Серия «Политология. Религиоведение»
2018. Т. 24. С. 24–32
Онлайн-доступ к журналу:
http://izvestiapolit.isu.ru/ru/index.html

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 327+32.019.5+004
DOI https://doi.org/10.26516/2073-3380.2018.24.24

Дезинформация как инцидент информационной безопасности

В. Е. Муценек

Иркутский государственный университет, г. Иркутск

Аннотация. Рассматривается дезинформация как инцидент информационной безопасности, влияющий на принятие решений во внешнеполитической деятельности. Представлен анализ инцидентов, связанных с дезинформацией, отражены перспективы развития международного сотрудничества в области информационной безопасности.

Ключевые слова: информационная безопасность, международные отношения, дезинформация, пропаганда.

Для цитирования: Муценек В. Е. Дезинформация как инцидент информационной безопасности // Известия Иркутского государственного университета. Серия Политология. Религиоведение. 2018. Т. 24. С. 24–32. https://doi.org/10.26516/2073-3380.2018.24.24

В методологии информационной безопасности термин «инцидент информационной безопасности» долгое время трактуется, согласно ГОСТ Р ИСО/МЭК 27000-2012, ГОСТ Р ИСО/МЭК 27002-2012, как «одно или несколько нежелательных событий, которые со значительной степенью вероятности подвергают опасности деловую деятельность и угрожают информационной безопасности». К инцидентам традиционно относят события, объектами которых являются уже существующая информация, основные и вспомогательные технические средства.

Стандарт ГОСТ Р ИСО/МЭК 27002-2012 в качестве элементов неисчерпывающего перечня возможных инцидентов приводит: потерю услуг, оборудования или средств обслуживания; неисправности или перегрузки систем; ошибки оператора; несоблюдение политик или рекомендаций; нарушения мер физической безопасности; неконтролируемые изменения систем; программные сбои; нарушения доступа. В контексте информационной безопасности как совокупности интересов личности, общества и государства в информационной сфере[1], с учетом устоявшихся в методологии состояний, характеризующих информацию и информационный ресурс (целостность, доступность, конфиденциальность), становится очевидным изъян существующего подхода к рассмотрению инцидентов информационной безопасности.

[1] Доктрина информационной безопасности Российской Федерации [Электронный ресурс] : утв. Президентом Российской Федерации В. В. Путиным 5 декабря 2016 г., № 646 // Президент России : сайт. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 01.05.2017).

В предыдущей работе, посвященной информационному противоборству, уже отмечалась взаимосвязь сфер влияния сторон противоборства и средств массовой информации в формировании общественного мнения [8]. Фактически СМИ и эксперты, являющиеся необъективными наблюдателями в силу пересечения поля собственных интересов с интересами какой-либо из сторон противоборства, являются источниками и ретрансляторами одновременно информации и дезинформации.

Рассмотрим индивида как носителя информации. Подразумевается, что информация, обрабатываемая человеком в мыслительной деятельности, может обладать всеми характеристиками информации, обрабатываемой автоматизированными системами: конфиденциальностью, целостностью и доступностью. Индивид может являться производителем информации и выступать в качестве носителя информации.

Конфиденциальность производимой информации определяется индивидом субъективно из оценки возможных последствий ее неконтролируемого распространения, при этом набор критериев формируется из градированных и формализованных систем, таких как уголовное и административное право, и комплекса социальных норм. Доступность производимой информации определяется психофизиологическими состояниями, изменяющими функционирование сенсорно-информационной, кратковременной и долговременной памяти. Что же касается целостности, она представляется сомнительной.

Исследования в области философии дискретного мира дают возможность оперировать терминами «квант-остановка», «постоянная память внешних условий» и «непостоянная информация» [2]. Применяя дискретную концепцию «памяти» к носителям информации как материальным объектам, можно отметить, что, во-первых, любая объективная информация, носитель и производитель которой совпадают, в квант возникновения и во все другие моменты времени будет оставаться неизменной для объективного внешнего наблюдателя. Появление непостоянной информации в процессе наблюдения изменяющегося объекта возможно только тогда, когда мгновенные значения «постоянной памяти» претерпевают изменения в зависимости от изменений носителя. Наблюдатель, оперирующий в области традиционной «непрерывной» философии, не имеет представления о ранее существующих квантах и, соответственно, не способен зафиксировать изменение. В отрыве от объекта, производящего информацию, получить представление об изменениях объекта становится невозможным даже для наблюдателя в системе дискретного мира, поскольку в носителе информации, не являющемся первоначальным источником, мгновенные значения «постоянной памяти» присутствуют не полностью и до получателя ретранслируются через представления, которые могут быть искажены.

Возможность искажения представлений лежит в основе дезинформации как процесса. В результате происходит изменение структуры и объема ранее сформированных представлений. Таким образом, производство и распространение дезинформации можно приравнять к инцидентам информационной безопасности, характеризуемым угрозой нарушения целостности.

В попытке охарактеризовать возможные причины намеренного искажения информации целесообразно обратиться к поведенческой психологии. Анализируя причины лжи и обобщая труды других ученых и публицистов, американский психиатр Чарльз Форд выделил некоторые весьма интересные с точки зрения информационной и национальной безопасности причины: ложь с целью получения голосов избирателей; ложь с целью изменения политического курса; ложь для поддержания национальной безопасности и военных операций [4].

Данная классификация характеризует ложь лиц, находящихся на государственной службе. Причинно-следственный характер этих видов искажений рационален, связан исключительно со служебной деятельностью индивида и не требует дополнительного изучения личности источника информации. Однако личностные качества и психофизиологическое состояние играет большую роль в принятии решений, поэтому целесообразно, оценивая возможность дезинформации, учитывать и такие детерминанты, как: ложь с целью почувствовать власть; ложь с целью преодоления собственного подавленного состояния; ложь с целью сохранения самоидентичности [Там же].

В силу недостаточности информации в представлении даже в случае отсутствия намеренных искажений представление не будет обладать абсолютной объективностью. Внешнеполитическая деятельность, требующая принятия решений в условиях неопределенности, опирается на многосторонние форматы для уточнения сведений, необходимых для принятия решения. Однако внесение намеренных искажений и последующая ретрансляция без верификации способны прямо или косвенно влиять на формирование позиций участников переговоров.

С точки зрения психологии участники переговорного процесса в формате постоянно действующей конференции являются социальной группой. Справедливым было бы предположить вероятность развития в данной социальной группе синдрома группового мышления.

Характеризуя синдром группового мышления, Ч. Форд обращается к исследованию доктора Ирвина Л. Джениса из Йельского университета, проанализировавшего последствия синдрома на примере систематических просчётов внешней политики США. Опасность проявления синдрома группового мышления заключается в игнорировании предсказуемых последствий и пренебрежении оценкой рисков. В числе признаков проявления синдрома: иллюзия безнаказанности; слепая вера в моральные принципы группы; совместная рационализация; устойчивость стереотипов [Там же]. Четыре других признака, упомянутых Фордом, можно ввиду семантического сходства обобщить в один, назовем его «отрицание чуждых идей».

В сравнении с отрицанием «импорта идей», прекрасно иллюстрируемым философией учхе [1], «отрицание идей» – явление абсолютно деструктивное, так как любая идея, кроме коллективно сформированной внутренней идеи группы, способна разрушить иллюзию и вызвать дискомфорт членов группы. Поэтому внешние идеи, отступающие от общих правил группы, отвергаются даже при наличии научного обоснования.

Проиллюстрируем типичный продукт дезинформации в рамках синдрома группового мышления на примере аналитического отчета Департамента политики Европарламента «Стратегические коммуникации ЕС. Взгляд на противодействие пропаганде»[2].

Отчёт привлекает внимание неофициальным стилем изложения, что может свидетельствовать об исключительно пропагандистском назначении документа. Ключевые факты, формирующие мнение читателя, сокращаются, первоисточники информации намеренно упускаются из контекста. Это можно наблюдать на протяжении всего отчета – наиболее заметны данные особенности во врезках.

Еще одним характерным признаком дезинформации является искажение фактов в пользу картины восприятия, формируемой властями Европейского союза. Фактически, некоторые фрагменты отчета (например, страница 10) нивелируют серьезность миграционного кризиса и его причинно-следственные связи под предлогом использования этих событий Россией для «убеждения европейской аудитории в фокусированности ЕС на выдуманной угрозе со стороны России и недооценке реальных угроз с юга». В качестве примера (опять же опуская конкретные факты) даются отсылки к террористическим атакам в Париже и Брюсселе, в то время как «на государственном телевидении России» отсутствуют репортажи об «узбекском мигранте, убившем ребенка в Москве» [Там же]. Очевидно, подразумеваются террористические акты 13 ноября 2015 г. и 22 марта 2016 г. соответственно. На новостном портале ВГТРК от 29 февраля 2016 г. имеются несколько сообщений об убийстве ребенка в Москве. В сообщении от 13:59 названо место рождения подозреваемой[3]. Таким образом, преступление в подробностях было освещено государственными СМИ непосредственно в день совершения. В данной ситуации указание источников информации рушит картину коллективного самообмана, тщательно создаваемую авторами аналитического отчета.

В условиях формирования глобального информационного пространства сведения о традиционных инцидентах информационной безопасности подвергаются намеренным искажениям с целью воздействия на общественное мнение. При этом для подтверждения ошибочных или искаженных выводов могут быть использованы (в том числе неосознанно) особенности рынков средств защиты информации и услуг связи.

Например, в попытках анализа ситуации с распространением вируса WannaCry сыграла роль популярность технологических решений в области резервного копирования и антивирусной защиты. Материалы, созданные по отчетам с пользовательских компьютеров компаниями Acronis[4] и «Лаборатория Касперского» [5], опубликованы со значительной для инцидентов такого мас-

[2] EU Strategic Communications. With a view to counteracting propaganda [Электронный ресурс] // European Perliament. URL: http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA%282016%29578008_EN.pdf (дата обращения: 01.06.2017).

[3] Вести.ру: Новости, фото и видео дня [Электронный ресурс]. URL: http://www.vesti.ru (дата обращения: 01.06.2017).

[4] Блог компании Acronis [Электронный ресурс]. URL: https://habrahabr.ru/company/acronis/blog/ (дата обращения: 01.06.2017).

штаба временной разницей, однако на иллюстрации, предоставленной «Лабораторией Касперского», по тяжести последствий Россия занимает наихудшую позицию, что явно не соответствует материалу, предоставленному компанией Acronis. Это объясняется долями продуктов «Лаборатории Касперского», выявивших вирус, на внутреннем и внешних рынках.

В контексте внешнеполитического противоборства инциденты информационной безопасности представляют интерес в качестве основы для дезинформации. Рассмотрим попытки определить национальную принадлежность автора вируса WannaCry. Так, различные средства массовой информации называли возможными источниками Россию и КНДР, позже – КНР [7; 11]. В качестве основания для указания КНР как страны происхождения вируса отмечается использование диалектизмов китайского языка и взаимное соответствие английского и китайского вариантов сообщений при обработке в сервисе Google Translate [11]. Однако географическая разобщенность приведённых в примерах диалектизмов не позволяет однозначно утверждать, что автор вируса – гражданин КНР или носитель китайского языка. Наличие в тексте сообщения диалектизмов может быть связано с особенностями формирования «лучших вариантов перевода» для сервиса Google Translate, при котором пользователи имеют возможность предлагать собственные варианты перевода.

Классическим случаем дезинформации, совмещенным с синдромом группового мышления, являются попытки найти след «вмешательства России в выборы Президента США». Задача формирования общественного мнения здесь упрощается, поскольку целевая аудитория в большинстве своём не имеет представления о том, как именно могут быть похищены защищаемые сведения. Попытки обратить внимание общественности на то, что источником утечки информации стал инсайдер в составе избирательного штаба Демократической партии США, привели лишь к трансформации части аргументов [6]. Не способствует установлению объективной истины и то, что в методологии информационной безопасности прямые каналы утечки (в том числе через инсайдера) могут являться элементами составных (комплексных) каналов утечки информации. В данном контексте не важно, как именно осуществляется утечка, так как последствия утечки по материально-вещественному каналу (передача документов через инсайдера) не отличаются от последствий утечки по каналу связи (при перехвате информации из компьютерной сети).

Отмечаемое непредоставление официальными лицами США доказательств причастности «российских хакеров» к утечке писем Джона Подесты может свидетельствовать о реализации одного из нескольких сценариев:

1) утечка осуществлена через инсайдера, разочарованного в политике Демократической партии США;

2) утечка с применением программно-технических средств разведки имела место, но доказательства получены путем, исключающим использование их в судебном разбирательстве (т. е. являются недопустимыми);

3) утечка с применением программно-технических средств разведки имела место, но доказательства не предаются огласке для обеспечения безопасности агента-нелегала на территории государства-конкурента или группы государств;

4) утечка с применением программно-технических средств разведки имела место, но доказательства не предаются огласке, так как не удовлетворяют направленности текущего внешнеполитического курса;

5) утечка была сфабрикована для создания информационного повода к массовой кампании по дезинформации.

Подтвердить или опровергнуть правильность какого-либо из этих предположений станет возможным только после опубликования доказательств, в данный момент не остаётся иного выхода, чем считать все сценарии равновероятными.

Проблема использования дезинформации в конфликтах универсальна. Дезинформация применяется всеми участниками внешне- и внутриполитического противоборства. Из недавних исследований в области пропаганды стоит отметить работу Маккелви и Дюбуа [9]. В своей работе исследователи рассматривают социальные сети в контексте внутриполитической борьбы в Канаде, классифицируют ботов на четыре группы: «ослабители», «усилители», «боты прозрачности» и «слуги», анализируют комплекс правовых мер, принятых правительством Канады для защиты информации от ботов.

«Ослабители» в социальных сетях выборочно снижают последствия распространения сведений, негативно освещающих деятельность политиков. Исследователи относят к «ослабителям» и сети из взломанных компьютеров, зараженных вредоносным программным обеспечением (так называемые ботнеты) [Там же], игнорируя существенное с точки зрения информационной безопасности различие в объектах атаки: целью бота в социальной сети является информация, и в ходе атаки становится возможно нарушение представления наблюдателя о внешних условиях, т. е. нарушение целостности, в то время как атаки типа «отказ в обслуживании», выполняемые с помощью ботнетов, нарушают доступность информации и направлены на средства вычислительной техники и оборудование компьютерных сетей (пресечение распространения информации в результате таких атак достигается за счет сбоев программного и аппаратного обеспечения, вызываемых повышенной нагрузкой или заведомо ошибочными входными данными).

Две другие рассмотренные группы – «усилители» и «боты прозрачности» обладают сходной целью: фокусирование внимания аудитории на действиях и личности политика. «Боты прозрачности» при этом ретранслируют только информацию, касающуюся неправомерных действий. Отмечается использование «ботов прозрачности» средствами массовой информации. Рассмотренная в работе [Там же] группа ботов «слуги» представляет собой средства автоматизированного сбора и анализа информации. Эти средства могут быть использованы в разведывательной деятельности, но не обладают возможностями ретрансляции информации в социальной сети и потому не могут быть отнесены к средствам пропаганды.

Использование социальных сетей для распространения дезинформации и пропаганды детально освещено в работе Дж. Прайера [10]. Отмечается возрастающее с 2006 г. применение средств информационного противоборства террористическими организациями (приведены примеры активности ИГИЛ[5]). Проиллюстрированы технологии «захвата тега», использования мобильных

[5] Террористическая организация. Запрещена на территории России.

приложений для формирования ботнета «усилителей», использования утечек информации для формирования общественного мнения. Применение этих технологий ассоциируется Дж. Прайером со всеми рассмотренными акторами: террористическими организациями и правительствами государств, относящихся к разным геополитическим блокам. В то же время злоумышленник – частное лицо (не аффилированный со сторонами противоборства) не рассматривается в качестве возможного источника угрозы, что является упущением.

Дж. Прайер констатирует, что в основе современных методов ведения информационной войны со стороны России лежат пропагандистские методы времен холодной войны, хотя и варьирующиеся в зависимости от среды доставки. Прогнозируется дальнейшее доминирование России в информационном противоборстве [Там же].

Что возможно противопоставить использованию инцидентов информационной безопасности для дестабилизации международной обстановки? А. М. Тамицкий в своей работе [3] указывает на необходимость совершенствования международной архитектуры информационной безопасности, развивая ее от региональной до общемировой. Для достижения этого понадобится заключение межправительственного соглашения в рамках постоянно действующей международной конференции, обладающей инструментами судебного разрешения споров. Такой международной конференцией могла бы стать ООН. В настоящее время проекты Конвенции по кибербезопасности разрабатываются многими странами – участниками ООН. По сообщениям СМИ, российско-китайский проект Конвенции разработан в рамках Шанхайской организации сотрудничества и посвящен борьбе с несанкционированным вмешательством в компьютерные системы как с уголовным преступлением[6].

В открытом доступе находится российский проект соответствующей Конвенции, в котором охватывается более широкий спектр вопросов информационной безопасности, а именно: информационные войны, дезинформация как угроза внешнеполитической стабильности, противодействие терроризму в киберпространстве, вопросы суверенитета в информационном пространстве, право на самооборону и адекватные ответные действия[7].

Однако международные договоры подобного рода могут быть проигнорированы государствами, рассматривающими информационную войну в качестве допустимого средства достижения преимущества. Кроме этого, механизм внесения поправок, предусмотренный проектом Конвенции, имеет недостаток: в отличие от оговорок к Конвенции, не предусмотрено требование непротиворечивости поправок целям Конвенции, что делает возможным возникновение неравных условий и создание ситуации, требующей пересмотра Конвенции всеми участниками.

Таким образом, перспективным с методологической стороны является придание статуса инцидентов информационной безопасности событиям, в формировании которых дезинформация сыграла ключевую роль. Ограничение

[6] Вести Экономика [Электронный ресурс]. URL: http://www.vestifinance.ru/articles/82974 (дата обращения: 01.06.2017).

[7] Конвенция об обеспечении международной информационной безопасности (концепция) [Электронный ресурс] // М-во иностр. дел РФ. URL: http://www.mid.ru/foreign_ policy/official_ documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения: 01.06.2017).

распространения ложных сведений с целью дестабилизации политической обстановки и формирования общественного мнения должно сопровождаться обеспечением права атакуемого государства на симметричные адекватные ответные действия. С целью предотвращения проявлений синдрома группового мышления для информационных потоков структур государственного управления стран – участников Конвенции по информационной безопасности предлагается ввести обязательное требование верифицируемости информации.

Список литературы

1. *Муценек В. Е.* Институциональный подход в управлении на примере Корейской Народно-Демократической Республики // Актуальные проблемы экономики, менеджмента и туризма : сб. науч. ст. Иркутск : МГЛУ ЕАЛИ, 2015. С. 104–112.

2. *Саркисов В. А.* Понятие «память» и механизм рождения и формирования человека [Электронный ресурс] // Научно-техническая библиотека : сайт. URL: http://www.sciteclibrary.ru/texsts/rus/stat/st5750.pdf (дата обращения: 01.05.2017).

3. *Тамицкий А. М.* Информационная безопасность как фактор международных отношений в Арктическом регионе [Электронный ресурс] // Вестн. Север. (Аркт.) федер. ун-та. Сер. Гуманит. и соц. науки. 2013. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-faktor-mezhdunarodnyh-otnosheniy-v-arkticheskom-regione (дата обращения: 01.06.2017).

4. *Форд Чарльз.* Психология обмана. Как, почему и зачем лгут даже честные люди : пер. с англ. Е. А. Любимцевой. М. : Эксмо, 2013. 400 с.

5. Эпидемия шифровальщика WannaCry: что произошло и как защититься // Блог Лаборатории Касперского [Электронный ресурс]. URL: https://blog.kaspersky.ru/wannacry-ransomware/16147/ (дата обращения: 01.06.2017).

6. *Boyer D.* WikiLeaks figure says ‘disgusted’ Democrat leaked Clinton campaign emails [Electronic resource] // The Washington Times. URL: http://www.washingtontimes.com/news/2016/dec/14/craig-murray-says-source-of-hillary-clinton-campai/ (date of access: 01.06.2017).

7. *Durden T.* WannaCry Ransomware Attack Linked To China, Not Russia Or North Korea. URL: http://www.zerohedge.com/news/2017-05-29/wannacry-ransomware-attack-linked-china-not-russia-or-north-korea (date of access: 01.06.2017).

8. *Kalinina V. V., Mutsenek V. E.* Mass Media as an Instrument of Information Confrontation // On The Way To A Stable World: Security And Sustainable Development: a collection of scientific papers. San Diego: Ron Bee & Associates, 2015. pp. 14–17.

9. *McKelvey F., Dubois E.* Propaganda in Canada: The Use of Political Bots [Electronic resource] // The Computational Propaganda Project. URL: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Canada.pdf (date of access: 07.05.2018).

10. *Prier J.* Commanding the Trend: Social Media as Information Warfare // Strategic Studies Quarterly. 2017. Vol. 11, issue 4. P. 50–85.

11. *Wang Wei.* Linguistic Analysis Suggests WannaCry Hackers Could be From Southern China [Electronic resource] // The Hacker News. URL: http://thehackernews.com/2017/05/china-wannacry-ransomware.html (date of access: 01.06.2017).

Disinformation as an Information Security Incident

V. E. Mutsenek

Irkutsk State University, Irkutsk

Abstract. The article considers disinformation as an information security incident influencing a decision-making process in a foreign policy. An analysis of incidents involving disinformation has been provided. Prospects of international cooperation development in the field of information security have been provided.

Keywords: information security, international relations, disinformation, propaganda.

For citation: Mutsenek V.E. Disinformation as an Information Security Incident. *The Bulletin of Irkutsk State University. Series Political Science and Religion Studies,* 2018, vol. 24, pp. 24-32. https://doi.org/10.26516/2073-3380.2018.24.24 (in Russian)

References

1. Mutsenek V.E. Institucional'nyj podhod v upravlenii na primere Korejskoj narodno-demokraticheskoj respubliki [Institutional approach in governance based on the example of the Democratic People's Republic of Korea]. *Aktual'nye problemy ehkonomiki, menedzhmenta i turizma* [Topical Issues of Economics, Management and Tourism]. Irkutsk, Eurasian Linguistic Institute of Moscow St. Linguistic Univ., 2015, pp. 104-112. (in Russian)

2. Sarkisov V. A. *Ponyatie «pamyat'« i mekhanizm rozhdeniya i formirovaniya cheloveka* [The concept of "memory" and mechanism of birth and formation of man]. Available at: http://www.sciteclibrary.ru/texsts/rus/stat/st5750.pdf (date of access: 01.05.2017). (in Russian)

3. Tamickij A. M. Informacionnaya bezopasnost' kak faktor mezhdunarodnyh otnoshenij v Arkticheskom regione [Information security as factor of foreign relations in Arctic region]. *Vestnik Severnogo (Arkticheskogo) Federal'nogo Universiteta. Seriya Gumanitarnye i social'nye nauki* [Bulletin of the Northern (Arctic) Federal University, Series of Humanities and Social Sciences], 2013. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-faktor-mezhdunarodnyh-otnosheniy-v-arkticheskom-regione (date of access: 01.06.2017). (in Russian)

4. Ford Ch. *Psihologiya obmana. Kak, pochemu i zachem lgut dazhe chestnye lyudi* [Lies! Lies!! Lies!!! The Psychology of Deceit. Translated from English by E.A. Lyubimceva]. Moscow, Eksmo Publ., 2013, 400 p. (in Russian)

5. *Epidemiya shifroval'shchika WannaCry: chto proizoshlo i kak zashchitit'sya* [Epidemy of WannaCry ransomware: what happened and how to defend]. Available at: https://blog.kaspersky.ru/wannacry-ransomware/16147/ (date of access: 01.06.2017). (in Russian)

6. Boyer D. WikiLeaks figure says 'disgusted' Democrat leaked Clinton campaign emails. *The Washington Times.* Available at: http://www.washingtontimes.com/news/2016/dec/14/craig-murray-says-source-of-hillary-clinton-campai/ (date of access: 01.06.2017).

7. Durden T. WannaCry Ransomware Attack Linked to China, Not Russia or North Korea. Available at: http://www.zerohedge.com/news/2017-05-29/wannacry-ransomware-attack-linked-china-not-russia-or-north-korea (date of access: 01.06.2017).

8. Kalinina V.V., Mutsenek V.E. Mass Media as an Instrument of Information Confrontation. *On the Way to a Stable World: Security and Sustainable Development: a collection of scientific papers.* San Diego, Ron Bee & Associates, 2015, pp. 14-17.

9. McKelvey F., Dubois E. Propaganda in Canada: The Use of Political Bots. *The Computational Propaganda Project.* Available at: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Canada.pdf (date of access: 07.05.2018).

10. Prier J. Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 2017, vol. 11, issue 4, pp. 50-85.

11. Wang Wei. Linguistic Analysis Suggests WannaCry Hackers Could be From Southern China. *The Hacker News.* Available at: http://thehackernews.com/2017/05/china-wannacry-ransomware.html (date of access 01.06.2017).

Муценек Витус Евгеньевич
старший преподаватель, Институт математики, экономики и информатики
Иркутский государственный университет
Российская Федерация, 664003, г. Иркутск, ул. К. Маркса, 1
тел. 8(3952)242214
e-mail: 9043550@list.ru

Mutsenek Vitus Evgenievich
Senior Lecturer, Institute of Mathematics, Economics and Informatics
Irkutsk State University
1, K. Marx st., Irkutsk, 664003, Russian Federation
tel.: 8(3952)242214
e-mail: 9043550@list.ru

Дата поступления: 18.08.2017
Received: August, 18, 2017