. С. 22-37].

Задачи исследования охватывают:

– анализ системы и функционала OSINT на современном этапе развития цифровых технологий;

– актуализация предмета анализа, выявление существующих и потенциальных угроз, связанных с использованием арсенала OSINT неправительственными участниками международных отношений;

– сопоставление отечественного и зарубежного стратегического инструментария по регуляции институциональной сферы приложения OSINT;

– выработка заключений и перспектив развития роли цифровой разведки в фокусе системообразующих факторов глобальной политической коммуникации.

Основная часть. Анализ открытых данных, традиционно проводимый новостными и информационными агентствами с использованием культурных, социальных и дипломатических каналов, сегодня все больше опирается на высокие технологии в области Земли и космической инфраструктуры (Maxar Technologies, Vricon, Inc., PlanetScope), спутниковых изображений высокого разрешения (Capella Space Synthetic Aperture Radar), картографических данных (OpenStreetMap), широковещательных служб авиации (ADS-B Exchange, Flightradar24) и других служб геопространственного дистанционного зондирования, а также системы мониторинга сферы ИКТ (кроссплатформенные репозитории (OSINT Framework, sub3suite), инструменты графического анализа (Maltego), структурирования данных (IBM SPSS Modeler)).

Консолидация материалов для построения первичных систем знаний производится путем извлечения информации из социальных сетей, блогов, форумов, общественных баз, данных сотовых операторов, бизнеса, городской инфраструктуры, интернет-рынков, криптовалют и блокчейн, судебных материалов и правовых актов, веб-аналитики, веб-мониторинга, средств сопоставления и обработки данных, академических ресурсов и неофициальной литературы и пр.

Анализ RAND посвященный переосмыслению OSINT второго поколения как разведывательной дисциплины приводит методологический цикл, состоящий из получения, проверки, определения ценности и презентации результата.

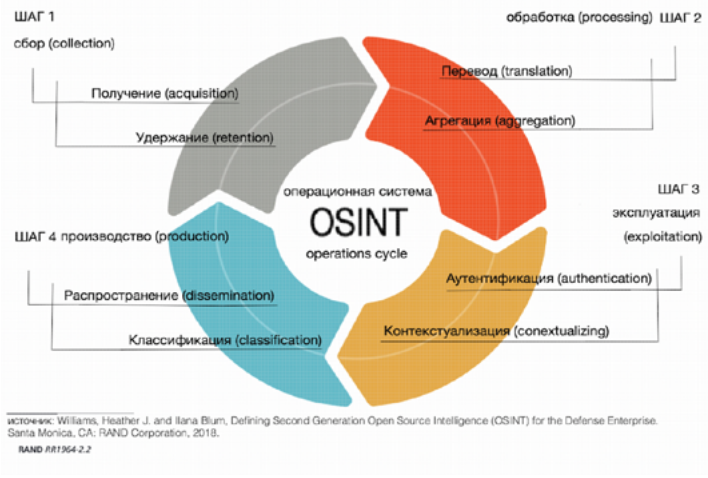

Рисунок 1. Операционная система OSINT

Компоненты данных распределяются по спектру компликации от наиболее простых источников данных – СМИ, серой литературы, полноформатного мультиплатформенного освещения к сложным социальным сетям [32. С. 13-18].

Цифровизация разведки опирается на классическую сетевую модель коммуникации – систему интеграции и возвращения критически важной информации через диверсифицированные каналы из целевой аудитории и обратно. Расширение каналов связи ставит задачу обработки больших объемов данных, посредствам аутсорсинга и разработки механизмов верификации и атрибуции.

Специализированные ресурсы сбора и интерпретации данных широко представлены международными неправительственными организациями и реализуются сетями журналистов-расследователей (Центр по исследованию коррупции и организованной преступности (Organized Crime and Corruption Reporting Project (OCCRP)); Transparency International; Международный консорциум журналистов-расследователей (International Consortium of Investigative Journalists (ICIJ)); Глобальная сеть журналистов-расследователей (Global Investigative Journalism Network (GIJN)); Международный центр журналистов (International Center for Journalists (ICFJ)); Сеть журналистов-расследователей в Восточной и Юго-Восточной Европе (Network for investigative journalists in East and Southeastern Europe (SCOOP) и др.).

OSINT охватывает растущий класс профессионалов в таких областях, как журналистика, кибер-безопасность, юриспруденция, социальные науки, инвестиционные исследования, антикризисное управление и права человека

и пр. Для удовлетворения потребностей такого широкого круга исследователей производится неограниченный объем инструментов экстрадиции и трансформации данных.

Справочник i-intelligence по ресурсам OSINT в общественных (surface), глубоких (deep web), и теневых сетях (darknet) содержит тысячи директорий, исчерпывающее исчисление которых, в виду беспрерывной многопользовательской генерации, не представляется возможным [4].

Наряду с положительными аспектами, технология OSINT сталкивается с вызовами, затрагивающими социальные коммуникации в целом. Низкий порог доступа окупается ростом популярности инструментов среди акторов, намеренно или неумышленно допускающих неточности в процессе сбора и сопоставления информации. Свойственные СМИ, популярные в блогосфере методы манипуляции нарративом обогащаются средствами OSINT, с одной стороны упрощая цели пропаганды, с другой – перенасыщая информационное поле неконструктивной коммуникацией и подрывая доверие к самому жанру аналитической журналистики.

Вследствие широкого распространения резонансных материалов и общественного запроса на квалифицированную обработку массива информации, в геометрической прогрессии множатся публикации имитирующие профессиональные работы.

Зачастую сотрудничество с правительством неизбежно для беспрепятственного доступа к ресурсам и технологиям. Опасные условия труда, сложности финансирования и необходимость компромиссов с властью – составляющие кризиса СМИ и также ограничивают расследовательскую журналистику.

Правительства и организации (от масштабных наднациональных корпораций до небольших общественных союзов) избегают раскрытия аспектов своей деятельности, ведущих к репутационным издержкам, что, стоит заметить, справедливо не только в отношении авторитарных правительств и государств с переходной демократией.

Согласно Индексу финансовой секретности (Financial Secrecy Index (FSI)) от Tax Justice Network, по шкале закрытости финансовых юрисдикций и их влияния на глобальные финансовые потоки, США, Великобритания, Люксембург, Германия, Швейцария и Нидерланды занимают первые строки рейтинга в качественном и количественном соотношении [10].

Несмотря на высокое положение в Индексе восприятия коррупции с коррелирующим уровнем демократии западных государств, Глобальная антикоррупционная сеть в постоянной рубрике «Trouble at the Top» указывает на существенные недостатки в области финансового сектора «образцовых» стран [19].

Неблагоприятной тенденцией, характерной для киберпространства, является необходимость постоянного совершенствования навыков,

что способствует соответствующему росту технологий маскировки и сокрытия общественно значимой информации.

Достоверность подаваемой информации – ключевой аспект в борьбе за внимание в перенасыщенном поле ИКТ, в среде многовекторных ложных сообщений бремя доказательств возлагается на журналистов-фактчекеров. Информационный шторм, образующийся вокруг масштабных событий, повышает ресурсоемкость и скорость обработки больших данных, что безусловно отражается на стоимости извлечения эффективных материалов. Необработанная информация включает огромное количество записей, которые собираются с использованием технических средств для выявления взаимодействий или сообщений, представляющих критический интерес.

В области кибербезопасности OSINT – одна из наиболее противоречивых тем [18. С. 68-86]. По мере того, как информация в Интернете становится все более защищенной, благодаря доступности и распространению технологий шифрования, репортеры OSINT прибегают к альтернативным источникам и изощренным путям поиска и распространения информации.

Вместе с тем, регулярные нарушения стандартов прозрачности со стороны компаний, непосредственно формирующих сетевое пространство, вызывают наибольшую обеспокоенность.

Отголоски скандала с данными Facebook и Cambridge Analytica не стихают по прошествии лет [2]. И, несмотря на предпринимаемые меры, сегодня практически каждый пользователь сталкивается с риском скрытого отслеживания со стороны разработчиков и передачи данных третьим лицам. Доступ к платформам в глобальной сети несет собой издержки – владельцы не всегда обладают информацией о целях и конечных назначений данных, представляющих ценность как для рыночных рекламодателей, так и для политических кампаний по манипуляции мнением.

В большинстве случаев, остается надеяться, что персональные данные, попадающие под защиту от третьих лиц, сохраняют конфиденциальность. При этом публичные индивидуальные характеристики, которыми пользователи делятся в социальных сетях не менее ценны для исследователей. Такая информация активно используется в качестве материалов OSINT, решающее значение играют целеполагания и субъективные стандарты этики акторов, собирающих психометрические показания в массовом порядке.

Стратегии противодействия так называемым «плохим акторам» в Интернете продолжают разрабатываться и совершенствоваться. Несмотря на то, что технологии остаются частью проблемы OSINT, они так же предоставляют решения [27]. Множества алгоритмов машинного и ручного способа маркировки вводящей в заблуждение информации реализованы как на базе платформ и официальных расширений браузеров, так и правительственными и неправительственными кампаниями по защите

общественных интересов. В большинстве случаев противодействие злонамеренной информации производится путем привлечения и обучения пользователей.

Растущая цивилизованность OSINT создает движение «информация как сопротивление», в котором цифровая активность подразумевает разоблачение и распространение бесхозяйственности государства, коррупции и репрессий. Эта культура сопротивления приобретает все более организованную цифровую идентичность после разоблачения злоупотреблений государственной слежкой в связи с рассекречиванием программы PRISM, слежки АНБ, расследованием Wikileaks и множественными коррупционными скандалами со сливами глобальных оффшорных схем. По недавнему заключению Зейнеп Туфекчи, «нынешняя культура и идентичность этого сообщества (прим. OSINT) в основном антигосударственны» [1. С. 380-382].

Подъем активности и приобщение государств к гражданскому пулу OSINT наблюдается после избрания президента Трампа и с актуализацией проблемы дезинформации, триггером, которой послужили множественные расследования иностранного вмешательства в выборные процессы США, Великобритании и Европы.

Прозрачность, в том числе в отношении предположений и неопределенности, нивелирует вероятность распространения слухов, а также обеспечивает общественный контроль официальной информации и открытых правительственных данных. Государственные учреждения кооперируют с неправительственными партнерами с целью укрепления доверия в обществе и участия в регуляции технологический компаний. Движение против дезинформации, за транспарантное правительство и безопасные выборы набирает сторонников в глобальном измерении, где OSINT становится ключевым инструментом определения, распознавания угроз и преодоления препятствий.

На стыке разведки, прогнозирования, стратегии и политики, коммерческие услуги оказывают множества региональных центров. К примеру, швейцарская компания i-intelligence специализируется на индивидуальных исследованиях и консультациях в сфере национальной безопасности, правоохранительных органов, кризисного управления, борьбы с терроризмом и мошенничеством.

Государственная служба связи (Government Communication Service (GCS)) британского правительства ведет обновляемый набор инструментов для противодействия дезинформации RESIST – руководство для организаций по идентификации, пресечению, разработке ответных мер и повышению устойчивости аудитории к ложной информации [22].

Великобритания разработала общегосударственный подход к реагированию на дезинформационные атаки. Эти усилия возглавляет Департамент цифровых технологий, культуры, СМИ и спорта (Department for digital,

culture, media and sport), который координирует действия по разоблачению иностранной дезинформации, предупреждению общественности и оценке соответствующих ответов через Группу по борьбе с дезинформацией (Counter Disinformation), в которую входят спецслужбы, технические эксперты, МИД, а также другие государственные учреждения [23].

Меры правительства США по противодействию информационным беспорядкам интегрированы в общенациональный подход в сотрудничестве с соответствующими заинтересованными сторонами. Усилия, направленные на сетевую координацию взаимодействий системы государственных институтов с союзниками, сосредоточились на финансовом обеспечении представителей СМИ, аналитиков, активистов и независимых исследователей, поощряется деятельность технологических кампаний по регулированию и соблюдению правил поведения на платформах.

Исследования по обширным тематическим направлениям так или иначе связанными с дигитализацией и совершенствованию инструментов, внедряемых Google, производит Google News Initiative (GNI) – глобальный центр сотрудничества и поддержки журналистов, издателей, ученных и ассоциаций, посредством мероприятий, рабочих групп и тренингов.

Крупнейший хостинг исходного кода GitHub, Inc., используемый обычно для координации программистов, содержит широкий набор инструментов на уровне программного обеспечения исследователей OSINT и включает: платформы для экстрадиции, изменения и удаления exif метаданных файлов практически всех форматов, по машинному поиску семантического отпечатка и наиболее важных тем, новостные рейтинги, графы связанных открытых данных (LOD), инструменты визуализации и картографии энергетического и сельскохозяйственного секторов, отслеживание транзакций по всему миру, сканнеры безопасности и конфиденциальности веб-сайтов (по стандарту GDPR) и многое другое [24].

На пересечении журналистики, технологий и общественных интересов, работает один из старейших институтов Poynter, помогающий журналистам оттачивать навыки и повышать уровень квалификации, объединяя преподавателей и отраслевых экспертов.

Разворачиваются экспериментальные лаборатории такие как Центр журналистских расследований (Centre for Investigative Journalism (CIJ)) по обучению инструментам всесторонних журналистских материалов.

Под эгидой организации Репортеры без границ (Reporters Without Borders (RSF)), в партнерстве с Французским информационным агентством (Agence France Presse (AFP)), Европейским вещательным союзом (European Broadcasting Union (EBU)) и Глобальной сетью редакторов (Global Editors Network) (GEN)), реализуется Инициатива доверия журналистам (Journalism Trust Initiative (JTI)) – проект по саморегулированию СМИ, предназначенный для борьбы с дезинформацией в Интернете. Программа предполагает

также национальное продвижение согласованного набора стандартов доверия и прозрачности СМИ посредством Рабочего соглашения Европейского центра стандартизации ((European Committee for Standardization) CEN) [34].

«Золотой стандарт» информационного права, разрабатываемый в рамках ЕС, расчищает пространство между свободой слова и цензурой с опорой на самоуправление в сфере ИКТ.

На предмет обеспечения честных выборов в Европейский парламент, Европейская комиссия проводит регулярное отслеживание исполнения добровольных обязательств IT компаний, в отношении дезинформации [31].

От платформ требуется предоставлять большую прозрачность и подотчетность их политики. В частности: демонетизировать дезинформацию; ограничить распространение форм манипулятивного поведения (таких как боты, поддельные учетные записи, организованные кампании по манипулированию, захват учетных записей); обеспечить пользователям доступ к рекомендательным системам по выявлению деструктивного контента и инструментам маркировки дезинформации; расширить охват проверки фактов и раскрыть данные для исследователей; обеспечить систему самооценки; создать Центр отчетности с детальным указанием конкретных мер по выполнению обязательств и Целевую группу под председательством Комиссии и в составе подписавших сторон, представителей Европейской службы внешних действий (European External Action Service), Европейской группы регуляторов аудиовизуальных медиауслуг (European Regulators Group for Audiovisual Media Services (ERGA)) и Европейской обсерватории цифровых медиа (European Digital Media Observatory (EDMO)), с опорой на поддержку экспертов, для дальнейшего взаимодействия и адаптации Кодекса с учетом технологических, социальных, рыночных и законодательных изменений [25].

Результаты исследования и выводы. Западные правительства широко поощряют устойчивость общества к ложным нарративам, а также формируют систему управления, способствующую доступу и конструктивному взаимодействию общественности с информацией и данными. Платформы, заинтересованные в глобальном коммерческом участии и унификации правил предоставления услуг поддерживают строгие принципы Общеевропейского регламента по защите данных (General Data Protection Regulation (GDPR)). Европа постепенно выстраивает единые нормы права, подкрепляя свои действия через всестороннее сотрудничество. Соединенные штаты не исключают внедрения опыта союзников в федеральное законодательство [17].

Концепция современного цифрового конституционализма включает в себя не только традиционные конституционные инструменты, а скорее воплощает в себе набор принципов и ценностей, которые информируют и направляют их [29. С. 76-99].

Транспарентность является ключевым критерием, определяющим статус страны на глобальной арене и требующим встраивания в социальную ткань множества международных акторов, испытывающих прочность внутригосударственного политического устройства. На фоне глубокой экономической и технологической интегрированности, система международных отношений остается чувствительной к предсказуемости ее участников, изоляция которых может существенно повлиять на расстановку сил в глобальном масштабе.

Фактором успешной цифровой интеракции в поле сетевого взаимодействия главным образом является экономическое благополучие, формирующее как внутренний потенциал технологического обеспечения для взаимодействия граждан с внешним миром, так и оснащение, и сопровождение инфраструктуры страны на высоком, относительно внешнего мира, уровне безопасности.

Сохранность суверенитета в данном контексте находится на балансе между ассимиляцией и интерференцией по отношению к внешней среде, в процессе реализации национальных интересов. Устойчивость к дефрагментации государственной системы, необходимой для обеспечения безопасного и эффективного развития в глобальной динамике, пропорциональна готовности к преобразованию иерархических элементов общественного контроля в децентрализованные динамичные образования.

Правительства стран с равномерным технологическим распределением и относительно устойчивым развитием приходят к концептуальным разногласиям касательно архитектуры международного правового поля и роли государств в цифровом управлении. В информационно-коммуникационной сфере формируется дихотомия между «глобальной и открытой» интернет-моделью западных демократий и «суверенным и контролируемым» подходом развивающихся стран.

Роль России, как системообразующего полюса силы в локусе постсоветских государств весьма неоднородна. На сегодняшний день, члены ГУАМ ориентированы к союзу с Европой, при этом сближение с РФ, в ракурсе историко-цивилизационного подхода, сохраняется в Беларуси, Армении, Казахстане, Кыргызстане, Таджикистане и Узбекистане. Государства координируют нормотворческую и технологическую архитектуру киберпространства на базе ШОС, СНГ, Евразийского экономического союза, Таможенного союза, Союзного Государства и ОДКБ [13; 21].

Понятия информационной и кибер-безопасности, имплементированные в странах ШОС, расширяют государственный контроль за коммуникационным сектором. Выдвигаемые инициативы через инструментарий ООН требуют возведения широкого ряда зарубежных элементов информационного противостояния в статус прямой угрозы национальной безопасности, что воспринимается западными странами как попытка легитимации

цензуры с негативными последствиями для прав человека на международном уровне [33]. На фоне сохраняющихся разночтений и принципиальной непримиримости, острая необходимость поиска консенсуса в области кибер-безопасности привела к принятию в 2018 году резолюций США и России. Совокупные результаты Группы правительственных экспертов (ГПЭ) [7] и Рабочей группы открытого состава (РГОС) [9] были приняты Генеральной ассамблеей и РГОС 2021-2025 гг. приступила к выполнению своего второго мандата [20].

Несмотря на формальную готовность к поиску компромиссов, взаимодействие сторон по некоторым аспектам кибер-безопасности и развития (затрагивающие вопросы непосредственно хакерских атак и целенаправленных покушений на жизненно важные аспекты инфраструктуры), цикл многосторонних и двусторонних переговоров президентов США и России в течение 2021 года, отношения неуклонно двигались в сторону эскалации и поляризации. При этом цифровая среда стала не только одним из основных предметов диспозиций и фактической ареной современной «холодной войны» формата 2.0, но и непосредственно инструментом ее ведения.

Владение эффективными инструментами, преуспевающими финансовыми и интеллектуальными ресурсами предоставляет преимущество в использовании открытых данных в целях нейтрализации репутации противника как в границах его юрисдикции, так и на международном уровне. Громкие разоблачения глобальных, региональных, частных и специализирующихся на отдельных направлениях расследователей становятся ведущим нарративом, формирующим информационную повестку [2; 6; 28; 26].

Применение OSINT рискованно для правительств в той же мере, в какой они извлекают выгоду, нанося ущерб зарубежным или внутренним оппозиционным группам, поскольку варьирующий баланс сил позволяет внешним субъектам эксплуатировать внутренние препятствия, эффективно подавляя традиционную пропаганду [11].

Как иллюстрирует группа исследователей, использовавших китайскую платформу Baidu Maps для обнаружения цифровых артефактов, имеющих признаки центров содержания под стражей в Синьцзяне, намеренно скрытая информация успешно используется в качестве целевого источника OSINT [12].

Кроссплатформенный анализ позволяет отслеживать скрытые объекты, относящиеся к государственной тайне. К примеру, безобидная рекламная кампания производителей фитнес-трекеров Strava, визуализирующая своих пользователей по всему миру обернулась раскрытием секретных военных баз благодаря наблюдательному пользователю в Twitter [15].

Демократический нейтральный источник, наделенный чрезмерным кредитом доверия в случае непреднамеренной ошибки, смены вектора притяжения или в силу иных обстоятельств может нанести существенный урон

государственной политике. В этом отношении правительства, ведущие ограниченную информационную политику менее уязвимы, и в то же время менее устойчивы, по сравнению с транспарентными сообществами, обладающими гибкими правовыми инструментами и различными источниками быстрой реакции на конфликт [16].

Решение дилеммы гонки цифровых вооружений в информационно-коммуникационном секторе, возлагаемое на многослойную глобальную экосистему национальных и наднациональных институтов, НКО, НПО, представителей СМИ, аналитических институтов, технологических компаний, частных лиц и всевозможных заинтересантов по приоритетным направлениям, оправдано целью планомерного выстраивания универсальной архитектуры права, которая бы обеспечила не хрупкий баланс и временный консенсус, а устойчивое, комфортное сосуществование рычагов правительственного управления и общественного контроля.

Операционный цикл OSINT на нынешнем этапе развития высоко политизирован. Для достоверности процесса и его результатов, специалистам-практикам и правительствам следует сохранять дистанцию, обеспечивать плюрализм доноров и источников данных.

OSINT в качестве инструмента, сокращающего существующие бюрократические процессы сбора и оценки разведывательной информации, одновременно влияя на политические процессы и повествование в СМИ, сохранит свою актуальность. В мире смартфонов с большим объемом данных и распространенных повсеместно социальных сетей тщательный событийный анализ необходим для построения всеобъемлющих нарративов.

Неминуемое развитие Искусственного интеллекта (ИИ) в данном направлении предвосхищает «Революцию в вопросах разведки» (Revolution in Intelligence Affairs (RIA)) в ближайшем будущем [5]. В перспективе развития ИИ, климатической повестки, последствий продолжительной пандемии COVID'19 и других предстоящих гуманитарных кризисов, научный потенциал интеллектуальных дисциплин заслуживает более пристального внимания экспертного сообщества и глобального академического взаимодействия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. *Аттери А., Ширмер Б.* Туфекчи Зейнеп: Твиттер и слезоточивый газ: сила и хрупкость сетевого протеста // Norsk Sosiologisk Tidsskrift. 2019. № 3 (05).

2. *Базби С.* исполнительный редактор Global Investigation to the Pandora Papers // Авторы Washington Post. 2021 // https://www.washingtonpost.com/business/2021/10/03/about-pandora-papers-Investigation/.

3. *Брайант Э.* Мнение: правительства не смогли извлечь уроки из скандала с Cambridge Analytica // OCCRP. 2020 // https://www.occrp.

org/en/37-ccblog/ccblog/13225-governments- have-failed-to-learn-of-the-cambridge-analytica-scandal.

4. *Бельсканоа А., Курц Р., Баумгартне Ю., Бенетис В.* Справочник по инструментам и ресурсам разведки с открытым исходным кодом // I-Intelligence. 2020.

5. *Винчи А.* Грядущая революция в разведывательных делах: как будут трансформироваться искусственный интеллект и автономные системы // Foreign Affairs. 2020 // https://www.foreignaffairs.com/articles/north-america/2020-08-31/coming-revolution-intelligence-affairs.

6. *Гриценко Е.* Как журналисту удалось привлечь 80 000 инстаграмеров к закупкам в Казахстане // Global Investigative Journalism Network. 2022 // https://gijn.org/2022/04/14/how-a-journalist-got-instagrammers-interested-in-procurement-in-kazakhstan-gijn/.

7. Доклад Группы правительственных экспертов по содействию ответственному поведению государств в киберпространстве в контексте международной безопасности (A/76/135) // ООН // https://undocs.org/home/mobile?finalsymbol=a%2f76%2f135&language=e&devicetype=desktop&langrequested=false.

8. Закон об ассигнованиях на национальную оборону на 2006 финансовый год // 3411 публичный закон 109-163 Стратегия Министерства обороны в отношении разведывательных данных из открытых источников.

9. Заключительный Доклад РГОС по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности от 10.03.2021 г. // Генеральная ассамблея ООН // https://front.un-arm.org/wp-content/uploads/2021/03/final-report-a-ac.290-2021-crp.2.pdf.

10. «Индекс финансовой тайны 2020» // Официальный сайт FSI // https://fsi.taxjustice.net/en/introduction/fsi-results.

11. Интернет вещей: Для устранения рисков безопасности в Министерстве обороны США необходимы расширенные оценки и рекомендации // U.S. Government Accountability Office // https://www.gao.gov/products/gao-17-668.

12. *Киллинг А., Раджагопалан М., Бушек К.* Пробелы на картах Китая помогли нам раскрыть лагеря Синьцзяна // Buzzfeed News. 2020 // https://www.buzzfeednews.com/article/alison_killing/satellite-images-investigation-xinjiang-detention-camps.

13. Конвенция ШОС по противодействию экстремизму от 9 июня 2017 года // Официальный интернет-портал правовой информации // http://publication.pravo.gov.ru/document/view/0001201910280036.

14. *Либор Б.* OSINT, новые технологии, образование: расширение возможностей и угроз. Новая парадигма // Журнал стратегической безопасности. 2013. № 3.

15. *Липтак Э.* Тепловая карта фитнес-трекера Strava показывает расположение военных баз. Геолокация не является новой проблемой

для военных // Грань. 2018 // https://www.theverge.com/2018/1/28/16942626/strava-fitness-tracker-heat-map-military-base-internet-of-things-geolocation.

16. *Майкл М., Гилл П.* Сравнение демократизации интеллекта // Разведка и национальная безопасность. 2014. № 29 (4).

17. *Найяр С.* Пришло ли время для американской версии GDPR? // Forbes. 2022 // https://www.forbes.com/sites/forbestechcouncil/2022/02/01/is-it-time-for-a-us-version-of-gdpr/?sh=3102f79d637a.

18. *Онурхан Й.* Кибербезопасность и методы разведки с открытым исходным кодом // В книге: Применение методов научных исследований в области разведки, безопасности и борьбы с терроризмом. 2019.

19. Отчет CPI 2020: проблемы в топ-25 странах // Официальный сайт Transparency International // https://www.transparency.org/en/news/cpi-2020-trouble-in-the-top-25-countries.

20. Организационная Сессия РГОС 2021-2025 г. // Женевская интернет-платформа Digital Watch // https://dig.watch/events/oewg-2021-2025-organisational-session/oewg-2021-2025-organisational-session.

21. Постановление Парламентской Ассамблеи Организации Договора о коллективной безопасности. Москва, 2020. No 13-5.4 // https://paodkb.org/download_pdfs?path=%2fuploads%2fdocument%2ffile%2f136%2fr_30_11_2020_13-5.4.pdf.

22. *Паммент Дж.* Набор инструментов для противодействия дезинформации RESIST 2 // Государственная служба связи Великобритании. 2020 // https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/.

23. Проект «Countering Disinformation» // https://www.counteringdisinformation.com/.

24. Презентация программы «Social Impact» // GITHUB // https://socialimpact.github.com/.

25. Пресс-релиз. По укреплению Кодекса правил по Дезинформации. Брюссель, 2021 // https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585.

26. Расследование команды OCCRP. Что такое Suisse Secrets? // OCCRP. 2017 // https://www.occrp.org/en/suisse-secrets/what-is-suisse-secrets-everything-you-need-to-know-about-the-swiss-banking-leak.

27. Расследование: Взгляд на дезинформацию и как с этим бороться: часть 1 // Maltego Team. 2020 // https://www.maltego.com/blog/infographic-misinformation-and-disinformation/#misinformation-and-disinformationwhy-do-they-thrive.

28. *Салливан Д., Раду П.* Что такое «ландромат»? // OCCRP. 2017 // https://www.occrp.org/en/azerbaijanilaundromat/what-is-a-laundromat.

29. *Селест Э.* Цифровой конституционализм: новое систематическое теоретизирование // Международный обзор права, компьютеров и технологий. 2019. № 33 (1).

30. «Справочник НАТО по разведке из открытых источников 2002 г.» // Веб-архив // https://web.archive.org/web/20060104082427/http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/nato%20osint%20reader%20final%2011oct02.pdf.

31. Свод правил по дезинформации «Code of Practice on Disinformation» // Европейская Комиссия // https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

32. *Уильямс Дж.Х., Блум И.* Определение интеллектуальных данных с открытым исходным кодом второго поколения для оборонного предприятия // Rand Corporation. Н.-Санта-Моника, Калифорния, 2018 // https://www.rand.org/pubs/research_reports/RR1964.html.

33. *Шакиров О.* Двойная Кибербезопасность В ООН // Пир-Центр. Москва, 2020 // https://pircenter.org/blog/view/id/439.

34. «The Journalism Trust Initiative» партнеры и соучредители // https://www.journalismtrustinitiative.org/about.

I.A. KISHUEVA
Postgraduate student of the Department
of Foreign Regional Studies and Foreign Policy,
RSUH, Moscow, Russia

OPEN-SOURCE INTELLIGENCE AS A TOOL OF DIGITAL COACTION IN THE DYNAMICS OF INTERNATIONAL RELATIONS

OSINT (Open-Source Intelligence) as a subject of this article is a set of political communication tools in the framework of international relations progress. The material and methodological base of the study includes a wide range of data and verified sources to shape a comprehensive understanding of the implementation mechanism and risks associated with different government systems and the relevance of open-source intelligence technologies to current tasks of interstate interaction.

This study consistently concretizes the subject of digital technologies based on the graphical representation of the OSINT methodological cycle developed by the RAND Corporation. System analysis reflects the correlation of institutional formations involved in the mechanism of data accumulation and filtering. Provided in the study examples illustrates the positive and negative trends of open-source digital intelligence technologies. A conceptual analysis of the Western and Eastern approaches to the regulation of the digital communication sphere facilitates the identification of the bifurcation areas of the elements that determine the structure of international relations. The purpose of the study is to provide an up-to-date description of OSINT technologies in the current international agenda and develop directions for risk reduction and raise the effectiveness of Open-Source Intelligence.

Key words: *OSINT, digital communication, international relations, multistakeholder governance, digital constitutionalism.*