DOI:10.17951/we.2018.4.2.171. | Wschód Europy • Восток Европы • East of Europe vol 4, 2 / 2018

Сергей Даниленко
ORCID ID: https://orcid.org/0000-0003-3873-2525

Юлия Нестеряк
ORCID ID: https://orcid.org/0000-0002-5955-7693

Марина Гринчук
ORCID ID: https://orcid.org/0000-0001-5835-2808

Институт международных отношений Киевского национального университета имени Тараса Шевченко, Украина

Современные тенденции в сфере коммуникационной безопасности

Последняя четверть двадцатого столетия, не говоря уже о начале нынешнего, на наш взгляд, в области управления как обществом, так и производственными процессами, характеризовалась стремлением ученых, разработчиков, политиков и бизнесменов ограничить влияние человеческого фактора. Поэтому в этот период так активно развиваются информационно-коммуникативные технологии, а гуманитарные направления стагнируют или теряют свой авторитет. Собственно, убрать человека, ограничить его несовершенное вмешательство в текущие процессы, в лучшем случае улучшить результат за счет использования искусственного интеллекта – это те задачи, которые в середине XX столетия решали главные мировые политические и научные центры. Если рассмотреть с этой точки зрения ведущие технологические компании мира, то Facebook и Google – это не что иное, как воплощение подтверждающего предубеждения (*confirmationbias*) в технологиях. Вместо того, чтобы бороться с проблемой однобокого восприятия, они его усиливают из-за того, что пользователи видят (в основном в медисфере – наиболее коммуникационно ориентированной) только то, что соответствует их психологическому профилю. Таким образом, постепенно разрушается основа научного общества – способность населения критически мыслить и сомневаться[1].

[1] Fritz Breithaupt and Martin Kolmar, *Akademiker*: *Wo Experten Zögern*, ZEIT Campus, 2018, https://www.zeit.de/2018/28/akademiker-wissenschaftler-intellektuelle-prestige-autoritaet [accessed 1 September 2018].

Украинские исследователи Д. Дубов и Н. Ожеван провозглашают «большой переход от machina ex homo до homo ex machina»[2]. Еще с большей решительностью они утверждают, что смена Модерна Постмодерном на уровне технологий ознаменована переходом от информационно-коммуникативных технологий третьей волны индустриализма (Industry 3.0) к нано-, био-, инфо-, когнитивно-кибернетических технологий четвертой волны (Industry 4.0). Авторы рассматривают возможности возникновения конвергентного общества, как общества трансгуманистического, тесно связанного с новым качеством проникновения технологий в природу человека[3].

Современная ситуация, которая демонстрирует сопротивление «всего человеческого» в нынешнем, еще информационном типе общества, побуждает говорить о необходимости различать технологическую, информационную безопасность и безопасность человека в информационной эпохе – коммуникативную.

Исследователи информационного пространства и сопредельных с ним сфер человеческой деятельности последовательно и настойчиво рекомендуют различать коммуникативную безопасность в противовес безопасности информационной, ядром которой по праву есть кибербезопасность. Об этом пишут в разных контекстах исследовательские центры и известные ученые. Но человеческое в человечестве сопротивляется тем подходам в политике, образовании, потреблении и развлечениях, где человека вынуждают двигаться по определенному алгоритму, упрощающие его когнитивные усилия. В июле 2018 года французский парламент проголосовал за законопроект о запрете использования гаджетов в младшей и средней школе, за исключением тех случаев, если эти устройства нужно будет использовать в образовательных целях. Такое нововведение было предвыборным обещанием президента Эммануэля Макрона, и уже с сентября 2018 года оно вступило в силу. Такая инициатива французских чиновников связана с новым мировым трендом, который получил название «цифровой детокс» (Digital detox). Это означает сознательный отказ от гаджетов на определенный промежуток времени, чтобы окунуться в какое-то дело или отдохнуть от внешнего мира, сконцентрировавшись на себе. А все потому, что все больше пользователей высоких технологий признают свою зависимость от гаджетов, а исследователи говорят об угрозе депрессии и других негативных последствиях из-за их чрезмерного использования[4].

В качестве примера приводится история одной семьи, описанная американским изданием New York Post под заголовком «Цифровой героин»: как гаджеты превращают детей в психотических наркоманов». Это рассказ о том, как мать приобрела шестилетнему сыну iPad, чтобы тот пользовался им в школе. Но потом ребенок ак-

[2] М. Ожеван, Д. Дубов, *Homo Ex Machina*, [в:] *Філософські, культурологічні та політичні передумови формування конвергентного суспільства. Монографія*, Київ: НІСД, 2017, с. 6.

[3] *Apple Reports Third Quarter Results*. Sec. gov, 2018, https://www.sec.gov/Archives/edgar/data/320193/000032019318000098/a8-kexhibit991q320186302018.htm [accessed 1 September 2018].

[4] *Франція гаджети у школах заборонила. А Україна?* Ukrinform.ua, 2018, https://www.ukrinform.ua/rubric-society/2509517-francia-gadzeti-u-skolah-zaboronila-a-ukraina.html?utm_source=messenger&utm_medium=0108 [accessed 1 September 2018].

тивно увлекся игрой «Minecraft», и одной ночью мать зашла в его комнату и с ужасом увидела, как он сидел не шевелясь, упав в кататонический ступор, в то время как рядом лежал iPad[5]. Специалист, описавший этот типичный случай, доктор Николас Кардарас – исполнительный директор одной из крупнейших в США реабилитационных клиник – Dunes, рассказывает, что процесс выздоровления от такой зависимости занял много усилий и времени, но через четыре года состояние пациента улучшилось и теперь он научился пользоваться гаджетами в меру.

Таким образом, мы указали одно из наиболее узнаваемых проявлений проблемы коммуникационной безопасности, состоящей в том, что она приводит к пассивности, уходу от действительности, «выпаданию» человека из реального мира, общественной жизни, где он может реализоваться, виртуализации восприятия происходящего вокруг тебя и с тобой (хотя сообщается и о новой тенденции)[6].

Крайняя форма такого поведения – суицидальные случаи. Известная история – деятельность сообщества «Синий кит», связанная с самоубийствами несовершеннолетних. В процессе давления на психику, подросток практически полностью погружается в «игру» и теряет ощущение реальности. Сейчас дети быстро выполняют свои минимальные обязанности и возвращаются обратно в киберпространство, требуя оставить их в покое. Именно таким образом ребенок отвлекается от реальности, и «в реальном мире остается лишь оболочка, тело, а душа ребенка, его интеллект – уже там»[7].

В последнее время широкую огласку получила смертельно опасная игра под названием «Момо». Несмотря на то, что первоначальную версию уже удалили, на данный момент существует множество клонов, которые считывают персональную информацию пользователей с гаджетов, и используют ее для шантажа. Принцип действия следующий: человек (чаще всего, это подросток) получает запрос на переписку в одной из социальный сетей. После добавления в список контактов и начала переписки, «Момо» начинает терроризировать пользователей ночными сообщениями пугающего содержания, с изображением сцен насилия и звонками. Также, «Момо» раздает различные задания, которые нужно обязательно выполнить. В случае невыполнения, «Момо» переходит к шантажу и угрозам. Не секрет, что все это приводил к суицидальным случаям[8].

---

[5] Nicholas Kardaras, *It'S 'Digital Heroin': How Screens Turn Kids Into Psychotic Junkies*, NY Post, 2018, https://nypost.com/2016/08/27/its-digital-heroin-how-screens-turn-kids-into-psychotic-junkies/ [accessed 1 September 2018].

[6] *Consumer Interest In VR Is Declining According To Sales Data Trends*, Thinknum, 2018, https://media.thinknum.com/articles/sales-data-shows-that-consumer-interest-in-vr-is-waning/ [accessed 1 September 2018].

[7] *Почему «Синий кит» убивает детей*, Politeka, 2018, https://politeka.net/news/410917-pochemu-sinij-kit-ubivaet-detej/ [accessed 1 September 2018].

[8] *Может заставить ночью пойти на кладбище или приставить нож к горлу чем опасна Момо*, „Факты", 2018, http://fakty.ua/277967-mozhet-zastavit-nochyu-pojti-na-kladbicshe-ili-pristavit-nozh-k-gorlu-chem-opasna-momo [accessed 1 September 2018].

Гораздо опаснее для человека, общества и государства нам представляется проблема, когда деструктивное коммуникативное влияние принуждает индивида, другими словами – пользователя, *к активным действиям*, опасным как для него самого, так и для окружающих. На наш взгляд, как раз в этом должно состоять ключевое направление в изучении коммуникативной безопасности. Это феномен мы наблюдали еще во время Арабской весны[9].

В своем докладе в Генштабе Вооруженных сил Украины эксперт по информационной политике и коммуникативным технологиям Г. Почепцов указал, что глобальное развитие и распространение новейших технологий, в частности, Интернет-технологий, обусловило необходимость рассматривать коммуникативную безопасность как одну из приоритетных задач сегодняшнего дня. Он убежден, что коммуникативное пространство принадлежит массовому сознанию, к нему имеет доступ каждый. Оно открыто как для своих, так и для чужих. Чаще всего, для облегчения проникновения в коммуникативное пространство создается псевдо-источник информации, сообщение которого начинают цитировать другие.

Изменение, оперативная заменяемость, вытеснение информации является тем, что отличает коммуникативное пространство от информационного. В коммуникативном пространстве информация меняется постоянно, в информационном – наоборот, тут преобладает не вытеснение старого – новым, а структурирование, архивация, закрытость. Поэтому, ценность текстов и сообщений в информационном пространстве значительно выше, ведь в коммуникативном пространстве они заменяются новыми слишком часто. Г. Почепцов также отмечает, что коммуникативное пространство сейчас борется за внимание потребителя, поскольку информации в настоящее время больше, чем нужно, и человек уже физиологически не в состоянии ее охватить. Есть необходимость в своеобразных «смысловых переводчиках», которые рассказывают о том, как понимать то или иное явление. «Защита коммуникативного пространства — это новая задача. Ее нельзя решать методами защиты информационного пространства», – считает ученый. Соответственно, этими двумя разными пространствами должны заниматься разные специалисты[10].

Таким образом, *первым доктринальным трендом* мы будем считать неминуемое дальнейшее разделение коммуникационной и информационной (с доминантой на кибербезопасности) безопасности на основе человеческой природы, ее физиологических, психологических и интеллектуальных особенностей.

Вторым направлением, которое, по нашему мнению, будет активно обсуждаться и к которому будут прилагаться усилия государств, общества и отдельного

[9] С. Даниленко, *Громадянський вимір комунікативної революції: модернізація суспільних комунікацій від друкарського верстата до соціальних мереж*, Київ: IMB, 2010, с. 310.

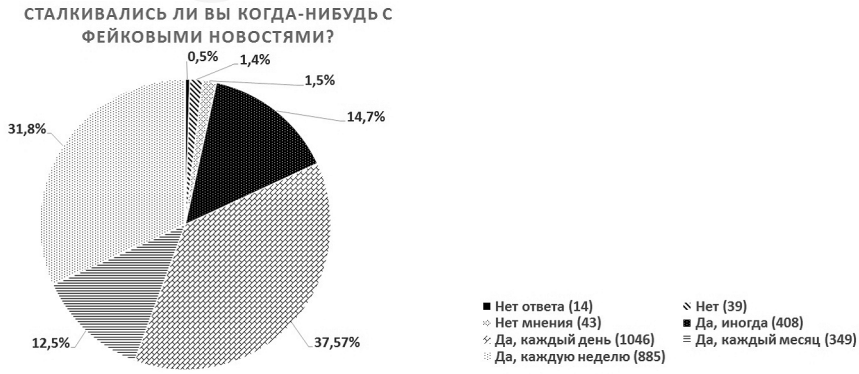
[10] Г. Почепцов, *Коммуникативная безопасность в противовес безопасности информационной*, „Хвиля", 2018, http://hvylya.net/analytics/society/georgiy-pocheptsov-kommunikativnaya-bezopasnost-v-protivoves-bezopasnosti-informatsionnoy.html [accessed 1 September 2018].

человека, является проблема нарастающей *дезинформации (disinformation)*, пришедшей на смену более мягкой угрозе коммуникативной безопасности – *постправде (post-trush)*.

По данным отчета Европейской Комиссии 2018, глобальная сеть стремительно развивается – сейчас существует около 1,3 млрд веб-сайтов и около 3,7 млрд пользователей, которые ежедневно пользуются Интернетом, обмениваются информацией. Согласно отчету Freedom House 2017 года, онлайн-манипуляция и дезинформация были официально зафиксированы во время выборов в минимум 18 странах.

Дезинформация – это постоянно действующий феномен, имеющий институциональный характер, т.е. продуцированный определенными структурами, в большинстве случаев – государственными, с четко очерченной целью и исполнителями, которые получают за это вознаграждение. Такая деятельность носит силовой характер, и ее последствия сопоставимы с действием других силовых факторов – энергетики, традиционного оружия, террористических атак и т.д. Развитие онлайн-платформ кардинально усложнило контроль потоков ложной информации. Согласно опросу Евробарометра, Международного проекта регулярных опросов общественного мнения (Eurobarometer), 83 процента европейцев считают фейковые новости угрозой демократии. Начиная с 2015 года, Оперативная рабочая группа по стратегическим коммуникациям EastStratComTaskForce собрала около 3900 примеров про-кремлевской дезинформации, которая была продублирована на разных языках и распространялась ежедневно[11].

По данным Европейской Комиссии за 2018 год, 37,6 процентов респондентов ежедневно сталкиваются с дезинформацией (на диаграмме)[12].



[11] *Digital Single Market TACKLING THE SPREADING OF DISINFORMATION ONLINE*, European Commission, 2018, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51605 [accessed 1 September 2018].

[12] *Synopsis Report Of The Public Consultation On Fake News And Online Disinformation*, European Commission, 2018, https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-online-disinformation [accessed 1 September 2018].

На основе приведенного анализа мы может утверждать, что в настоящее время ключевым вопросом коммуникативной безопасности является *защита от дезинформации.*

Главным источником «производства» дезинформации от институциональных (организованных, управляемых из единого центра) источников является Интернет. Причины увеличения количества неправдивой информации, по мнению исследователей, следующие:

- Интернет предоставляет возможность любому в любом месте публиковать какую-либо информацию;
- цифровой контент легко подделывать или оперативно изменять;
- многие люди имеют стимулы для распространения ложных сообщений;
- алгоритмы социальных сетей предоставляют большее предпочтение «эмоциональному контенту», чем рациональному, осмысленному, фактическому;
- общественность все больше обращается к цифровому Интернет-контенту с целью получения, назовем их условно, – «знаний»[13].

Задача преодоления или хотя бы нейтрализации дезинформации состоит в том, чтобы отличить ложную информацию от достоверной. Это задача не из простых для подавляющего большинства пользователей. Взять хотя бы недавний отчет в «Financial Times» относительно китайской версии популярного издания «The Washington Post». Сайт китайского издания полностью скопировал внешний вид сайта «The Washington Post» и использовал репутацию и популярность издания для привлечения большего количества читателей с китайским языком[14].

Согласно отчету за первую половину 2018 года Группы высокого уровня по противодействия фейковым новостям, действующей при Европейской Комиссии, предлагаются следующие методы борьбы с дезинформацией:

- повышение прозрачности новостей, публикуемых онлайн, и обмен информации о системах их распространения;
- стимулирование медийной и информационной грамотности для борьбы с дезинформацией и помощь пользователям в нахождения достоверной информации в сети Интернет;
- разработка инструментов для расширения возможностей пользователей и журналистов для борьбы с дезинформацией и содействие взаимодействию с новейшими информационными технологиями;
- сохранение разнообразия как базы устойчивого развития европейской медиасистемы;

[13] *How To Survive In The Fake-Information Age*, "Computer World", 2017, https://www.computerworld.com/article/3229925/internet/how-to-survive-in-the-fake-information-age.html [accessed 1 September 2018].

[14] *Fake News: Washington Post Clone Emerges In China*, "Financial Times", Ft.com, 2018, https://www.ft.com/content/fc4cf168-a2a3-11e7-9e4f-7f5e6a7c98a2 [accessed 1 September 2018].

- содействие дальнейшему исследованию влияния дезинформации для оценки уже принятых мер и разработки новых[15].

Подобные инициативы прозвучали и на конференции ОБСЕ «Усиление свободы и плюрализма средств массовой информации в Украине во время конфликта в Украине и вокруг нее», состоявшейся 26 июня 2018 г. в Киеве[16].

Что касается конкретных европейских стран, то Великобритания является одним из лидеров в борьбе с дезинформацией на государственном уровне[17]. Но даже это не помогло ей полностью уберечься от влияния во время референдума о выходе из ЕС. На официальных сайтах размещается информация для пользователей о том, как можно распознать фейковую информацию. Например, на сайте городского совета Ковентри (Coventry) содержится список вопросов, которые пользователи должны задать сами же себе. Если на большинство из них ответ «нет», это означает, что сообщение может быть фейковым. Кроме вопросов, на сайте содержится список проверенных веб-сайтов, где содержится правдивая информация, а также список онлайн-библиотек[18].

Британская регуляторная структура Ofcom опубликовала актуальный отчет о новостном потреблении британцев[19]. Респондентам пришлось в течение недели вести медиадневник, ежедневно записывая свои действия по отношения к потреблению информации. Основные выводы исследователей на базе глубинных интервью могут стать основой для научной гипотезы или прогноза, куда будет сосредоточен удар «институционализированной дезинформации». Еще раз довелось подтвердить, что главным устройством, проводником потребления новостей для современного человека стал смартфон. Три четверти респондентов поглощали новости в основном с мобильных устройств. При этом планшет – не мобильное устройство, его паттерны потребления схожи с компьютером. Обычно читатель с ноутбуком и планшетом лучше знает, чего он хочет. Иногда читатель вынужден использовать немобильное устройство, если смартфоном не принято пользоваться на работе.

В целом основной платформой потребления новостей остаются социальные медиа. Интерфейс новостной ленты становится повсеместно распространенным

---

[15] *JRC Digital Economy Working Paper*, 2018-02, European Commission, 2018, https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf [accessed 1 September 2018].

[16] *Конференція ОБСЄ: Дезінформація руйнує плюралізм ізсередини*, Detector media, 2018, https://detector.media/infospace/article/138943/2018-06-29-konferentsiya-obse-dezinformatsiya-ruinue-plyuralizm-izseredini/ [accessed 1 September 2018].

[17] *Local Government Association*, https://www.local.gov.uk/about/news/councils-warn-residents-about-fake-news-and-misinformation [accessed 2 September 2018].

[18] *Libraries – core services*, Coventry City Council, http://www.coventry.gov.uk/ffn [accessed 2 September 2018].

[19] *Scrolling news: The changing face of online news consumption. A report for Ofcom*, https://www.ofcom.org.uk/__data/assets/pdf_file/00 22/115915/Scrolling-News.pdf?utm_campaign=-ti-obma nul-svoego-redakt&utm_source=sendpulse&utm_medium= email&spush=c19kYW55bGVua29AdWtyLm5ldA [accessed 2 September 2018].

и удерживает людей внутри приложений[20]. Это затрудняет потребителю оценку новостей, так как они смешиваются с другими сообщениями – развлекательными, постами от друзей и т.п. А главное, что они могут смешиваться с интерпретацией, комментариями, оценками, легко превращаясь в постправду.

Поэтому главный стандарт медиапотребления – пассивное потребление новостей, а аналитика часто и не попадает в поле зрения рядового читателя. Смартфон побуждает читателя скроллить, свайпить и просматривать, а не искать, сравнивать и исследовать. Социальные медиа размывают границы между новостями и другим контентом. Это влияет на способность людей критически воспринимать то, что они видят. Пока нет утешительных прогнозов, что люди в скором времени осмысленно возьмутся за критическое восприятие потока новостей. Это факт будет оставаться той основой, которая будет стимулировать заинтересованные стороны к использованию дезинформации. Респонденты не всегда понимали, что какие-то из предложенных им историй были новостями; иногда понимали, но не относились к ним как к новостям. Главным показателем важности статьи, с их точки зрения, является ее популярность. Как ее можно «накачать» разными методами – тролли, боты и т.д.

Британский пример подсказывает нам ключевой вывод о том, что собственное мнение людей об их медиапотреблении не совпадает с их реальными привычками, реальным взаимодействием с медиа. Хотя многие знают о проблемах, сопровождающих новости – fake news, алгоритмы, «социальный пузырь» и, наконец, дезинформация с целью повлиять на вопросы социального устройства, – это знание не превращается в адекватное действие по отношению к таким негативным проявлениям в информационной сфере. Иными словами, знаем, но продолжаем игнорировать возможность того, что это происходи именно с тобой. Участники исследования согласны, что надо мыслить критически, но не практикуют такой подход, соприкасаясь с медиапространством, не «включают» критическое мышление. Они либо считают, что это слишком сложно, либо думают, что обладают врожденной способностью определять правдивость новостей. Появляются суеверия нового века. Так, молодые респонденты считают, что если у новости есть картинка или видео, то новости стоит доверять. Возможно, это последствия роста популярности таких форматов социальных сетей, как Instagram.

В обзоре «Борьба с дезинформацией: европейский подход» публикуется четыре основных принципа для противодействия этому явлению:

- улучшение прозрачности способа получения информации;
- разнообразие информации;
- достоверность информации;

[20] *Glavred.Info провел глобальный редизайн сайта*, MMR, 2018, http://mmr.ua/show/glavredinfo_provel_globalynyy_redizayn_sayta#1665853227.1535877535 [accessed 2 September 2018].

- инклюзивные решения с широким привлечением заинтересованных сторон[21].

Можно утверждать, что европейские политики, часть общества готовы вооружиться новыми знаниями, понимать особенности нынешней информационной ситуации в Европе и попытаться изменить сложившиеся традиции информационного потребления, как когда изменялась культура потребления, скажем, в сфере питания, переработке мусора или использования электромобилей. Эффективная пропагандистская деятельность с акцентом на дезинформацию, проводимая уже больше десятилетия Российской Федерацией, принудила к переосмыслению некоторых постулатов европейской жизни. Европейский комиссар по вопросам безопасности Джулиан Кинг (Julian King) убежден, что ЕС теперь лучше понимает, как Кремль распространяет дезинформацию. Благодаря детальному мониторингу ЕС было каталогизированы более 4 тыс. примеров дезинформации. Среди них была информация об отравлении Скрипалей в Солсбери (Великобритания) и про сбитый самолет MH17[22].

На основе и украинского, и собственного опыта последних годов ЕС разработал ряд мероприятий, направленных на противодействие манипуляциям и фейкам. Например, от Интернет-платформ в Европе планируют требовать большей прозрачности относительно того, кто использует микро-выборки для распространения месседжей. Сейчас инструменты в социальных медиа могут быть очень легко использованы – государствами или другими заинтересованными сторонами (экстремистами, радикалами, террористами) – для того, чтобы разрушить демократические системы и использовать их как оружие.

Страны-члены ЕС вскоре должны опубликовать свои планы по противодействию вмешательствам в выборы и способам получить данные избирателей. Комиссия стремится объединить усилия, чтобы преодолеть опасности от манипуляций в социальных сетях, которые называют «современным оружием массового уничтожения». По мнению европейских специалистов, злоупотребления в социальных сетях имеют три формы:

– усилия, направленные на изменение общественного мнения из-за появления вредной информации в «нужном месте» во время политических кампаний;
– фальшивые новости, которые помогают раскачать общественные настроения и повлиять на результат;

[21] *Fake News*, "Digital Single Market", 2018, https://ec.europa.eu/digital-single-market/en/fake-news [accessed 2 September 2018].

[22] D. Boffey, *Britain's Top EC Commissioner Lays Out Plan To Tackle 'Disinformation*, "The Guardian", 2018, https://www.theguardian.com/world/2018/jun/20/britains-top-eu-commissioner-lays-out-proposal-to-tackle-disinformation [accessed 2 September 2018].

– распространение целенаправленных месседжей на базе психометрии, для чего используют детальные данные о пользователях (то есть то, что сделала Cambridge Analytica).

Для нашего первого тренда – дезинформация приводит население к неосмысленным активным действиям – как раз две первые формы являются крайне важными. Ведь в условиях популистской демократии, каковой сегодня страдают или заражены большинство европейских демократий, политические кампании становятся наиболее уязвимыми к внешнему информационно-коммуникативному влиянию. Это можно было наблюдать во время президентских выборов во Франции, референдума в Каталонии или Brexit в Великобритании.

Европейцы работают над кодексом, который должен разъяснить пользователям Интернета, почему они видят те или иные месседжи и посты в социальных сетях. И Совет Европы, и Европейская комиссия системно публикую пресс-релизы и другие обобщенные материалы, которые направлены на распространение знаний и приобретение элементарных умений пользователей, которые обращаются к Интернету, к традиционным медиа как главному источнику знаний о мире.

Показательным в этом отношении может послужить опыт Украины, которая испытывает на себе открытое агрессивное информационное влияние Российской Федерации, где использование дезинформации является одним из ключевых инструментов деструктивного влияния. На наш взгляд, на сегодняшнем этапе волна российской дезинформации как раз и направлена на то, чтобы часть граждан Украины превратить в неосмысленную, ложно ориентированную, но при этом активную толпу. В условиях ощутимого, а местами и доминирующего, присутствия России в национальном информационном пространстве Украины да еще в преддверии президентской и парламентской избирательных кампаний, коммуникативная безопасность вновь обостряется и становится вопросом сохранения суверенитета и территориальной целостности государства, которое переживает период демократического транзита.

Украинское государство, первым столкнувшись с российской информационной агрессией, вынуждено было разрабатывать концептуальные документы для обеспечения своей информационно-коммуникационной безопасности в новых условиях. Уже в 2015 году был создан Экспертный совет при Министерстве информационной политики, первоочередным заданием которого стала разработка проекта Концепции информационной безопасности Украины. Документ стал основой, идейным источником итогового документа – Доктрины информационной безопасности, принятой Советом национальной безопасности и обороны[23].

Следует отметить, что уже этот документ был больше ориентирован как раз на вопросы не информационной, а коммуникационной безопасности. В нем,

[23] Указ Президента України №47/2017. Офіційне Інтернет-Представництво Президента України, 2018, https://www.president.gov.ua/documents/472017-21374 [accessed 2 September 2018].

кроме идеи об устойчивом развитии украинского общества в информационную эпоху, предусматривалось еще и активное участие гражданина, наравне с обществом и государством, как равноправного субъекта в формировании информационно-коммуникационной безопасности страны. В частности, в документе разработан концепт «стратегический контент» и поставлен вопрос о необходимости его имплементации в практику коммуникационной деятельности соответствующих государственных учреждений. Этот концепт для нас важен в разрезе коммуникационной безопасности в том смысле, что он работаем в связке с другим важным атрибутом – «стратегическим нарративом» ориентированным исключительно на работу с человеческим когнитивным аппаратом.

Важным является также предложение о необходимости наладить эффективную деятельность соответствующего координационного органа в сфере государственной информационно-коммуникативной политики, четко определив его функциональные задачи. Таким органом может стать структурное подразделение – назовем его «Ситуативный кабинет», который работает в сфере задач Совета национальной безопасности и обороны Украины.

Наработанные документы вводят в нормативные акты и практику коммуникативной деятельности государственных и общественных структур понятия, которые долгое время оставались предметом исключительно научных исследований. Кроме упомянутого выше стратегического контента, также: национальный информационный продукт, государственная информационная политика, национальное информационное пространство (киберпространство, кибербезопасность) и др.

Наконец, третьей тенденцией в сфере коммуникационной безопасности следует считать *невозможность преодоления или полной нейтрализации негативных последствий* действия институционально продуцированной, целенаправленной дезинформации. Даже при нынешнем развитии средств и методов распространения информации как индивидуально, так и массово, нейтрализации будет лишь частичной.

Первая и главная причина та, что человек имеет достаточно ограниченный по отношению к новым требованиям когнитивный аппарат. Точнее, он, возможно, больше ориентирован на накопление информации, работу с объемом, но не качеством информации. Ее качественная обработка – довольно новое цивилизационное приобретение человечества, и то не всех его представителей, а лишь части. Сегодня людям нужна способность осмысливать информацию, отличать важное от второстепенного и даже вредоносного. И, прежде всего, объединять большое количество фрагментарной информации в общую картину мира[24].

Г. Почепцов выдвигает гипотезу, что расширенные возможности дезинформации связаны с возросшими потоками информации, которые потребитель уже

[24] Юваль, Ной Гарарі, *Що 2050-й рік готує людству*, ZBRUC, https://zbruc.eu/node/82383 [accessed 2 September 2018].

не может адекватно оценивать. Одновременно любой сегодняшний текст выстроен так, чтобы забрать внимание аудитории. Таким образом, внимание как характеристика нашего когнитивного аппарата отстает от динамики технологий и политического, общественного заказа. К коллективному источнику информации (государь и его бюрократия, кардиналы и митрополиты, общественные собрания, а позже – традиционные СМИ) социальные медиа сделали каждого их нас источником информации. В результате мы имеем не просто много сообщений; они еще и ориентированы на то, чтобы захватить внимание потребителя, ведь большие объемы информации сделали дефицитом не информацию, а внимание. Внимание же, в отличие от информации, оказалось ресурсом ограниченным: у человека ограниченное время для работы с информацией[25].

По каким-то причинам думать и самостоятельно принимать решения, нести ответственность на основе полученной извне информации оказывается для современно человечества все больше непомерной ношей. Нельзя утверждать, что сегодня человечество более безответственно. Человек и раньше был готов обманываться. Но список источников информации для жителя средневекового города был несравнимо уже.

Перегруженное внимание и наслоение информации мешает человеку принимать взвешенное решение, что ему, собственно, и вредит в вопросах оценки явлений в информационной сфере. Внимание скользит по монитору компьютера и одно сообщение вытесняется следующим, все же оставляя часть предыдущей картины мира. Таким образом, деструктивная информация не вытесняется целиком. На этот феномен обратили внимание американские ученые. Сайт FiveThirtyEight, который специализируется на статистическом анализе, опубликовал датасет с тремя миллионами твиттов российских троллей – результат работы двух профессоров Clemson University Дарена Линвила и Патрика Уоррена[26].

В контексте нашего исследования нам интересен тот вывод упомянутых коллег, что стирание твиттов из аккаунтов, идентифицированных Twitter как тролли, не несет особой пользы, ведь ущерб уже был нанесен, а для предупреждения будущих атак неплохо было бы использовать информацию, полученную в результате предыдущего анализа. Но внимание сосредоточенно на новом сообщении. Теряется смысл прикладывать усилия к разоблачению деструктивной информации. Особенно, если это касается перенастройки смыслов. Переподключение нейронов и перемонтаж синапсов – очень тяжелая работа (Гарари). Значит можно утверждать, что действует феномен невозможности преодоления или полной нейтрализации негативных последствий влияния дезинформации.

[25] Г. Почепцов, *Усиление борьбы с дезинформацией*, Research Gate, https://www.researchgate.net/publication/326096950 _Usilenie_borby_s_dezinformaciej [accessed 2 September 2018].

[26] O. Roeder, *Why We'Re Sharing 3 Million Russian Troll Tweets*, Five Thirty Eight, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/ [accessed 2 September 2018].

В связи с коммуникационной безопасностью можно говорить лишь о частичной коррекции. Поэтому процесс «коммуникационного оздоровления» протекает сложно и довольно неопределенное время при наличии надлежащих условий – повышения уровня информационного образования, максимальной блокировки вредоносного контента, активного и системного продуцирования собственных нарративов и т.д. Тут нет единого рецепта усиления коммуникационной безопасности с учетом максимальной открытости такого пространства. Приходится учить людей от обратного – не верить медиа, особенно социальным сетям[27]. Современные СМИ не выполняют должным образом своих функций – давать обществу не только знание фактов, но и понимание того, что происходит[28].

Подытоживая, отметим, что сегодня достаточно научных и практических оснований различать коммуникационную и информационную безопасность, учитывая их особенности к открытости и противоположных векторов в стремлении расширить/ограничить участие разных субъектов в работе с информацией. На наш взгляд, это ключевой тренд в понимании того, как нужно менять подходы в работе с информацией, особенно той, что продуцируется институционально.

Соответственно, ключевым вопросом коммуникативной безопасности является защита от дезинформации, которая, в отличии от фейков, есть продукт не индивидуального, а институционального производства. Тут мы находим полностью осознанный процесс, который имеет четкие задачи, заказчика и исполнителя. Эти его особенности дают нам основания в правовой плоскости выводить его за рамки свободы слова и поступать соответственно.

Наконец, ограниченность человеческих когнитивных возможностей, если брать не теоретическую, а практическую сторону, в первую очередь возрастающий дефицит внимания, возросшую вследствие технической революции «текучесть» новостей, диктует невозможность преодоления или полной нейтрализации негативных последствий влияния дезинформации, ее последствий, прежде всего на протекание общественно-политической жизни общества. Соответственно, это будет производной и для других сфер жизни современно информационно-коммуникационного общества – экономики, науки, образования, сферы развлечений и досуга. Задача будет состоять в способности того или иного человеческого сообщества прогнозировать и регулировать такое влияние.

[27] *У Twitter та Youtube запустили фейкову інформаційну кампанію «Не Вір Кожному Твіту»*, Media Sapiens, 2018, http://ms.detector.media/ethics/manipulation/u_twitter_ta_youtube_zapustili_feykovu_informatsiynu_kampaniyu_ne_vir_kozhnomu_tvitu/ [accessed 2 September 2018].

[28] *Війна і ЗМІ: про систему координат*, detector.media, 2018, https://detector.media/infospace/article/140198/2018-08-16-viina-i-zmi-pro-sistemu-koordinat [accessed 2 September 2018].

Аннотация: Авторы обосновывают утверждение, что в современном информационном поле следует различать коммуникационную и информационную безопасность. Эти две разновидности отличает доминирование человеческого фактора, если говорить о коммуникационной безопасности. А технический компонент распространения, сохранения и защиты информации в этом понимании занимает второстепенное значение, но актуализируется, когда мы говорим о безопасности информационной, где существует тенденция к закрытости пространства.

Гораздо опаснее для человека, общества и государства, по мнению авторов, является проблема, когда деструктивное коммуникативное влияние принуждает индивида (пользователя) к активным действиям, опасным как для него самого, так и для окружающих. Первым доктринальным трендом в сфере коммуникационной безопасности авторы называют неминуемое дальнейшее разделение на основе человеческой природы, ее физиологических, психологических и интеллектуальных особенностей, коммуникационной и информационной (с доминантой на кибербезопасности) безопасности. Вторым направлением, которое, по их мнению, будет активно обсуждаться и к которому будут прилагаться усилия государств, общества и отдельного человека, будет проблема нарастающей дезинформации (disinformation), пришедшая на смену более мягкой угрозе коммуникативной безопасности – постправде (post-truth). Наконец, третьей тенденцией в сфере коммуникационной безопасности следует считать невозможность преодоления или полной нейтрализации негативных последствий действия институционально продуцированной, целенаправленной дезинформации. Даже при нынешнем развитии средств и методов распространения информации как индивидуально, так и массово, нейтрализация может быть лишь частичной. Поэтому наименьшие последствия влияния деструктивной информации, иными словами – эффективная коммуникационная безопасность, буде там, где «информационное здоровье» человека, общества и государства будет максимально обеспечено их общими усилиями.

Ключевые слова: коммуникативная безопасность, информационная безопасность, кибербезопасность, дезинформация, эмоциональный контент, подтверждающее предубеждение, конвергентное общество, когнитивизм, нарратив

Aktualne trendy w sferze komunikacji bezpieczeństwa

Streszczenie: Autorzy uzasadniają twierdzenie, że współczesna przestrzeń informacyjna powinna wyróżniać bezpieczeństwo komunikatywne i bezpieczeństwo informacyjne. Te dwa typy wyróżniają się dominacją czynnika ludzkiego, jeśli mówimy o bezpieczeństwie komunikatywnym. Komponent techniczny dystrybucji, przechowania i ochrony informacji ma znaczenie drugorzędne. Niemniej jednak staje się to istotne, gdy mówimy o bezpieczeństwie informacyjnym, które ma tendencję do zamkniętej przestrzeni.

Bardziej niebezpieczny dla osoby, społeczeństwa i państwa, zdaniem autorów, jest problem, gdy niszczący wpływ komunikacyjny zmusza osobę (użytkownika) do podjęcia aktywnych działań, niebezpiecznych zarówno dla niego samego, jak i dla innych. Jako pierwszy doktrynalny trend w dziedzinie

bezpieczeństwa komunikacyjnego autorzy podają nieuniknioną dalszą separację opartą na ludzkiej naturze, jej fizjologicznych, psychologicznych i intelektualnych cechach, bezpieczeństwo komunikacyjne i bezpieczeństwo informacyjne (z dominującym bezpieczeństwem cybernetycznym). Drugi kierunek, który ich zdaniem będzie aktywnie dyskutowany i który będą stosować państwa, społeczeństwa i jednostki, to problem zwiększenia dezinformacji (*disinformation*), zastępujący łagodniejsze zagrożenie bezpieczeństwa komunikacyjnego – post-prawdy (*post-truth*). Trzecią tendencją w dziedzinie bezpieczeństwa komunikacyjnego jest niemożność przezwyciężenia lub całkowitego zneutralizowania negatywnych skutków działania celowej dezinformacji produkowanej instytucjonalnie. Nawet przy obecnym rozwoju mediów neutralizacja może być tylko częściowa. Dlatego też najmniejsze konsekwencje oddziaływania niszczącej informacji, skutecznego bezpieczeństwa komunikacji będą tam, gdzie „zdrowie informacyjne" osoby, społeczeństwa i państwa będzie maksymalnie zapewnione przez ich wspólne wysiłki.
Słowa kluczowe: bezpieczeństwo komunikacyjne, bezpieczeństwo informacyjne, cyberbezpieczeństwo, dezinformacja, treść emocjonalna, społeczeństwo konwergentne, kognitywizm, narracja

Current Trends in Communication Security

Abstract: Authors claim that in the modern information field one should differentiate between communication and information security. These two types are distinguished by the dominance of the human factor, as far as communication security is concerned. A technical component of the distribution, preservation and protection of information is of the secondary importance. Nevertheless, it becomes relevant when we talk about information security, which has a tendency to closed space.

Authors claim that for a person, society and state it is much more dangerous when a destructive communicative influence forces an individual (user) to take active actions, which are dangerous both for himself and for others. The first doctrinal trend in the field of communication security is the inevitable further separation of communication and information (with a dominant cyber security) security, based on human nature, its physiological, psychological and intellectual features. Authors claim that the second direction, which will be actively discussed and to which the efforts of states, society and the individual will be applied, is the problem of increasing disinformation that came after the milder threat of communicative security – post-truth. And the third tendency in the field of communication security is the impossibility of overcoming or completely neutralizing the negative consequences of the action of institutionally produced, purposeful disinformation. Even with the current development of the means and methods of disseminating of information both individually and en masse, neutralization can only be partial. Therefore, the least consequences of the impact of destructive information, in other words, the effective communication security will be possible if the "informational health" of a person, society and the state is ensured by their common efforts.
Keywords: communicative security, information security, cyber security, disinformation, emotional content, confirming prejudice, convergent society, cognitivism, narrative

Список литературы

Apple Reports Third Quarter Results, Sec.gov, 2018, https://www.sec.gov/Archives/edgar/data/320193/000032019318000098/a8-kexhibit991q320186302018.htm [accessed 1 September 2018].

Boffey D., *Britain's Top EC Commissioner Lays Out Plan To Tackle 'Disinformation'*, "The Guardian", 2018, https://www.theguardian.com/world/2018/jun/20/britains-top-eu-commissioner-lays-out-proposal-to-tackle-disinformation [accessed 2 September 2018].

Breithaupt FM Kolmar, *Akademiker: Wo Experten Zögern*, ZEIT Campus, 2018, https://www.zeit.de/2018/28/akademiker-wissenschaftler-intellektuelle-prestige-autoritaet [accessed 1 September 2018].

Digital Single Market TACKLING THE SPREADING OF DISINFORMATION ONLINE, European Commission, 2018, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51605 [accessed 1 September 2018].

Fake News, "Digital Single Market", 2018, https://ec.europa.eu/digital-single-market/en/fake-news [accessed 2 September 2018].

Fake News: Washington Post Clone Emerges In China, "Financial Times", Ft.com, 2018, https://www.ft.com/content/fc4cf168-a2a3-11e7-9e4f-7f5e6a7c98a2 [accessed 1 September 2018].

Glavred.Info провел глобальный редизайн сайта, MMR, 2018, http://mmr.ua/show/glavredinfo_provel_globalynyy_redizayn_sayta#1665853227.1535877535 [accessed 2 September 2018].

How To Survive In The Fake-Information Age, "Computer World", 2017, https://www.computerworld.com/article/3229925/internet/how-to-survive-in-the-fake-information-age.html [accessed 1 September 2018].

JRC Digital Economy Working Paper, 2018-02, Europeam Commission, 2018, https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf [accessed 1 September 2018].

Kardaras N., *It'S 'Digital Heroin': How Screens Turn Kids Into Psychotic Junkies*, NY Post, 2018, https://nypost.com/2016/08/27/its-digital-heroin-how-screens-turn-kids-into-psychotic-junkies/ [accessed 1 September 2018].

Libraries – core services, Coventry City Council, http://www.coventry.gov.uk/ffn [accessed 2 September 2018].

Local Government Association, https://www.local.gov.uk/about/news/councils-warn-residents-about-fake-news-and-misinformation [accessed 2 September 2018].

Roeder O., *Why We'Re Sharing 3 Million Russian Troll Tweets*, FiveThirtyEight, 2018, https://fivethirtyeight.com/features/why-were-sharing-3-million-russian-troll-tweets/ [accessed 2 September 2018].

Scrolling news: The changing face of online news consumption A report for Ofcom, https://www.ofcom.org.uk/__data/assets/pdf_file/0022/115915/Scrolling-News.pdf?utm_campaign=-ti-obma nul-svoego-redakt&utm_source=sendpulse&utm_medium= email&spush=c19kYW55bGVua29AdWtyLm5ldA [accessed 2 September 2018].

Synopsis Report Of The Public Consultation On Fake News And Online Disinformation, European Commission, 2018, https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-online-disinformation [accessed 1 September 2018].

Війна і ЗМІ: про систему координат, detector.media, 2018, https://detector.media/infospace/article/140198/2018-08-16-viina-i-zmi-pro-sistemu-koordinat [accessed 2 September 2018].

Георгий Почепцов: Коммуникативная безопасность в противовес безопасности информационной, „Хвиля", 2018, http://hvylya.net/analytics/society/georgiy-pocheptsov-kommunikativnaya-bezopasnost-v-protivoves-bezopasnosti-informatsionnoy.html [accessed 1 September 2018].

Почепцов Г., *Усиление борьбы с дезинформацией*, Research Gate, https://www.researchgate.net/publication/326096950_Usilenie_borby_s_dezinformaciej [accessed 2 September 2018].

Даниленко С., *Громадянський вимір комунікативної революції: модернізація суспільних комунікацій від друкарського верстата до соціальних мереж*, Київ: IMB, 2010, с.310.

Конференція ОБСЄ: Дезінформація руйнує плюралізм ізсередини, detector media, 2018, https://detector.media/infospace/article/138943/2018-06-29-konferentsiya-obse-dezinformatsiya-ruinue-plyuralizm-izseredini/ [accessed 1 September 2018].

Может заставить ночью пойти на кладбище или приставить нож к горлу: чем опасна Момо, „Факты", 2018, http://fakty.ua/277967-mozhet-zastavit-nochyu-pojti-na-kladbicshe-ili-pristavit-nozh-k-gorlu-chem-opasna-momo [accessed 1 September 2018].

Ожеван М., Дубов Д., *Homo Ex Machina*, [в:] *Філософські, культурологічні та політичні передумови формування конвергентного суспільства: Монографія,* Київ: НІСД, 2017, с.6.

Почему «Синий кит» убивает детей, „Politeka", 2018, https://politeka.net/news/410917-pochemu-sinij-kit-ubivaet-detej/ [accessed 1 September 2018].

У Twitter та Youtube запустили фейкову інформаційну кампанію «Не вір кожному твіту», Media Sapiens, 2018 http://ms.detector.media/ethics/manipulation/u_twitter_ta_youtube_zapustili_feykovu_informatsiynu_ kampaniyu_ne_vir_kozhnomu_tvitu/ [accessed 2 September 2018].

Указ Президента України №47/2017. Офіційне Інтернет-Представництво Президента України, 2018, https://www.president.gov.ua/documents/472017-21374 [accessed 2 September 2018].

Франція гаджети у школах заборонила. А Україна? Ukrinform.ua, 2018, https://www.ukrinform.ua/rubric-society/2509517-francia-gadzeti-u-skolah-zaboronila-a-ukraina.html?utm_source=messenger&utm_medium=0108 [accessed 1 September 2018].

Юваль, Ной Гарарі, *Що 2050-й рік готує людству*, ZBRUC, https://zbruc.eu/node/82383 [accessed 2 September 2018].