УДК 32

Кибербезопасность информационных потоков: современное восприятие вызовов информационной безопасности с технологической, социо-информационной и политической точек зрения

Леви Дмитрий Андреевич

Кандидат политических наук,
доцент кафедры европейских исследований,
Санкт-Петербургский государственный университет,
199034, Российская Федерация, Санкт-Петербург, Университетская набережная, 7/9;
e-mail: d.levi@spbu.ru

Аннотация

Многозначность понятия информационной безопасности цифрового мира или кибербезопасность автор статьи предлагает рассматривать через призму трех векторов: технологического, социально-информационного и политического. Каждый характеризуется уникальными особенностями и контролируется специфическими операторами/медиаторами, обеспечивающими статус-кво вектора и его участие в общем понимании кибербезопасности. В статье предлагается оценить разнонаправленность векторов, различия в подходах к угрозам. По мнению автора, для обеспечения эффективности в поддержании информационной безопасности по направлению политического и социо-информационного вектора использование технологических подходов может оказаться наиболее эффективным по сравнению с любыми ограничительными тактиками. Технологический уровень угроз представляется автору наиболее прозрачным в части возможностей взаимодействия и сотрудничества, автор описывает логику работы CERT (CSIRT), принципы самоорганизации безопасности в цифровом мире. Подчеркивается разрыв в организации между технологическим вектором и гуманитарно-политическими, во-многом перечеркивающий перспективы по сближению правовых порядков в единообразного восприятия в части информационной безопасности. В ходе рассуждений автор сопоставляет возможности влияния на информационные потоки приемлемые на различных уровнях восприятия информационной безопасности и приходит к приходит к выводу о жизнеспособности лишь гибридных форм медиаторов и операторов, базирующихся на технологическом уровне и определяющем информационное редактирование и ранжирование контента.

Для цитирования в научных исследованиях

Леви Д.А. Кибербезопасность информационных потоков: современное восприятие вызовов информационной безопасности с технологической, социо-информационной и политической точек зрения // Теории и проблемы политических исследований. 2018. Том 7. № 5А. С. 255-263.

Ключевые слова

Информационная безопасность, цифровая безопасность, кибербезопасность, цифровая дипломатия, политическая безопасность, информационные войны, поисковые системы.

Введение

В риторике исследователей политических и информационных процессов в различных государствах понятие информационной безопасности за последние 20 лет порядком утратило прежнее значение и терминологическую остроту. Виной тому, конечно, не только развитие общества или рост культуры коммуникации, но и технологическое перерождение процесса межличностной и политической коммуникации, что привело к трансформации самого понятия безопасности для информации. Между тем, как и в традиционном научном обороте традиционная безопасность может носить как черты жесткой (hard), так и черты мягкой (soft) безопасности, информационная безопасность может иметь универсальные ценности, предполагающие наличие пространства для международного сотрудничества и даже гармонизации международного права, так и сугубо уникальные, разночтение которых приводит не только к похолоданиям в отношениям между государствами, но и более затяжным информационным войнам. В настоящей статье постараемся разделить современное понятие информационной безопасности в первую очередь в связи с использованием наиболее актуальных каналов распространения информационного взаимодействия, сети Интернет и того, что обычно называют кибер-пространством.

Основная часть

Многочисленные исследования прошлого выстраивали вполне логичную цепочку от источника новости через комментатора и медиа-канал к получателю информации. Политическая наука успешно освоила модель коммуникационного черного ящика и предложила объяснять политическую волю комментаторов или политической/финансовой близостью к политическим/финансовым кругам или идейной ангажированностью [Easton, 1990, 72]. Демократические и политэкономические авторы [например: Поцелуев, 2010, 17.; Балацкий, 2013, 7] предложили объяснить многообразие подходов СМИ к освещению событий и комментариям широтой спектра мнений: действительно, при развитом рынке спроса и предложений, почти любая точка зрения может получить признание и быть востребованной. И, следовательно, быть экономически жизнеспособной. Однако демократизация технологий, во-многом, разрушила привычную систему управления информацией, по сути, сделав нечто такое с каналом передачи информации, что девальвировало ценность комментатора для политической власти. А снижение порога ответственности, ввиду неурегулированности цифровых информационных контактов, привело к деградации ценности самих каналов. Традиционные медиа-каналы, включая телевидение, в обществах с развитыми современными коммуникационными сетями стали постепенно утрачивать свою значимость для политического процесса, а в обществе модой стало говорить о том, что СМИ, как явление, не заслуживают доверия. В результате политический процесс остался практически без одного из самых главных инструментов реализации своих манипулятивных возможностей, которые так успешно обрел с момента начала издания газет, периода геббельсовского визионерства роли радио и, конечно, телевидения, эпохи первых американских теледебатов.

Конечно, сгущать краски в данном вопросе – это некоторое лукавство. И общества разные, и проницаемость общества для новых коммуникационных технологий – разная, и экономический и образовательный ресурс также очень разный. Но тенденция есть тенденция, и игнорировать ее недопустимо, она приводит нас в век разных скоростей цветных фейсбучных

революций, твиттера Трампа проч. [Панцерев, 2016, 15] Между тем это вступление необходимо для того, чтобы пояснить необходимость пристального внимания именно к информации, распространяемой по цифровым каналам, цифровой информации по форме доставке и способу потребления и ее безопасности. Для мира газет и телевидения понятие информационной безопасности ограничивалось особой ролью главного редактора, куратора, собственника издания и набором ограничений для журналистской самостоятельности. Для мира цифрового информационная безопасность превратилась в многогранный объект, который уже не просто является «цифровой информационной безопасностью», а именно «кибербезопасностью», термином, сочетающем и технические, и социальные, и политические аспекты данного понятия.

Три вектора кибербезопасности информационных потоков содержат как легко разделяемые по своей природе элементы, так и тесно связанные. Так к технической безопасности можно отнести понятия безопасности проведения транзакций, конфиденциальности сведений, безопасности сетей и IoT, вопросы безопасности инфраструктурных объектов. При этом безопасность понимается скорее как технический вопрос: достоверность передачи данных из пункта А в пункт Б, безопасность и адекватность программного обеспечения и т.п. При этом о нарушении безопасности равнозначно можно говорить и в ситуации злонамеренных действий 3х лиц и в ситуации случайных действий, ошибок, аварий и т.п. Источник или причина технической небезопасности – практически заведомо осуждаем, если, конечно, удается найти виноватых. В данном секторе мало эмоций, здесь просто договариваться, но здесь очень много экспертов и мало государства.

К социально-информационной безопасности отнесем безопасность национальных ценностей, представлений о будущем, безопасность новостей и безопасность среды. Тут определение информационной безопасности начинает тонуть в гуманитарной неопределенности: политологи сместят вопрос в сторону стабильности политического строя и преемственности власти [Галушкин, 2015, 8], социологи – в сторону устойчивости социальных систем, журналисты об общественных угрозах [Березинская, Азаров, 2017, 47-49]. Нарушение безопасности в социально-информационном ключе понимается как распространение «неправильной» информации или модификация «правильной» ценностной информации. Тут есть место для концепции квадрантов ценностей Парсонса, [Заславская, Леви, 2012, 10-25] информационных войн в той части, где стороны находятся в «окопах», переругиваются твитами или фейковыми новостями, а их фактические действия публике не разъясняются. Виновники нарушения социально-информационной безопасности, как правило, достаточно абстрактны. В ключевых словах этого вектора говорят о традициях, национальных ценностях.

Третий вектор рождается из политической безопасности. Тут речь идет уже не об абстрактных ценностях: медицинских страховках, расовой терпимости и доступности образовании. Подтягиваются ценности чудовищной мобилизирующей силы: ценности религиозные, идеологические, где вопрос публичного спора состоит не в обмене аргументами, а в борьбе за уничтожение инакомыслия. Власть традиционно воспринимает политическую информационную угрозу острее всего, поскольку при всей ее мобилизирующей силе, ее наличие способно разрушить всю систему власти, а не просто согнать одну политическую фракцию и заменить ее другой. Здесь с осуждением нарушителей безопасности совсем все сложно и появляется место для тонкого льда трансграничной пропаганды, цифровой и народной дипломатии ценностей [Цветкова, Ярыгин, 2013, 119-124], а также рисков появления т.н. «пятых колонн». Возмутителями информационной безопасности политического уровня признаются «иностранные враги», непонятные массовой аудитории сотрудники каких-то организаций,

террористические лидеры с другого континента, конечно, харизматичные носители противоположных идеологий или образов мысли. При разборе угроз кибербезопасности политический вектор наиболее перенаселен политическими пропагандистами, здесь меньше всего профессионалов как социологии, так и журналистики, а искать договороспособного оппонента можно месяцами. Ключевые слова – национальные интересы, родина, патриотизм.

В чем польза от такого деления аспектов информационной безопасности? Одной из ключевых задач в изучении данного явления и процесса, безусловно, является понимание ключевых акторов процесса с одной стороны и не менее значимых ключевых медиаторов, способных находиться в разных плоскостях информационных столкновений. Предложенное разделение позволяет удивительно четко выделить и первых, замкнутых в рамках своей трети явления, и вторых, способных перемещаться и выступать управляющими процессами. Остановимся на них подробнее.

Для мира международного права понимание и организация международной системы криптобезопасности информационных потоков — это катастрофа. В первую очередь потому, что информационная безопасность и стандарты этой безопасности изначально понимались как технические и оформлялись RFC-письмами-рассылками для всех заинтересованных лиц. Потому что только открытые стандарты умеют быстрее всего прогрессировать и развиваться. Тем не менее, для изучения угроз и защиты от пагубных вторжений в работу систем экспертное мировое сообщество осознало, что важно делиться информацией: если вас взломали, вы должны об этом рассказать, сделать выводы, чтобы не взломали вашего соседа. А не скрывать информацию. С 1990-х годов сформировалась целая система взаимодействия независимых информационных CERT-центров (от Computer emergency response teams) или CSIRT (от Collaboration security incident reponse teams). Такие центры возникали вокруг университетов, коммерческих компаний и становились центрами привлечения экспертов, инструментами позиционирования своего уровня на рынке ИТ. Основными задачами CERT стали формирование т.н. Good practice guides – правил правильной организации информационных или коммуникационных систем. С точки зрения CERT, любая технологическая угроза – это то, с чем необходимо бороться, уязвимость или «закладка» в аппаратном или программном обеспечении, не важно, как она туда попала, фактор риска, требующий обнаружения и исправления. Гораздо позднее в Европе CERT попытаются координировать в рамках ENISA – Европейского Агентства по сетевой и информационной безопасности (EU Regulation No 460/2004, Regulation No 526/2013), но и тут координация ограничится исключительно формированием единой правовой позицией для расследования инцидентов, плюс, развития стратегий кибербезопасности в отдельных странах ЕС. Для понимания масштаба – в США таких центров около 70, в ЕС около 50, в России в 2012 было три, в 2017 пять [Лукацкий, 2012]. Автономность, открытость и неурегулированность работы CERT стало квинтэссенцией калифорнийского подхода к организации коммуникации в цифровом пространстве.

Собственно, для обеспечения технической безопасности, существования глобальных антивирусов и глобальных операционных систем и глобального интернета этого оказалось достаточно на многие годы. На политическом уровне шли дебаты о регулировании адресного пространства и доменных зон интернета, но этот спор скорее носил характер спора ради чистоты правовой формулы, чем влиял на реальную безопасность или защищенность информационных каналов интернета. До наступления кризиса в отношениях с Россией деятельностью CERT вообще мало кто интересовался на уровне социально-информационной и политической безопасности. За то редкое выявление путей хищения средств через интернет и прочие

криминальные действия в информационном пространстве распутывались без привлечения специалистов CERT. Понимание ценности специалистов, их востребованности в любых юрисдикциях долгое время препятствовала государствам оказывать давление на экспертные ИТ компании, что позволило даже говорить о начале формирования нетократических основ в некоторых государствах [Леви, 2014, 77]. Но несколько печальных историй, самая печальная для России касается истории развития лаборатории Касперского, поставили в этом направлении известную точку [Жегунов, www]. В 2017 году в России вступил в действие 187 закон, который, естественно, законодательно указал на то, что отслеживать безопасность для критически значимых объектов в России может только государство. Закон, по сути, предложил создать министерство пене-тестов (тестов на пенетрацию систем), которое бы занималось исключительно попытками проверить на крепость все возможные инфраструктурные решения и хранило бы в тайне выводы об организации наиболее эффективной безопасности. Реализация такого подхода в России уже тоже «нашла свои грабли», как, например, в части внедрения практически на 100% нарушающих действующее законодательство (в части ФЗ о защите персональных данных) медицинских информационных систем во всех более-менее уважающих себя медицинских кабинетах и клиниках, так и в опыте обеспечения безопасности банковского и финансового сектора (по некоторым оценкам, неофициально связываемым с экспертным сообществом Group IB). То, что российский подход ушел от калифорнийского очень далеко – это, бесспорно, но, справедливости ради, надо отметить, он еще не достиг уровня цензуры китайского метода, определяющего исчерпывающий список разрешенных возможностей против безграничного перечня запрещенных.

В отличие от экспертного технического уровня координация акторов социально-информационного и политического векторов никогда особо не шла дальше деклараций. На социально-информационном уровне в основном доминировали СМИ и медиа-ресурсы. В течение длительного времени одни могли игнорировать других, но переток аудитории в цифровой мир привел к вынужденному слиянию. Конкурентная борьба ранжировала участников рынка по оперативности поставки информации, фактов, комментариев и способности формировать сообщества и репосты. Добавление социальных сетей, возможность анонимных вбросов информации и даже массового ведения бизнеса в сетях без опоры на физический мир оказалось очень интересным ресурсом для социально-информационного конструирования и политического манипулирования. Россия столкнулась с одномоментным появлением «армии троллей» на внутреннем политическом пространстве в примерно в 2006-2007. На международную арену первые потоки государственного участия официально пролились с начала 2000-х, когда США начали проводить эксперименты с тем, что позднее назовут цифровой дипломатией. Россия открыла для себя минусы исключения из возможности участвовать в обеспечении политической информационной безопасности уже в 2008 году в ходе информационной кампании по поддержке Российско-Грузинского столкновения.

Международная координация и попытка урегулировать отношения в цифровых информационных каналах на общественно-социальном и политическом уровнях предпринимается с завидной регулярностью. Первым документом из этой череды стала Будапештская конвенция Совета Европы 2001 года. Последним «Парижский призыв к доверию и безопасности в киберпространстве» ноября 2018 года. И тот и другой документ носят декларативный характер. Оба документа содержат элементы технических компетенций для придания документам черт объективности, но оба не содержат конкретных указаний, как именно планируется защищать сеть и укреплять безопасность. Ну а лакмусовой бумажкой

политической составляющей, позволяющей смело раз и навсегда вычеркнуть, например, Парижский призыв, из списка значимых документов, является упоминание в одном из пунктов декларацию о намерении подписантов «способствовать предотвращению иностранного вмешательства в предвыборный процесс через действия в киберпространстве».

Восприятие системы криптобезопасности информационных потоков, понимаемое как совокупность трех описанных выше составляющих, применяемое к каждому конкретному государству, будь то Россия, США или, например, Эстония, позволяет рассматривать информационную безопасность как явление, содержащее общие универсальные и одновременно совершенно различные ценности, мешающие однозначно договориться о режиме взаимной дружественной безопасности. Получается система сродни лебедю, раку и щуке: экспертно-технологический уровень утверждает о потребностях сотрудничества в сфере информационной безопасности, требует международной правовой координации в области защиты информационных потоков и эффективно борется с уязвимостями, свойственными в широком смысле цифровым информационным каналам без оглядки на то, кто и как этими уязвимостями планирует пользоваться. Политический уровень, напротив, заинтересован в сохранении исключительных возможностей оказания влияния на информационные потоки, в т.ч. посредством технологических уязвимостей при условии пресечения вторжения в сферу его интересов носителей и распространителей альтернативных политических мотиваторов. Это скорее сродни национальному протекционизму, чем международной координации и сотрудничеству. Общественно-информационная составляющая информационной безопасности стремится разделить информационные потоки на белые и черные, допустимые и нет, и в этой связи нередко лишь привлекает внимание к запретным темам [Sparrow, 2011, 77] из-за нестабильности критериев. А значит, уже только на основе предложенного деления составляющих криптобезопасности говорить о перспективе единообразного толкования и обеспечения информационной безопасности в Европе, в мире в ближайшее время не приходится.

Кто выступит координатором, способным сблизить понимание информационной безопасности и понизить ощущение информационной уязвимости? Надо полагать, эта миссия будет отведена технологическим службам, которые вырастают из сервисных и превращаются в последние два десятилетия в социальные сети и народные СМИ. Укрупнение этих проектов приводит к тому, что они более не являются полностью технологическими. Работа с большим объемом пользователей превращает вчерашние форумы и блоги в политические трибуны. Можно, конечно, пригласить в качестве медиатора государство, и оно тут же попытается «посчитать и зарегистрировать» все имеющиеся площадки, но более удачный путь нащупал в 2003 Государственный департамент, осознав, что наличие «неправильной» информации в информационной среде – это еще не провал. Лучшими медиаторами станут скорее акторы, способные на технологическом уровне подготовить алгоритмы ранжирования и переформулирования одних и тех же новостей и информационных вызовов для разной аудитории так, чтобы при всей своей остроте наиболее провокационные оказывались наименее находимыми. Акторы мира политической коммуникации будут технологическими, а критерием популярности информации и ее ценности станет скорее доступность информации в поиске, простота ее обнаружения.

Влияние на этот процесс с политического и общественного уровня опосредовано, однако находится на том уровне, что договоренности в агрегации, участие в разработке алгоритмов ранжирования ценностного и новостного контента на уровне грантов дают для государства или

политической силы государства инструмент и ресурс гораздо более эффективный, чем может предложить количественное продвижение, типовые SMM методики или попытки вытеснения нежелательного ценностного контента. Тут, конечно, нет монополии, но в условиях экономики цифрового мира, где независимые надгосударственные платежные средства вроде биткоинов еще не развиты, количество поисковых систем, агрегаторов новостей и проч. ограничено, и тем более количество экспертов, которые способны дорабатывать решения дня сегодняшнего до стартапов дня завтрашнего минимально, подобного рода решения окупаются втрое. «Центры силы», компании, способные концентрировать вокруг себя визионеров дня будущего, научные центры, которые способны придумывать принципиальные алгоритмы и сервисы, которыми далее пользуются тысячи разработчиков и миллионы пользователей – их число тем более вычисляемо всего несколькими десятками.

Заключение

Получается, что наиболее надежным, хотя и не быстрым способом, добиться обеспечения качественного реформирования ситуации с управляемостью социальной и политической информационной безопасностями можно через взаимодействие с техно-экспертным уровнем специалистов в области постановки задачи, прикладной информатики в сфере общественно-политического управления и международных отношений. А это скорее уровень компаний – поисковых систем, медиа-анализаторов 2.0 и аналогичных решений, которых можно отнести к гибридным формам операторов информационных потоков. И в этом балансе политического, социального и технологического будет заключаться новый смысл черного ящика системы коммуникации и системы обеспечения криптобезопасности информационных потоков. А как сможет этим воспользоваться бизнес или государство, превратится ли этот инструмент в цензуру или нет - покажет только время, конкуренция и совершенство алгоритмов.

Библиография

1. Балацкий Е. Концепция сложности и экономическая теория демократии // Общество и экономика. 2013. № 5. С. 5-24.
2. Березинская М.Д., Азаров А.Ю. Информационная безопасность современного общества // Информационное общество: состояние, проблемы, перспективы. 2017. С. 45-52.
3. Галушкин А.А. К вопросу о значении понятий национальная безопасность, информационную безопасность, национальная информационная безопасность // Правозащитник. 2015. № 2. С. 8-19.
4. Заславская Н.Г., Леви Д.А. Вычисление вектора развития системы общих ценностей и оценка потенциала общественно-политических действий на примере отношений России и Европейского Союза. СПб.: Арт-Эго, 2012. 346 с.
5. Жегунов И. Орки, победившие технарей. Как силовики внедрились в «Лабораторию Касперского». URL: https://meduza.io/feature/2018/01/22/orki-pobedivshie-tehnarey
6. Леви Д. Процесс формирования политической нетократии как фактор глобального развития в странах БРИКС и остальном мире // БРИКС в системе международных отношений: новый этап глобального партнерства. Сборник научных трудов. СПб., 2014. С. 76-85.
7. Лукацкий А. Сколько CERTов в России. URL: https://www.securitylab.ru/blog/personal/Business_without_danger/23400.php
8. Панцерев К.А. Твиттерные революции в странах Северной Африки – обратная сторона развития информационного общества // Азия и Африка сегодня. 2016. № 4 (705). С. 14-19.
9. Поцелуев С.П. Диалог и квазидиалог в коммуникативных теориях демократии. Ростов-на-Дону, 2010. 496 с.
10. Цветкова Н.А., Ярыгин Г.О. Политизация цифровой дипломатии: публичная дипломатия Германии, Ирана, США и России в социальных сетях // Вестник Санкт-Петербургского университета. Серия 6. Философия. Культурология. Политология. Право. Международные отношения. 2013. № 1. С. 119-124.
11. Easton D. The Analysis of Political Structure. New York: Routledge, 1990. 352 p.

12. Sparrow B. Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips // Science. 2011. Vol. 333. № 6043. P. 776-778.

Cybersafety of information flows: modern perception of information security challenges from a technological, socio-informational and political point of view

Dmitrii A. Levi

PhD in Political Science,
Associate Professor of European Studies Department,
Saint Petersburg State University,
199034, 7/9, Universitetskaya embankment, Saint Petersburg, Russian Federation;
e-mail: d.levi@spbu.ru

Abstract

The author of the article proposes to consider the multiple meanings of the concept of information security of the digital world through the prism of three vectors: technological, social information and political. Each is characterized by unique features and is controlled by specific operators/mediators ensuring the status quo of the vector and its participation in the general understanding of cybersafety. The article proposes to evaluate the multidirectionality of the vectors, the differences in the approaches of the threats. According to the author, to ensure effectiveness in maintaining information security in the direction of the political and socio-informational vector, the use of technological approaches may be most effective than the use if any restrictive measures. The technological level of threats seems to the author most transparent in terms of interaction and cooperation, the author describes the logic of CERT (CSIRT), the principles of self-organization of security in the digital world. The gap in the organization between the technological vector and the social/political driven one is emphasized, which largely negates the prospects for legal harmonization of information security. In the course of the article, the author compares the possibilities of influencing information flows available for different levels of perception of information security and comes to the conclusion that only hybrid forms of mediators and operators based on the technological level and determining information editing and ranking of the viability are viable.

For citation

Levi D.A. (2018) Kiberbezopasnost' informatsionnykh potokov: sovremennoe vospriyatie vyzovov informatsionnoi bezopasnosti s tekhnologicheskoi, sotsio-informatsionnoi i politicheskoi tochek zreniya [Cybersafety of information flows: modern perception of information security challenges from a technological, socio-informational and political point of view]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 7 (5A), pp. 255-263.

Keywords

Information security, information safety, digital security, cyber security, cyber safety, digital diplomacy, political security, information wars, search engines.

References

1. Balatskii E. (2013) Kontseptsiya slozhnosti i ekonomicheskaya teoriya demokratii [The concept of complexity and the economic theory of democracy]. *Obshchestvo i ekonomika* [Society and Economics], 5, pp. 5-24.
2. Berezinskaya M.D., Azarov A.Yu. (2017) Informatsionnaya bezopasnost' sovremennogo obshchestva [Information security of modern society]. In: *Informatsionnoe obshchestvo: sostoyanie, problemy, perspektivy* [Information Society: state, problems, prospects].
3. Easton D. (1990) *The Analysis of Political Structure*. New York: Routledge.
4. Galushkin A.A. (2015) K voprosu o znachenii ponyatii natsional'naya bezopasnost', informatsionnuyu bezopasnost', natsional'naya informatsionnaya bezopasnost' [On the question of the meaning of the concepts of national security, information security, national information security]. *Pravozashchitnik* [Puman rights activist], 2, pp. 8-19.
5. Levi D. (2014) Protsess formirovaniya politicheskoi netokratii kak faktor global'nogo razvitiya v stranakh BRIKS i ostal'nom mire [The process of formation of political netocracy as a factor of global development in the BRICS countries and the rest of the world]. In: *BRIKS v sisteme mezhdunarodnykh otnoshenii: novyi etap global'nogo partnerstva. Sbornik nauchnykh trudov* [BRICS in the system of international relations: a new stage of global partnership. Collection of scientific papers]. St. Petersburg.
6. Lukatskii A. *Skol'ko CERTov v Rossii* [How many CERTS are in Russia]. Available at: https://www.securitylab.ru/blog/personal/Business_without_danger/23400.php [Accessed 10/10/2018]
7. Pantserev K.A. (2016) Tvitternye revolyutsii v stranakh Severnoi Afriki – obratnaya storona razvitiya informatsionnogo obshchestva [Twitter Revolutions in North Africa: The reverse side of the development of the information society]. *Aziya i Afrika segodnya* [Asia and Africa today], 4 (705), pp. 14-19.
8. Potseluev S.P. (2010) *Dialog i kvazidialog v kommunikativnykh teoriyakh demokratii* [Dialogue and quasi-dialogue in communicative theories of democracy.]. Rostov-on-Don.
9. Sparrow V. (2011) Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips. *Science*, 333, 6043, pp. 776-778.
10. Tsvetkova N.A., Yarygin G.O. (2013) Politizatsiya tsifrovoi diplomatii: publichnaya diplomatiya Germanii, Irana, SShA i Rossii v sotsial'nykh setyakh [Politicization of digital diplomacy: public diplomacy of Germany, Iran, USA and Russia in social networks]. *Vestnik Sankt-Peterburgskogo universiteta. Seriya 6. Filosofiya. Kul'turologiya. Politologiya. Pravo. Mezhdunarodnye otnosheniya* [Bulletin of St. Petersburg University. Series 6. Philosophy. Culturology. Political science. Right. International relationships], 1, pp. 119-124.
11. Zaslavskaya N.G., Levi D.A. (2012) *Vychislenie vektora razvitiya sistemy obshchikh tsennostei i otsenka potentsiala obshchestvenno-politicheskikh deistvii na primere otnoshenii Rossii i Evropeiskogo Soyuza* [Calculation of the vector of development of the system of common values and assessment of the potential of socio-political actions on the example of relations between Russia and the European Union]. St. Petersburg: Art-Ego Publ.
12. Zhegunov I. *Orki, pobedivshie tekhnarei. Kak siloviki vnedrilis' v «Laboratoriyu Kasperskogo»* [Orcs, who won the techies. As security forces infiltrated Kaspersky Lab]. Available at: https://meduza.io/feature/2018/01/22/orki-pobedivshie-tehnarey [Accessed 10/10/2018]