МРНТИ 19.61 https://doi.org/10.26577/HJ.2022.v66.i4.07

А.А. Ниязгулова*, Л.И. Тунгатарова

Международный университет информационных технологий, Казахстан, г. Алматы
*e-mail: nijasgulova@gmail.com

ТЕОРИЯ «СЕКЬЮРИТИЗАЦИИ» И ПРОБЛЕМА ПОЛИТИЧЕСКОЙ РИТОРИКИ В СОЦИАЛЬНЫХ СЕТЯХ

Под «информационной безопасностью» подразумевают комплекс мер, необходимых для защиты от утечки или взлома компьютерных систем, программ и данных. Однако в последнее время подходы к изучению информационной безопасности наполняются новыми социальными и политическими смыслами. Понятие «национальная безопасность» включает все новые референтные объекты, например, «кибербезопасность», связанную с предотвращением угроз и вызовов социально-политического характера, возникших с появлением социальных сетей и мессенджеров. Подобного рода понимание «кибербезопасности» в западных академических кругах получило теоретическое оформление в концепции Cyber Security Politics, рассматривающей «информационную безопасность» в контексте «интернет безопасности». На появление и развитие данного подхода во многом оказала влияние концепция «секьюритизации» речевых актов Копенгагенской школы.

Основные цели исследования – определить, как «кибербезопасность» связана в целом с теорией и практикой государственной политики безопасности, какова роль риторики политиков, специалистов медиасферы в социальных сетях, в избирательных кампаниях; показать методы воздействия слова на обеспечение и сохранение информационной безопасности.

На основе контент-анализа и дискурсивного анализа речевых актов, используемых в социальных сетях, таких как Фейсбук, Твиттер и др., получены следующие результаты: обозначена важность постановки проблемы угрозы социальных сетей безопасности человека и общества (в случаях использования соцсетей в преступных целях), указана необходимость решения проблемы на законодательном уровне.

Угрозы кибербезопасности являются одним из основных вызовов национальной безопасности, общественной безопасности, политики и экономики, с которыми сталкивается каждое государство в XXI веке. Кроме того, наличие многочисленных проблем кибербезопасности в различных сферах жизни естественным образом повышает политическую заинтересованность в их решении.

В частности, этот вопрос урегулирования угроз, исходящих от мессенджеров, находится на рассмотрении Конгресса США с точки зрения соответствия Конституционным положениям о свободе слова. Новизна исследования заключается в анализе казахстанского сегмента интернет-пространства, проведен сравнительный анализ проблемных случаев киберугроз в США и России. Результаты исследования имеют практическое значение для медиаспециалистов, контент-менеджеров социальных сетей в целях обеспечения интернет-безопасности.

Ключевые слова: «кибербезопасность», предотвращение социальных и политических угроз и вызовов, социальные медиа, риторика.

A.A. Niyazgulova*, L.I. Tungatarova

International Information Technologies University, Kazakhstan, Almaty
*e-mail: nijasgulova@gmail.com

The “Securitization” theory and the problem of political rhetoric in social networks

In the usual sense, “information security” means a set of measures necessary to protect against leakage or hacking of computer systems, programs and data. However, recently the concept of security has begun to change – in connection with this, the approach to the concept of information security has begun to be filled with new social and political meanings. Cyberspace is a defining feature of modern life.

Therefore, the concept of “national security” began to extend in terms of “Cyber Security Politics”, concept including new reference objects, such as Internet networks and messengers, socio-political threats and challenges. The emergence and development of this approach was largely influenced by the theory of speech acts of the Copenhagen School “securitization” concept.

The main purpose of the study is to determine how “cybersecurity” is connected in general with the theory and practice of state security policy, to determine the role of politicians and media specialists’ rhetoric in social media, in election campaigns; and to show the methods of speech acts influence on ensuring and maintaining information/Internet security.

Based on content analysis and discursive analysis of speech acts used in social media such as Facebook, Twitter and others, the following results were obtained: the importance of posing the problem of

the social threat of social media to the formation of mass consciousness is indicated, the need to solve the problem at the legislative level is pointed.

Cybersecurity threats are one of the main national security, public safety, politics and economy challenges every nation faces in XXI century. The existence of numerous cyber security issues on various spheres of life naturally increase political interest in resolving them.

The novelty of the study lies in the analysis of the Kazakhstani segment of the Internet, comparative analysis with problematic cases of cyber threats in the USA and Russia. The results of the study are of practical importance for the media professionals, content managers of social media, in order to mainain the Internet security.

Keywords: cybersecurity, concept of "securitization", preventing threats and challenges of a socio-political nature, social media, rhetoric.

А.А. Ниязгулова*, Л.И. Тунгатарова

Халықаралық ақпараттық технологиялар университеті, Қазақстан, Алматы қ.

*e-mail: nijasgulova@gmail.com

«Қауіпсіздік» теориясы және әлеуметтік желілердегі саяси риторика мәселесі

«Ақпараттық қауіпсіздік» деп компьютерлік жүйелердің, бағдарламалардың және деректердің жария болуынан немесе бұзудан қорғау үшін қажетті шаралар кешені түсіндіріледі. Соңғы кезде «қауіпсіздік» ұғымы жаңа мәнге ие болды, осыған байланысты ақпараттық қауіпсіздік түсінігіне көзқарас жаңа әлеуметтік және саяси мағыналармен толтырыла бастады.

Киберкеңістік – қазіргі өмірдің айқындаушы белгісі, сондықтан «ұлттық қауіпсіздік» ұғымына әлеуметтік желілер мен мессенджерлердің пайда болуымен туындаған әлеуметтік-саяси сипаттағы қауіптер мен сын-қатерлердің алдын алу тұрғысынан «киберқауіпсіздік» ұғымы сияқты барлық жаңа анықтамалық объектілер кіре бастады.

Батыс академияларындағы «киберқауіпсіздік» туралы осындай түсінік «интернет қауіпсіздігі» контекстінде «ақпараттық қауіпсіздікті» қарастыратын Cyber Security Politics тұжырымдамасында теориялық айшықтауға ие болды. Бұл көзқарастың пайда болуы мен дамуына Копенгаген мектебінің сөйлеу актілерін «секьюритизациялау» концепциясы көп әсер етті.

Зерттеудің негізгі мақсаты – «киберқауіпсіздік» тұтастай алғанда мемлекеттік қауіпсіздік саясатының теориясы мен практикасымен қалай байланысты екенін анықтау, саясаткерлердің, әлеуметтік медиа мамандарының, сайлау науқандарындағы риторикасының рөлін анықтау және сөздің ақпараттық қауіпсіздікті қамтамасыз ету мен сақтауға әсер ету әдістерін көрсету.

Facebook, Twitter және басқалары сияқты әлеуметтік желілерде қолданылатын сөйлеу актілерін контент-талдау және дискурсивті талдау негізінде келесі нәтижелер алынды: бұқаралық сананы қалыптастыруға әлеуметтік желілердің қоғамдық қауіп-қатері мәселесін қоюдың маңыздылығы айқындалған, мәселені заңнамалық деңгейде шешу қажеттілігі көрсетілген.

Киберқауіпсіздікке төнетін қатерлер – XXI ғасырда әрбір мемлекет алдында тұрған ұлттық қауіпсіздіктің, қоғамдық қауіпсіздіктің, саясат пен экономиканың негізгі сын-қатерлерінің бірі. Сонымен қатар өмірдің әртүрлі салаларында көптеген киберқауіпсіздік мәселелерінің болуы оларды шешуге саяси қызығушылықты арттырады. Атап айтқанда, мессенджерлерден туындайтын қауіп-қатерлерді шешудің бұл мәселесі сөз бостандығы туралы конституциялық ережелерге сәйкес келу тұрғысынан АҚШ Конгресінің қарауында жатыр.

Зерттеудің жаңалығы – интернет-кеңістіктің қазақстандық сегментін талдау, АҚШ пен Ресейдегі киберқауіптердің проблемалық жағдайларын салыстырмалы талдау. Зерттеу нәтижелері интернет қауіпсіздігін қамтамасыз ету мақсатында медиа мамандар, әлеуметтік желілердің контент-менеджерлері үшін практикалық маңызға ие.

Түйін сөздер: «киберқауіпсіздік», қоғамдық-саяси сипаттағы қауіптер мен сын-қатерлердің алдын алу, әлеуметтік желі, риторика.

Введение

На сегодняшний день национальная безопасность стала включать все новые референтные объекты, к числу которых относится и концепция «информационной безопасности», «кибербезопасности» с точки зрения предотвращения угроз и вызовов социально-политического характера. Подобного рода понимание «кибербезопасности» в западных академических кругах получило теоретическое оформление в концепции Cyber Security Politics. Круг вопросов, поднимаемых данной концепцией в русском переводе, можно было бы перевести как «интернет-безопасность», поскольку понятие «информационная безопасность» имеет и более «узкое» понимание, связанное в основном с хакерскими атаками, взломами сайтов и баз личных данных пользователей, несанкционированным доступом, перехватом, хищением информации и т. п. (Myriam Dunn Cavelty, Andreas Wenger, 2022:1).

Большинство современных исследователей придерживаются точки зрения, согласно которой безопасность определяется как состояние защищенности личности, общества и государства от внешних и внутренних угроз. Очень долгое время понятие безопасности связывалось прежде всего с военной угрозой, но после окончания «холодной войны», а также в связи с масштабным развитием научно-технической революции и, в частности, информационных технологий, данное понятие стало наполняться новым содержанием.

Актуальность. При таком противоречивом подходе к решению проблемы информационной безопасности в мире, даже при наличии общей обеспокоенности глобальных возможностей ITтехнологий в практически мгновенном распространении информации любого характера, актуальность обсуждения этих проблем в академической сфере с каждым годом все более возрастает.

По мнению специалистов из швейцарского Center for Security Studies, ETH Мириам Кавелти и Андреаса Вернера: «В современном мире возникает необходимость защиты национальных ресурсов и тайны обмена информацией, так как эта информация может спровоцировать конфликты политического и экономического характера между государствами и в конечном итоге привести к краху международных отношений.”

Цель исследования – определить, как «кибербезопасность» связана в целом с теорией и практикой государственной, экономической, социальной, экологической, военной политики безопасности, определить место риторики речевых актов политиков и специалистов медиасферы в теории «секьюритизации», распространяемые через мессенджеры.

Объектом исследования являются социальные сети Facebook, Twitter, YouTube на предмет анализа речевых риторик политиков и проблемы информационной или кибербезопасности в более широком общественно-политическом контексте.

Материал и методы исследования

В ходе исследования использованы такие методы как контент анализ СМИ, социальных сетей, анализ новых ИТ технологий и цифровых инструментов распространения информации. Методология опирается на концепцию секьюритизации Копенгагенской школы, сделан анализ взаимосвязи мыслей Копенгагенской, Парижской и израильской школ исследований и выводы об общей гуманистической направленности теории.

Научная методология. Рассматривая хронологию теоретических взглядов на процессы информатизации и проблемы безопасности, связанные с масштабным внедрением информационных технологий, можно сказать, что для первых концепций (О. Гайдаев, 2021:5) формирующегося «информационного» общества была свойственна надежда на проникновение научно-технической рациональности во все сферы жизнедеятельности общества, которая могла позволить гармонизировать его и максимально упорядочить. Это была пора технократического оптимизма, веры в успех власти технократов и неудержимого научно-технического прогресса.

В свою очередь работы более позднего периода (Roszak T., 2000) отличались уже меньшей степенью научно-технического фанатизма и большим вниманием к психологическим, духовно-нравственным, гуманистическим сторонам развития информационной цивилизации.

Очевидно, что существующие подходы, взгляды и концепции обеспечили основу для современного, более широкого понимания концепции безопасности.

Среди самых влиятельных научных школ, разработавших одну из самых востребованных концепций безопасности следует отметить Копенгагенскую школу. Здесь следует обратить внимание на несколько ключевых достижений исследователей Копенгагенской школы, которые коренным образом повлияли на развитие исследований безопасности, предложив так называемую концепцию «секьютиризации».

Среди основных положений данной концепции можно отметить создание расширенного понятия безопасности, которое больше не ограничивается военным содержанием. Авторы концепции «секьютиризации» предложили пять так называемых основных наиболее значимых «секторов» безопасности, включающих помимо военного, также: политический; экологический; экономический и социальный.

Придание исследованиям безопасности максимально междисциплинарный характер и разработка аналитического понятия «секьюритизация», помогает в исследовании того, как тот или иной случай может быть отнесен или не отнесен к вопросам безопасности (Williams Paul D,2008). Подобный подход лег в основание более объ-

ёмного понятия информационной безопасности, включив в него социально-политические аспекты.

Безопасность в первую очередь означает состояние, при котором отсутствуют какие-либо деструктивные элементы – риски, опасности или угрозы. Под такими деструкциями понимаются явления, действия, процессы, факторы и события, которые могут негативно повлиять на функционирование системы безопасности общества и государства.

Насколько деструктивны могут быть в данном контексте современные информационные технологии, в частности, так называемый Интернет-концепт Web 2.0?

Прямого ответа этот вопрос пока нет, но он лежит в основе политических и академических дебатов по данному вопросу.

Заслуга авторов концепции «секьюритизации» Копенгагенской школы состоит в том, что они одними из первых начинают говорить о том, что рассматривать безопасность в отношении только лишь государства – это есть сведение сложного к простому. При «классическом» понимании национальной безопасности она сводилась в основном только к безопасности государственной и противопоставлялась индивидуальной и общественной.

Однако следует подчеркнуть, что не все исследователи были согласны с такой трактовкой.

Уже к началу 80-х годов понятие национальной безопасности оказывается чрезвычайно проблемным для описания целого ряда процессов происходящих, как «внутри», так и «вне» государства.

Безопасность в более широком понимании – это междисциплинарный и межпарадигмальный комплекс подходов и концепций. В связи с этим многие ученые выделяют так называемые «мягкие» и «жесткие» вопросы безопасности. Основоположником такого взгляда на безопасность является английский ученый Б. Бузан, один из основателей Копенгагенской школы, сохраняющей свое влияние по сегодняшний день.

Копенгагенской школе исследований безопасности удалось создать принципиально иной подход к феномену безопасности, а также разработать инструментарий для изучения тех процессов, которые они назовут «секьюритизацией». Феномен безопасности стал рассматриваться максимально широко – принципиально новым моментом стало то, что угроза безопасности понимается Копенгагенской школой как социально сконструированный феномен, а сам процесс «секьюритизации» того или иного случая, то есть придания ему «уровня» опасности, имеет дискурсивную (или речевую) природу.

Обзор литературы

Один из представителей Копенгагенской школы и последователь Б.Бузана, исследователь из Дании О. Вэйвер отказался от абстрактного понятия безопасности вне определенного контекста и попытался сформулировать безопасность как речевой акт, при помощи которого элиты, представляя определенные события в качестве угрозы безопасности, легитимизируют свое право на чрезвычайные и решительные политические меры.

Также методологической базой исследования являются труды ученых Williams Paul, М. Кастельс, Т. Росзак, О. Вэйвер, которые исследовали тему кибербезопасности.

Важным выводом, который делается Копенгагенской школой, является то, что вопросы безопасности в меньшей мере относятся к физической реальности или к объективному положению дел, а скорее относятся к восприятию того или иного феномена как угрозы.

Говоря о безопасности, политик переносит ситуацию в особое поле, стремясь получить право действовать для нейтрализации нежелательной динамики. При этом, предвидя возможную критику, О. Вэйвер сразу делает оговорку, что безопасность — это больше, чем просто слово (Юрин А. Н, 2016).

Результаты и Обсуждение

Центральное место в теории «секьюритизации» занимает демонстрация риторики речевых актов политиков, как прежде всего того круга лиц, которые для принятия необходимых им политических решений нуждаются в том, чтобы убедить свою аудитории в существовании угрозы их безопасности.

Концептуализация секьюритизации как речевого акта важна, поскольку она демонстрирует, что слова не просто описывают реальность, но и в определенной степени, «конструируют» степень угрозы безопасности в данной реальности**,**

приуменьшая ее или наоборот преувеличивая – что, в свою очередь, может вызвать «нужные» политикам реакции со стороны той аудитории, к которой обращается политик (так называемый «секьюритизующий агент», к которым в последнее время можно отнести и блогеров, имеющих многотысячную аудиторию подписчиков в социальных сетях) .

Стремительное развитие информационных технологий и интернет- коммуникаций является необратимой тенденцией последних десятилетий Во всех сферах жизнедеятельности общества четко обозначился класс новых видов угроз и опасностей, связанных с применением новейших технологических средств, которые обладают множеством вариантов своего проявления: искажение информации, фальсификация реальности виртуальными мирами, манипулирование сознанием людей, подмена целей и образа жизни навязанными стандартами, информационные войны, и т. д.

Информация и дезинформация превращаются в опасное оружие сообразно тому, в чьих руках оказались сведения и с какой целью они применяются. С другой стороны, с появлением социальных сетей, в частности Фейсбука, начинает стремительно развиваться скорость распространения информации и, в частности, тех самых «секьюритизирующих речевых актов», о которых говорилось выше.

В современном мире начиная примерно с 2007 года особую популярность приобрели новые формы медиа, такие как социальные сети и мессенджеры или, иначе говоря, Интернет-концепт Web 2.0, который позволяет пользователям создавать онлайн-аккаунты с личными страницами пользователей, так называемые профили. Web 2.0 — это своего рода платформа для социального взаимодействия пользователей («юзеров»), к которой можно отнести все современные социальные сети, начиная от Фейсбука и заканчивая Инстаграмом.

Интернет-концепт Web 2.0 был создан в противовес существовавшей до него «версии» Интернета Web 1.0 – которая выполняла преимущественно информационно-справочную функцию: еще совсем недавно считалось, что Интернет – это скорее средство связи, общения, информирования, что соответствовало особенностям его реального использования.

Ключевой идеей создания Web 2.0 стало упрощение коммуникаций между людьми и методов самовыражения (написание текстов, выкладывание фото и много другое).

Современные социальные сети предоставляют пользователям возможность для коммуникаций и поддержания связи из разных точек мира, то есть всемирная сеть Интернета, с появлением социальных сетей расширила коммуникативные возможности до глобального размера и охвата. Социальные сети поэтому называют еще и мессенджерами, от английского слова messege – «сообщение», «послание».

Социальные сети, предоставив своим пользователям довольно много преимуществ, вместе с тем принесли им и дополнительные сложности: с появлением социальных сетей появилось и множество проблем, связанных с безопасностью самой информации. Сохранять конфиденциальную информацию становится все сложнее в связи с тем, что объем генерируемой информации непрерывно увеличивается.

Увеличение информационных потоков и развитие современных технологий актуализирует проблему информационной безопасности не только с позиций кибербезопасности, но и с точки зрения социальной и политической безопасности. В связи с этим в западных социальных науках появился особый термин «cyber security politics», происхождение которого тесно связано с концепцией «секьюритизации» Копенгагенской школы.

Современная динамика развития Интернет-концепта Web 2.0 в виде социальных сетей и мессенджеров показывает, как технологическая динамика взаимодействует с социальной и политической составляющей общественных процессов. Включение «технологии» в качестве категории исследования кажется очевидным, поскольку проблема кибербезопасности связана с развитием и использованием киберпространства, технологической среды, полностью созданной людьми. В свою очередь, политические предпочтения и контексты определяют эволюцию цифровых технологий.

За последнее десятилетие «кибер-инциденты» становятся…более разрушительными и во многих случаях более политическими, при этом параллельно появляется новый массив теоретически обоснованных исследований.

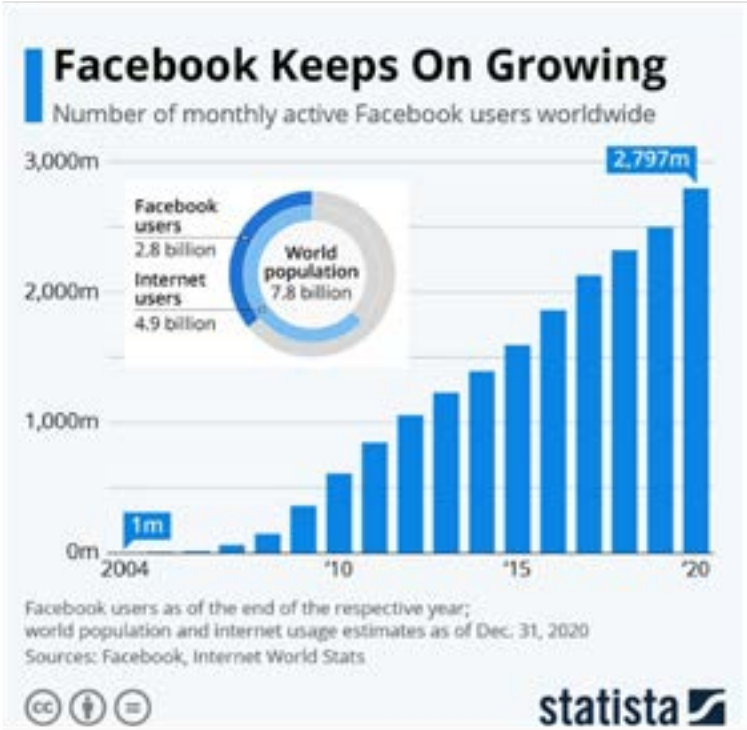

Рисунок 1 – Количество подписчиков Facebook продолжает расти (www.statista.com)

Информационная конфронтация между различными общественными группами и государствами ставит перед собой цель завладеть еще большим влиянием на общество.

В связи с этим, особое значение приобретает проблема влияния социальной сети и особенно такой наиболее массовой как Facebook (Meta), с точки зрения информационной безопасности (*Felix Richter,* Feb 4, 2021).

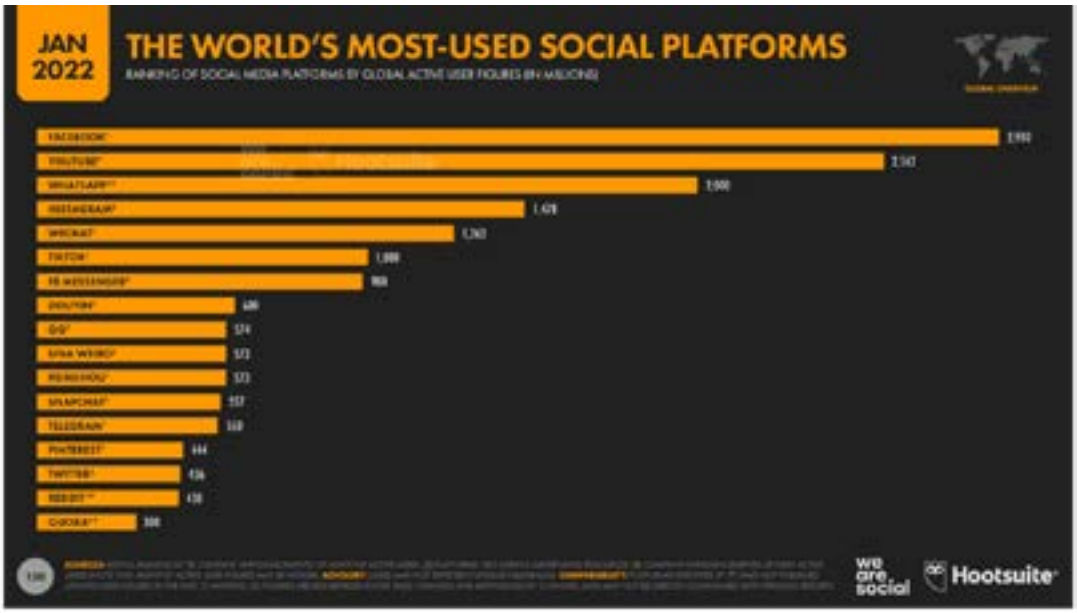

Рисунок 2 – Facebook возглавил рейтинг самых популярных сетей в мире (datareportal.com)

События, развернувшиеся в США впоследствии изнурительной президентской избирательной кампании 2020 и в оффлайн, и в онлайн формате, потрясли американское общество.

В ходе длительной предвыборной президентской кампании 2020 года компания Facebook принимала довольно жесткие меры против дезинформации, иностранного вмешательства и разжигания ненависти. По мнению сотрудников Facebook, они считали, что им в значительной степени удалось решить проблемы, которые четыре года назад привели к, возможно, самому серьезному кризису, практически к скандалу, беспрецедентному в истории Facebook, когда на президентских выборах 2016 года, сторонников Д.Трампа, кандидата от Республиканской партии США обвинили в хакерских взломах данных его конкурента – кандидата от партии демократов – Хиллари Клинтон.

Неожиданно для себя американские журналисты обнаружили, что правила публикации постов в Facebook хотя и казались одинаковы де-юре, на бумаге, но на деле – оказались де-факто не совсем для всех. Большие привилегии все это время имели некоторые американские политики, а руководство IT-гиганта систематически закрывало глаза на нарушения своих же собственных правил.

В частности, расследование показало, что Facebook через несколько дней после президентских выборов 2020 года ослабил свой контроль и мониторинг за деятельностью сообществ, распространявших сообщения деструктивного содержания. Мировые издания цитируют масштабное журналистское расследование «Досье Facebook». Изучены десятки тысяч внутренних документов компании, которые озвучила бывшая сотрудница кампании Ф.Хауген на слушаниях в конгрессе США в октябре 2021 года и ее резонансные показания открыли новую страницу в истории популярной социальной сети. Кампания даже была вынуждена сменить, спасая репутацию, название своего широкого «раскрученного» бренда с Facebook на Meta.

Рисунок 3 – Штурм Капитолия в Вашингтоне, округ Колумбия, 6 января 2021 года (s.abcnews.com)

В не менее ожесточенной предвыборной гонке 2020 года Facebook решительным образом блокировал те аккаунты, которые – по мнению кампании – нарушали правила проведения президентских выборов в 2020 году. Но после того, как стало ясно, что победу одержал по результатам голосования кандидат от Демократической партии Д.Байден, Facebook отменил несколько десятков предвыборных мер, которые использовались для блокировки контентов, разжигающих общественную напряженность и ненависть и содержащих недостоверную информацию. Запрет, который компания наложила на первоначальную группу Stop the Steal («Остановить Воровство» – название онлайн сообщества сторонников проигравшего выборы действующего

президента Д.Трампа, был впоследствии снят, чем воспользовались его сторонники.

Журналисты собрали в «досье Фейсбук» тысячи страниц внутренних документов компании, раскрытых Комиссии по ценным бумагам и биржам, которые предлагают важные новые доказательства роли Facebook в событиях. Пользовательские сообщения о «ложных новостях» достигли почти 40 000 в час, как показал внутренний отчет 6 января 2021 г.

Согласно отчету, в принадлежащем Facebook Инстаграме в подстрекательстве к насилию чаще всего сообщалось об аккаунте @realdonaldtrump — официальном аккаунте президента Трампа, а также на аккаунтах группы Stop the Steal и QAnon, не заблокированных вовремя (во время и особенно после выборов) в социальной сети Facebook (Крейг Сильверман, Крейг Тимберг, Джефф Као и Джереми Б. Меррилл,2022: 8)

Попытка штурма Капитолия (см. рис 3) (Timberg Craig, Elizabeth Dwoskin Elizabeth. and. Reed Albergotti. October 22) – когда риторика прежнего президента США Д.Трампа (и его команды, не согласной с результатами выборов в президенты 2020 года) о существовании угрозы американской демократии, растиражированная через социальные сети, и прежде всего Фейсбук, побудила его сторонников к «маршу на Вашингтон» – это свидетельство верности концепции секьюритизации или это следствие «неправовой деятельности» такой многомиллионной социальной сети, как Фейсбук?

Конгресс США вынужден был провести слушания по этому вопросу осенью 2021 года. Расследование до сих пор продолжаются.

Вследствие растущего беспокойства по поводу дестабилизирующей роли кибер-операций государственные и негосударственные субъекты более активно ищут способы контролировать риск эскалации и конфликтов с помощью различных средств.

Как отмечается на сайте ENISA – Агентства по кибербезопасности, созданного Евросоюзом в 2004 году, «в мире, который стал гиперсвязанным, киберпреступники представляют серьезную угрозу внутренней безопасности Европейского Союза и безопасности его граждан в Интернете».

Агентство по кибербезопасности, ENISA (European Union Agency for Cybersecurity), преследует «достижение высокого общего уровня кибербезопасности в Европе, действуя на основе Закона ЕС о кибербезопасности, вносит свой вклад в киберполитику ЕС, повышает надежность продуктов, услуг и процессов информационно-коммуникационных технологий (ICT) с помощью схем сертификации кибербезопасности, сотрудничает с государствами-членами и органами ЕС и помогает Европе подготовиться для кибер-вызовов завтрашнего дня. Посредством обмена знаниями, наращивания потенциала и повышения осведомленности Агентство работает вместе со своими ключевыми заинтересованными сторонами над укреплением доверия, повышением устойчивости инфраструктуры Союза и, в конечном счете, для обеспечения цифровой безопасности европейского общества и граждан ЕС» (ENISA, 2022:10)

«Киберугрозы стали более смелыми и сложными. Необходимо адаптировать нашу систему безопасности к новым реалиям и обеспечить защиту наших граждан и инфраструктуры», — заявил глава отрасли ЕС Тьерри Бретон. (Foo Yun Chee, 2022) В связи с этим Компании обязаны оценивать свои риски кибербезопасности, уведомлять власти и принимать технические и организационные меры для противодействия рискам со штрафами до 2% от мирового оборота за несоблюдение требований.

Довольно серьезно к проблемам информационной безопасности относятся и в Российской Федерации, где в 2016 году была принята Доктрина информационной безопасности – документ, представляющий собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. Предыдущая Доктрина информационной безопасности была утверждена Президентом Российской Федерации в сентябре 2000 года. Необходимость разработки новой редакции Доктрины была обусловлена с учётом нового характера угроз национальной безопасности в информационной сфере. Сравнение двух Доктрин (2000 года и 2016 года) свидетельствует о том, что они значительно отличаются друг от друга и по структуре, и по содержанию: в частности, если в документе 2000 года речь идет о росте влияния информационных технологий на национальные интересы страны, то в новой версии они уже признаются неотъемлемой частью всех сфер жизни. Примечательно, что Доктрина информационной безопасности 2016 года определяет национальные интересы России в информационной сфере, в частности, такие как, «обеспечение и защита прав и свобод граждан в части получения и использования информации, неприкосновенность частной

жизни, а также сохранение духовно-нравственных ценностей». Кроме того, среди основных информационных угроз, стоящих перед страной и обществом, отмечаются, например, такие как «спецслужбы отдельных государств пытаются дестабилизировать внутриполитическую и социальную ситуацию в различных регионах мира. Цель — подрыв суверенитета и нарушение территориальной целостности государств. Методы — использование информационных технологий, а также религиозных, этнических и правозащитных организаций.» (из Доктрины ИБРФ,2016:0). Иными словами, контекст описания информационных угроз носит откровенно политический, секьюритизирующий характер и выходит за рамки понимания кибербезопасности, данного ENISA – Агентства по кибербезопасности ЕС.

В Казахстане вопросы обеспечения информационной безопасности обострились осенью 2021 года при обсуждении законопроекта, «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам защиты прав ребенка» предполагавшего по мнению общественности меры по ограничению Интернета. Сенат в итоге предложил вообще убрать из законопроекта возможность, позволяющую уполномоченному органу по своему усмотрению ограничивать доступ либо приостанавливать работу интернет-ресурсов, социальных сетей и мессенджеров» (Щекунских В., 2022)

Но актуальность данной проблемы не потеряла свою остроту: Президент Казахстана К.-Ж. Токаев в своем ежегодном Послании народу в марте 2022 года отметил: «Сейчас век интернета. Огромный поток негативной информации отравляет сознание современного поколения. Массовое распространение получают ложные смыслы и недолговечные ценности. Это очень опасная тенденция» (Токаев, 2022).

Как мы видим, на современном этапе растущее внимание к вопросам информационной или кибер-безопасности сталкивается с проблемой понятия «безопасность» в более широком общественно-политическом контексте не только в академической среде.

Совсем недавно, в мае 2022 года в средствах массовой информации США появились сообщения о принятом в штате Техас новом законе, регулирующим деятельность интернет-ресурсов. Жители Техаса теперь могут подать в суд на Facebook, Twitter и YouTube за якобы цензуру их контента после того, как федеральный апелляционный суд встал на сторону закона штата, ограничивающего деятельность социальных сетей по модерированию своих платформ. То есть теперь закон Техаса запрещает любой платформе социальных сетей с 50 или более миллионами пользователей «блокировать, запрещать, удалять, демонетизировать, деактивировать, ограничивать, отказывать в равном доступе или видимости или иным образом дискриминировать» выложенный в Интернете контент.

По мнению экспертов в области права, данный закон создает огромную неопределенность в отношении того, как социальные сети будут фактически функционировать в Техасе, поднимает вопросы о том, как могут выглядеть контенты пользователей и смогут ли Facebook, Twitter и YouTube вообще управлять своими онлайн-пространствами. Создается опасный, по мнению многих экспертов прецендент по поводу нарушения прав Первой поправки Конституции США и их драматическим переосмыслением, которое возможно, затронет не только технологическую отрасль, но и всех. Это решение может изменить права и обязанности всех веб-сайтов; отношение к технологиям и Интернету.

Ряд экспертов считает, что принятие подобного закона – это своего рода месть однопартийцев (президентские выборы в штате Техас практически всегда выигрывает Республиканская партия) бывшего президента США Д.Трампа за его пожизненную блокировку в Интернете – 88 миллионов фолловеров аккаунта @realDonaldTrump в Twitter и 35 миллионов абонентов Трампа на его странице в Facebook больше не могут найти его посты на этих платформах – зачастую опасные и расистские – по мнению администрации данных социальных сетей. (Brian Fung, 2022).

Принятие данного закона в Техасе возвращает американскую общественность к вопросу, обострившемуся после штурма Капитолия в январе 2021 года – кто несет ответственность за опасные «речевые акты» (по терминологии концепции «секьюритизации») – тот, **кто** публикует или где опубликовано?

Заключение и выводы

В целом можно отметить, что проблема информационной безопасности все больше сдвигается в сферу обсуждения определенных общественных культурно-исторических ценностей, таких, например, как свобода слова. И если власти КНР пошли на полное государственное

цензурирование китайского Интернета, создав Great Firewall, то в США обсуждение проблемы свободы высказываний в Интернете опирается на отсылку к Первой поправке Конституции США о «Свободе слова, свободе религии, свободе прессы, свободе собраний, праве на подачу петиции», которая была принята в 1789 году.

За последнее десятилетие «кибер-инциденты» становятся более разрушительными и во многих случаях более политическими, при этом параллельно появляется новый массив теоретически обоснованных исследований. Определенную популярность в определении «Кибербезопасности», или «Интернет-безопасности» приобретает концепция комплексного подхода. Как отмечают сторонники такого подхода: «Мы фокусируемся на взаимосвязи между технологиями и миром политики и государственной практики — на том, что политические деятели говорят, и на том, что они делают в области кибербезопасности как политической проблемы, как на национальном, так и на международном уровне» (Myriam Dunn Cavelty, Andreas Wenger .2019: 0).

Еще одна ключевая проблема связана с информационными операциями и пропагандой, которые могут распространяться более целенаправленно и эффективно с помощью технологий искусственного интеллекта и платформ социальных сетей. Эти политические события поднимают важные исследовательские вопросы, требующие междисциплинарных ответов по поводу постановки проблемы – представляют ли интернет-технологии угрозу политической и социально-экономической сфере? Его актуальность для общества, вероятно, станет еще выше в будущем, когда новые цифровые технологии расширят пространственные границы киберпространства и возникнут новые сложные проблемы. Научное знание как проблемного, так и рефлексивного характера имеет решающее значение для понимания того, как будут информационные технологии влиять на политику и как они будут связаны с более широкими социально-экономическими изменениями, затрагивающими общество, экономику и государство в будущем.

Литература

Brian Fung, 2022. Texas has declared open season on Facebook, Twitter and YouTube with censorship law. May, 13,2022- https://edition.cnn.com/2022/05/13/tech/texas-hb20-social-media-law/index.html)

Cavelty Myriam Dunn, Wenger Andreas. Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation. – Switzerland: Routledge,2022.- 286 p. https://www.routledge.com/Cyber-Security-Politics-Socio-Technological-Transformations-and-Political/Cavelty-Wenger/p/book/9780367626747

Cavelty Myriam Dunn, Wenger Andreas. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. //Contemporary Security Policy. -2019 -том 41. Выпуск 1. – С.5-32

Foo Yun Chee. EU governments, lawmakers agree on tougher cybersecurity rules for key sectors. – May, 13,2022. https://www.reuters.com/technology/eu-governments-lawmakers-agree-tougher-cybersecurity-rules-key-sectors-2022-05-13/

Felix Richter. Facebook keeps on growing, Feb 4, 2021 https://www.google.com/search?q=facebook+keeps+on+growing&sxsrf=ALiCzsZ1zLH7-

Roszak T. The Cult of Information. The Folklore of computers and the True Art of Thinking. – New York: Pantheon Books, 2000.

Silverman Craig, Timberg Craig, Jeff Kao & Jeremy B. Merrill

What role did Facebook play in the January 6 insurrection? Jan 13, 2022. https://www.thebigq.org/2022/01/13/what-role-did-facebook-play-in-the-january-6-insurrection/

Timberg Craig, Elizabeth Dwoskin Elizabeth and Reed Albergotti. How Facebook played a role in the Jan. 6 Capitol riot / October 22, 2021. https://www.google.com/search?q=How+Facebook+played+a+role+in+the+Jan.+6+Capitol+riot

Williams Paul D. Security Studies: An Introduction. Routledge 2008 p.

Гайдаев О. С.. Теория секьюритизации, или хорошо забытое старое: к вопросу о теоретико□философских истоках и зарождении теории // Вестник РУДН. Серия: Международные отношения. – 2021. – № 1. – С.20 – 32. http://journals.rudn.ru/international□relations

Токаев К. Единство народа и системные реформы – прочная основа процветания. Послание Главы государства Касым-Жомарта Токаева народу Казахстана. https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-183048

Щекунских В. Выдуманная проблема «новой цензуры» в Казахстане/ апрель 24, 2022// https://ia-centr.ru/experts/vyacheslav-shchekunskikh/vydumannaya-problema-novoy-tsenzury-v-kazakhstane/

Юрин А. Н. К понятию безопасность: кто и как определяет угрозу сегодня? //апрель. 2016 // http://regional-dialogue.com/ru/security/#_edn22

Электронные ресурсы:

About ENISA – The European Union Agency for Cybersecurity https://www.enisa.europa.eu/about-enisa

Cyber security meets security politics: Complex technology, fragmented politics, and networked science, 2019 – https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855

Доктрина информационной безопасности Российской Федерации https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

Количество подписчиков Facebook продолжает расти// (https://www.statista.com/chart/10047/facebooks-monthly-active-users/)

Facebook возглавил рейтинг самых популярных сетей в мире. (https://datareportal.com/reports/digital-2022-future-of-facebook)

Штурм Капитолия в Вашингтоне, округ Колумбия, 6 января 2021 года https://s.abcnews.com/images/International/capitol-police-gty-rc- 10108_1610107317802_hpEmbed_25x16_992.jpg

References

Brian Fung, 2022. Tekhas ob”yavil otkrytyj sezon v Facebook, Twitter i YouTube s zakonom o cenzure. May, 13,2022- https://edition.cnn.com/2022/05/13/tech/texas-hb20-social-media-law/index.html)

Cavelty Myriam Dunn, Wenger Andreas. Politika kiberbezopasnosti. Social’no-tekhnologicheskie transformacii i politicheskaya fragmentaciya. – SHvejcariya: Routledge, 2022. – 286 p.

https://www.routledge.com/Cyber-Security-Politics-Socio-Technological-Transformations-and-Political/Cavelty-Wenger/p/book/9780367626747

Cavelty Myriam Dunn, Wenger Andreas. Kiberbezopasnost’ vstrechaetsya s politikoj bezopasnosti: slozhnye tekhnologii, fragmentirovannaya politika i setevaya nauka. //Sovremennaya politika bezopasnosti. – 2019 – tom 41. Vypusk 1. – S.5-32.

Foo Yun Chee. Pravitel’stva ES i zakonodateli dogovorilis’ ob uzhestochenii pravil kiberbezopasnosti dlya klyuchevyh sektorov.- May, 13,2022. https://www.reuters.com/technology/eu-governments-lawmakers-agree-tougher-cybersecurity-rules-key-sectors-2022-05-13/

Felix Richter. Facebook prodolzhaet rasti, Feb 4, 2021 https://www.google.com/search?q=facebook+keeps+on+growing&sxsrf=ALiCzsZ1zLH7-

Roszak T. Kul’t informacii. Fol’klor komp’yuterov i istinnoe iskusstvo myshleniya. – N’yu-Jork: Knigi Panteona, 2000.

Silverman Craig, Timberg Craig, Jeff Kao & Jeremy B. Merrill

Kakuyu rol’ sygral Facebook v vosstanii 6 yanvarya? Yanvar’ 13, 2022. https://www.thebigq.org/2022/01/13/what-role-did-facebook-play-in-the-january-6-insurrection/

Timberg Craig. ,. *Elizabeth Dwoskin Elizabeth*. and. *Reed Albergotti*. Kak Facebook sygral svoyu rol’ v bunte 6 yanvarya v Kapitolii/ Oktyabr’ *22, 2021* https://www.google.com/search?q=How+Facebook+played+a+role+in+the+Jan.+6+Capitol+riot

Williams Paul D. Issledovaniya bezopasnosti: vvedenie. Routledge, 2008 s.

Gaidaev O. S. The theory of securitization, or the well-forgotten old: on the issue of theoretical and philosophical origins and the origin of the theory [The theory of securitization, or the wellgforgotten old: on the question of theoretical and philosophical origins and the origin of the theory] // Bulletin of RUDN University. Series: International relations. – 2021. – No. 1. – P.20-32. http://journals.rudn.ru/international-relations

Tokaev K. Edinstvo naroda i sistemnye reformy – prochnaya osnova procvetaniya. Poslanie Glavy gosudarstva Kasym-Zhomarta Tokaeva narodu Kazahstana. https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-183048

Shchekunskih V. Vydumannaya problema «novoj cenzury» v Kazahstane/ aprel’ 24, 2022// https://ia-centr.ru/experts/vyacheslav-shchekunskikh/vydumannaya-problema-novoy-tsenzury-v-kazakhstane/

Yurin A. N. K ponyatiyu bezopasnost’: kto i kak opredelyaet ugrozu segodnya? //aprel’. 2016 // http://regional-dialogue.com/ru/security/#_edn22

Electronic resources:

Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

Ob ENISA — Agentstve kiberbezopasnosti Evropejskogo Soyuza. https://www.enisa.europa.eu/about-enisa

Kiberbezopasnost’ vstrechaetsya s politikoj bezopasnosti: slozhnye tekhnologii, fragmentirovannaya politika i setevaya nauka, 2019 g.https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855

Kolichestvo podpischikov Facebook prodolzhaet rasti//

(https://www.statista.com/chart/10047/facebooks-monthly-active-users/)

Faceebook vozglavil rejting samyh populyarnyh setej v mire.

https://datareportal.com/reports/digital-2022-future-of-facebook

Shturm Kapitoliya v Vashingtone, okrug Kolumbiya, 6 yanvarya 2021 goda https://s.abcnews.com/images/International/capitol-police-gty-rc-210108_1610107317802_hpEmbed_25x16_992.jpg