КИБЕРАТАКИ КАК СРЕДСТВО ПОЛИТИЧЕСКОГО ВЛИЯНИЯ

Аннотация

По мере того, как информационные технологии трансформируют глобальное общество, они естественным образом открывают новые возможности для вмешательства в политические процессы. Одним из эффективных инструментов такого рода воздействия являются кибератаки, которые позволяют быстро, ненасильственно и анонимно повлиять на политические позиции общественности и даже вмешаться в избирательный процесс, ставя под сомнения результаты голосования. Для составления полной картины происходящего в статье рассматриваются кейсы, подобранные из разных регионов: Америки, Европы и Азии.

Ключевые слова: кибератака, общественное мнение, выборы.

DOI: 10.51180/RPS.2020.16.3.007

Автор

Елена Сергеевна Волкова

Магистр факультета Международной уголовной юстиции
Университета Париж II Пантеон-Ассас
(Париж, Франция)

Ежедневно, по разным оценкам, в мире совершается от 400 тысяч [2] до 700 тысяч [11] кибератак. Включая в себя обширный спектр инструментов от простейших спам-рассылок с помощью спуфинга до сложнейших DDoS-атак, они становятся реальной угрозой для предприятий, частных лиц и особенно для государственных инфраструктур. Последний доклад организации по кибербезопасности FireEye показал, что атаки на национальные информационные системы вошли в топ-3 [18], а участившиеся за последние годы заявления государств о манипулировании общественным мнением извне и вмешательстве хакеров в избирательные кампании лишь подтверждают, что кибероперации способны повлиять на политический процесс.

Однако прежде, чем мы перейдем к рассмотрению кейсов, необходимо разобраться, что представляет собой кибератака. Принятая в 2016 году Доктрина информационной безопасности Российской Федерации характеризует киберугрозы и кибервторжения следующим образом: «Информационная угроза — совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [6]. Американская стратегия кибербезопасности дает, в свою очередь, более развернутое определение кибератаки, под которой понимает деструктивную, подрывную или иным образом дестабилизирующую злонамеренную кибердеятельность, направленную против интересов США в отношении сетей, систем, функций и данных [19]. Обе страны допускают тот факт, что использование современных информационных атак способно оказать влияние «на индивидуальное и общественное

сознание» [6; 19]. Эту точку зрения разделяют и другие страны. Так, стратегия национальной информационной безопасности Франции делает особый упор на защиту национальной инфраструктуры, поскольку государство уже сталкивалось в прошлом с «информационными атаками, призванными нанести удар по общественному мнению» [23], а Австралия прямо указывает в своей киберстратегии, что комплексная защита от кибератак необходима, чтобы предохранить демократические избирательные процессы от злонамеренных кибератак [8].

Сегодняшние кибератаки могут быть использованы в разных целях: дезинформировать граждан или отвлечь их от проблемы, повлиять на общественное мнение, что в конечном итоге способно дезориентировать общество, подкрепить чувство сомнения среди его представителей или привести к формированию стойкого мнения у конкретной целевой аудитории по определенному вопросу. Все это становится возможным благодаря быстрому развитию информационных технологий. Именно они делают киберпространство крайне привлекательным для совершения атак на национальные информационные системы: с одной стороны, виртуальная среда позволяет обеспечить всем участникам высокую степень подключения, низкую задержку получения информации, полностью игнорируя физическое расстояние или национальные границы, в то время как, с другой стороны, анонимность и отсутствие точной атрибуции кибератак ведут к полной беззаконности злонамеренных действий хакеров.

1. Кибератаки как инструмент политической пропаганды

На сегодняшний день одной из наиболее распространенных форм политического влияния с помощью кибератак является хактивизм, который представляет собой акт взлома или проникновения в компьютерную систему в политических или социальных целях, или то, что И.Н. Панарин определял как «бескорыстное» хакерство в целях политического активизма в книге «Информационная война и выборы» [3].

Хактивисты не оправдывают насильственные или деструктивные действия против своих врагов, вместо этого они сосредотачиваются на ненасильственных средствах разоблачения правительств и корпораций, за счет повышения осведомленности граждан и воздействия на них. И, по мнению Стивена Рэя, такой способ взаимодействия с государствами является наиболее эффективным, в сравнении с традиционными уличными протестами [22].

Хактивисты могут прибегнуть к разного рода инструментам, например, к DDoS-атакам, которые направлены на то, чтобы вызвать отказ в обслуживании путем отправки на атакуемый веб-сайт большого количества запросов с помощью ботов, чтобы превысить способность сайта обрабатывать их [16], — в таком случае сайт попросту перестанет открываться. Другим средством воздействия может стать технология дефэйсмента (defacement), которая позволяет заменить содержимое сайта своим собственным [29]. Однако арсенал хактивистов ничем не ограничен, и они могут воспользоваться другими популярными средствами нападения, например, спуфингом, который позволяет подменить данные атакующим и выдать себя за другое лицо. Выбор огромен и продиктован лишь изобретательностью хактивистов. Что действительно важно, так это желание повлиять на общество с помощью приведенных выше инструментов. Хактивисты бросают вызов обществу и государству, желая выразить свою позицию, и стремятся добиться социальных или политических изменений путем привлечения внимания к проблемам и влияния на общественное мнение.

Именно поэтому жертвами хактивистской деятельности часто становятся правительственные учреждения, транснациональные корпорации или любые другие субъекты, которые, по мнению хактивистов, несут ответственность за неправильные и незаконные действия.

Таким образом, хактивизм сегодня может представлять собой форму проявления так называемого электронного гражданского неповиновения (*Electronic Disturbance Theater)* (ECD), о которой в 1999 году писал Стивен Рэй [22]:

«По мере того, как хакеры становятся политизированными, а активисты — компьютеризированными, мы увидим рост числа киберактивистов, вовлеченных в то, что скоро станет более широко известным как электронное гражданское неповиновение. Те же принципы традиционного гражданского неповиновения, как вторжение и блокирование, будут по-прежнему применяться, но все больше таких действий будет происходить в электронной или цифровой форме. Основной средой электронного гражданского неповиновения станет киберпространство».

Одним из самых известных хактивистских движений на сегодняшний день является группа Anonymous, члены которой разбросаны по всему миру. Они поддерживают гражданские революции, борются против тоталитаризма и нарушений прав человека и выступают за свободу в интернете.

Рассмотрим случай в Каталонии, который произошел в октябре 2017 года на фоне референдума о независимости региона от Испании. В ходе голосования более 2 млн человек высказалось за независимость Каталонии [14], однако уже 17 октября Конституционный суд Испании вынес постановление, в котором отказался признавать легитимность референдума. Желая выразить поддержку населению Испании, хакерская группировка Anonymous решила вмешаться в политический конфликт между обществом и государством: «Мы хотим заявить, что желание каталонского народа выразить свою волю через референдум является точкой зрения большинства и распространяется на все слои общества». С этой целью хактивисты совершили ряд кибератак против сайтов Королевского дома Испании, Конституционного суда, Министерства общественных работ и транспорта и других правительственных учреждений. Некоторые из этих веб-ресурсов прекратили работу, в то время как на других был размещен баннер «Свободная Каталония». Еще одним инструментом поддержки референдума за независимость региона стала спам-рассылка с целью отключения учетных записей мэров каталонских городов, которые использовались для координации голосования, чтобы предотвратить манипулирование результатами референдума [27].

Мы может также обратиться к другому примеру — деятельности бразильских хактивистов Pryzraky Group, которые провели кибератаки против нескольких государств в борьбе за справедливость. В феврале-марте 2019 года группировка обрушила ряд правительственных сайтов в Судане (Торговая палата Судана, Министерство нефти и газа, Министерство внутренних дел и канцелярия президента) в рамках кампании #OpSudan с целью свержения режима Омара аль-Башира. На некоторых правительственных сайтах также было размещены сообщения в поддержку протестующих против режима Омара аль-Башира: «В Судане нет свободы и справедливости. Мы отдаем дань уважения всем жертвам этой революции. Мученики навсегда останутся в наших воспоминаниях. Люди никогда не сдадутся. Скоро победа!» [34]. Ситуация оказалась тем более примечательна, что в конце февраля президент Судана издал чрезвычайный указ о запрете публичных собраний, забастовок и шествий [24], сделав, таким образом, кибератаки единственным возмож-

ным средством выражения мнения. Через несколько недель, в марте того же года, хактивистами была запущена уже новая информационная кампания, сопровождающаяся DDoS-атаками против правительства Никарагуа. Пока правящая верхушка в лице президента Даниэля Ортега и вице-президента Росарио Мурильо подавляла протесты граждан, уставших «от репрессий и авторитаризма» [4], члены Pryzraky Group разместили сообщения о массовых нарушениях прав человека в отношении протестующих на сайтах Национальной полиции Никарагуа и Министерства иностранных дел Коста-Рики [33]. Атаку последнего хакеры объяснили необходимостью повысить осведомленность об этих правонарушениях [33]:

«Lo siento, Costa Rica por usar su plataforma para esto (prometemos no dañar nada ni comprometer la información confidencial de su gobierno), pero este es un mensaje de ayuda! Por los prisioneros que Daniel Ortega secuestra y tortura todos los días. Nada es normal en Nicaragua» [Мы приносим извинения Коста-Рике за использование ее платформы для этого [для этой кибератаки — прим. автора] (мы обещаем ничего не повредить и не поставить под угрозу конфиденциальную информацию вашего правительства), но это сообщение о помощи! Для заключенных, которых Даниэль Ортега похищает и пытает каждый день. В Никарагуа нет ничего нормального].

В обоих случаях кибератаки стали мощной объединяющей силой, которая смогла мобилизовать людей на протесты в реальном мире и дать манифестантам ощущение, что они могут рассчитывать на поддержку со стороны, что в конечном итоге привело к росту протестующих.

Наконец, обратимся к последнему примеру кибератак, используемых в целях пропаганды и политической манипуляции в информационном пространстве, осуществляемых с помощью спуфинга. В августе 2020 года во время пресс-конференции Тайваньского бюро расследований Лю Цзя-цзун, сотрудник отдела расследований кибербезопасности, обвинил Китай в причастности к многочисленным взломам инфраструктуры и краже правительственных документов и данных [25]. Было отмечено, что кибератаки проводятся начиная с 2018 года и являются частью китайской кампании по «вездесущему проникновению» на Тайвань. Похищая данные, прокитайские хакеры продвигают нарратив, соответствующий политическим интересам Китайской Народной Республики, активно прибегая к технологии спуфинга, или киберсимулякров, «выполняющих функцию репрезентации реальных пользователей» [1], как их определяет профессор С.В. Володенков. Доклад Mandiant Threat Intelligence отмечает, что для этих целей Китай использует фейковые «учетные записи, чтобы выдать себя за западные СМИ», включая применение идентичных имен пользователей и фотографий, используемых в учетных записях западных СМИ, которые они имитируют [30].

«Мы обнаружили, что фабрики по производству контента не просто придумывают фальшивую информацию. Они все больше и больше манипулируют мнениями» [26], — заявил в декабре прошлого года Джарвис Чиу, старший менеджер Института информационной индустрии, который оказывает поддержку правительству Тайваня в предотвращении дезинформации. По словам Чиу, взлом реальных пользователей и создание новых фейковых аккаунтов позволяют прокитайским хакерам смещать фокус дебатов и манипулировать общественным мнением.

Однако, по мнению многих исследователей, кибератаки способны выйти далеко за рамки «когнитивного уровня», который включает в себя операции по влиянию на мнение граждан и пропагандистскую деятельность, а также нанести ущерб технической части избирательной системы, повлияв тем самым на ход избирательного процесса [13].

2. Кибератаки и вмешательство в электоральный процесс

Использование новых технологий во время избирательных кампаний стало ключевой темой в последние годы, а опасения по поводу взлома баз данных, манипуляций со СМИ и иностранного технологического вмешательства в результаты голосования вызывают обеспокоенность государств во всем мире.

Внимание к этой проблеме особенно резко возросло из-за вмешательства в выборы в США в 2016 году. Ссылаясь на секретные данные о причастности России к кибератакам на избирательную систему Америки, бывший исполняющий обязанности директора Центрального разведывательного управления Майкл Мур назвал эти действия «политическим эквивалентом 11 сентября» [17]. Согласно американской версии произошедшего, Россия вмешивалась в американские выборы четырьмя основными способами: путем кражи информации, ее выборочного распространения, пропагандистской кампании и попыток взлома систем голосования по всей стране [15]. Основной причиной этих злонамеренных действий было объявлено «необоснованное вторжение в географическую сферу ее влияния», когда Америка поощряла антироссийские восстания во время Революции роз в Грузии в 2003 году, Оранжевой революции 2004 года на Украине и протесты в Москве в 2011 году [28]. Российским хакерам вменяли в вину взлом компьютеров Национального комитета Демократической партии, веб-сайтов избирательных комиссий в Аризоне и Иллинойсе [13], электронной почты председателя избирательной кампании Клинтона Джона Подеста [7] и Республиканского национального комитета [12], а также, согласно отчету Агентства национальной безопасности (далее АНБ) от 5 мая 2017 года, системы регистрации избирателей и «некоторых других элементов системы голосования» [31]. Хотя АНБ не делает выводов о том, оказали ли подобные действия какое-либо влияние на исход выборов, оно допускает вероятность того, что кибератаки привели к «обескураживающим результатам» [31]. Стоит отметить, что президент РФ Владимир Путин причастность государственных структур к кибератакам опроверг, допустив, однако, вероятность вмешательства в выборы США в 2016 году со стороны патриотически настроенных независимых хакеров: «Потому что хакеры — люди свободные <…> они проснулись сегодня, прочитали, что там что-то происходит в межгосударственных отношениях, если они настроены патриотически, они начинают вносить свою лепту, как они считают правильным в борьбе с теми, кто плохо отзывается о России. Теоретически это возможно» [5].

Опираясь на этот опыт, США приняли решение выстроить эффективную систему кибербезопасности при подготовке к выборам 2020 года. Америка заявила, что это ей помогло предотвратить прямое вмешательство в избирательный процесс, но «атмосфера беспокойства, создаваемая кибератаками, все же оказала *значительное* влияние» на ход кампании в этом году [20].

Однако вмешательство в выборы посредством кибератак не началось и не закончилось с выборами в Соединенных Штатах. Хакеры продолжают взламывать цифровые платформы избирательных систем по всему миру с намерением ввести электорат в заблуждение, нанося репутационный ущерб отдельным кандидатам или политической партии или ставя под сомнение избирательный процесс в целом. За последние несколько лет множество европейских государств в лице Великобритании, Италии, Франции, Грузии, Украины сообщили о вмешательстве в избирательный процесс путем кибератак. Так, группа хакеров Lizard Squard была ответственна за нападение на лейбористскую партию Великобритании во время всеобщих

выборов в стране в декабре прошлого года. Они провели крупную DDoS-атаку на цифровые платформы лейбористов, мотивируя это тем, что «правительство, поддерживающее террористов, не должно управлять страной» [21]. И, хотя кибератака не увенчалась успехом, лидер партии Джереми Корбин заявил, что нападения заставили его «сильно нервничать» в отношении предстоящих выборов [21]. В конечном счете, по мнению исследователя Крис Теноув, постоянная угроза оказаться мишенью для кибератак, какой стал Джереми Корбин в 2019 году, может повлиять на желание возможных кандидатов баллотироваться [10].

Не обошли кибератаки и Азию. Так, согласно ноябрьскому исследованию Mandiant Threat Intelligence, Китай стал самым активным игроком в Азиатско-Тихоокеанском регионе, вмешиваясь в электоральный процесс соседних территорий: Гонконга, Тайваня, Камбоджи [30]. Можно предположить, что вмешательство Китая в выборы является частью его более широкой стратегии защиты своих основных национальных интересов, как внутри страны, так и на региональном уровне, а оказание давления на политических деятелей, которые бросают вызов этим интересам, способно поддерживать в регионе статус-кво. Эти основные интересы, как они определены Коммунистической партией Китая, включают сохранение внутренней стабильности, экономическое развитие, территориальную целостность и повышение статуса Китая как великой державы.

Случай вмешательства китайских хакеров в камбоджийские выборы заслуживает отдельного рассмотрения. В 2017–2018 годах премьер-министр Хун Сен, находившийся на тот момент у власти уже 32 года, столкнулся с напряженной борьбой во время парламентских выборов. Увидев в Партии национального спасения Камбоджи и ее лидере Кем Сокха угрозу, власти приняли решение распустить оппозиционную партию, а ее председателя обвинить в «государственной измене». Пекин также решил политически поддержать авторитарного лидера и предоставил 20 миллионов долларов Национальному избирательному комитету. Однако поддержка китайского правительства не ограничилась финансовой помощью, так как, по мнению экспертов по кибербезопасности, Коммунистическая партия Китая решила поддержать действующего премьер-министра в киберпространстве. Согласно докладу Mandiant Threat Intelligence, прокитайская группа хакеров взломала компьютерные системы избирательной комиссии Камбоджи, Сената и нескольких камбоджийских министерств, чтобы оперативно получать информацию о ходе электоральной кампании, а также проникла в компьютеры членов запрещенной Партии национального спасения Камбоджи и камбоджийцев, выступающих за права человека и демократию, которые критиковали правящую Народную партию Камбоджи [9]. В ходе данной кибероперации злоумышленники получили доступ к системам с помощью фишинга и трояна, разослав своим жертвам зараженные электронные письма.

Рассмотренные выше кейсы показывают, что использование кибератак с целью политического влияния сегодня уже не редкость. При этом необходимо отметить, что попытка вменить в вину государствам кибератаки, запущенные с целью оказания влияния на население или на избирательный процесс, неизбежно сталкивается с отрицанием какой-либо причастности со стороны этих государств. Однако, рассматривая данную проблему не с юридической, а с политической точки зрения, гораздо важнее тот факт, что, кто бы ни стоял за кибератаками — киберхактивисты или прогосударственные структуры, — приведенные выше примеры показывают, насколько реальными и обыденными

становятся взлом национальной инфраструктуры и выведение ее из строя. Но самое интересное в этой проблеме — пожалуй, то, что часто ее можно предотвратить заранее, поскольку наиболее распространенными уязвимостями на сегодняшний день все еще являются использование устаревшего оборудования (например, машины для голосования могут долгое время не использоваться, поскольку выборы происходят лишь с определенной периодичностью, это значит, что их программное обеспечение обновляется гораздо реже, чем другие электронные системы) и дефицит цифровой грамотности среди сотрудников той или иной информационной системы, так как они менее способны оценить надежность или происхождение источников кибератаки и могут, сами того не зная, запустить ее. Именно поэтому проблема политического влияния посредством кибератак должна решаться комплексно, в противном случае киберугрозы смогут повлиять не только на результаты выборов, но и на ключевые демократические мероприятия по участию, общественному обсуждению и институциональным действиям граждан.

Литература

1. *Володенков С.В.* Киберсимулякры как инструмент виртуализации современной массовой политической коммуникации [Электронный ресурс] // Информационные войны. — 2020. — № 4 (32). — URL: http://pstmprint.ru/wp-content/uploads/2016/11/INFW-4-2014-3.pdf (дата обращения: 24.12.20).
2. Касперский считает, что пандемия привела к активизации кибератак на 20–25% [Электронный ресурс] // ТАСС. — 2020. — URL: https://tass.ru/ekonomika/10070887 (дата обращения: 24.12.20).
3. *Панарин И.Н.* Информационная война и выборы. — М.: Издательский Дом «Городец», 2003. — 416 с.
4. Почему в Никарагуа не стихают протесты [Электронный ресурс] // Независимая газета. — 2019. — URL: https://www.ng.ru/vision/2019-03-06/7_7525_nikaragua.html (дата обращения: 24.12.20).
5. Путин: хакерами может двигать патриотический настрой [Электронный ресурс] // BBC News. — 2017. — URL: https://www.bbc.com/russian/news-40118501 (дата обращения: 24.12.20).
6. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // Президент Российской Федерации [Офиц. сайт]. — URL: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (дата обращения: 24.12.20).
7. "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards? [Электронный ресурс] // Just Security. — 2016. — URL: https://www.justsecurity.org/35652/hacked-election-international-law-silentfaced-clatter-cyrillic-keyboards/ (дата обращения: 24.12.20).
8. Australia's cyber security strategy 2020, p. 17 [Электронный ресурс] // Australian Government [Офиц. сайт]. — URL: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf (дата обращения: 24.12.20).
9. Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally, Threat Research [Электронный ресурс] // FireEye. — 2018. — URL: https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html (дата обращения: 24.12.20).
10. *Tenove* C. Digital threats to democratic elections: How Foreign Actors Use Digital Techniques to Undermine Democracy [Электронный ресурс] // Centre for the Study of Democratic Institutions. — University of British Columbia. — Political Science. — 80 p. — URL: http://pdfs.semanticscholar.org/ca1e/7ee79c0eb0720cc2343f5198eae86d20ac94.pdf (дата обращения: 24.12.20).
11. Cyber Threat Map, [Электронный ресурс] // FireEye. — URL: https://www.fireeye.com/cyber-map/threat-map.html (дата обращения: 24.12.20).

12. *Sanger D.E., Shane S.* Russian Hackers Acted to Aid Trump in Election, U.S. Says [Электронный ресурс] // The New York Times. — 2016. — URL: http://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?_r=0 (дата обращения: 24.12.20).
13. Everything We Know About Russian Election-Hacking [Электронный ресурс] // Wired. — 2017. — URL: https://www.wired.com/story/russia-election-hacking-playbook/ (дата обращения: 24.12.20).
14. Generalitat de Catalunya, Referèndum d'autodeterminació de Catalunya, Resultats definitius, p. 2, [Электронный ресурс] // Generalitat de Catalunya [Офиц. сайт]. — 2017. — URL : https://web.archive.org/web/20171008152256/http://www.govern.cat/pres_gov/AppJava/docrel/nota-premsa/contingut/download/220434.htm?mode=static (дата обращения: 24.12.20).
15. *Van De Velde J.* The Law of Cyber Interference in Elections [Электронный ресурс] // SSRN. — 2017. — 25 p. — URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828 (дата обращения: 24.12.20).
16. *Schmitt M.*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. — Cambridge University Press, 2017. — 638 p.
17. *Morell M., Suzanne Kelly*, Fmr. CIA Acting Dir. Michael Morell: "This Is the Political Equivalent of 9/11" [Электронный ресурс] // The Cipher Brief. — 2016. –https://www.thecipherbrief.com/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091. Цитирован в *Spencer McKay, Tenove C.* Disinformation as a Threat to Deliberative Democracy [Электронный ресурс] // Political Research Quarterly. — 1–15. — University of Utah. — 2020. — 15 p. — URL: https://journals.sagepub.com/doi/abs/10.1177/1065912920938143?journalCode=prqb (дата обращения: 24.12.20).
18. M-Trends 2020, Special Report [Электронный ресурс] // FireEye. — 2020. — URL: https://content.fireeye.com/m-trends/rpt-m-trends-2020 (дата обращения: 24.12.20).
19. National Cyber Strategy of the United States of America [Электронный ресурс] // National Security Council. — 2018. — URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 24.12.20).
20. *Stedmon N.* The Impact of Cyber Security Threats on the 2020 US Elections [Электронный ресурс] // Cyber Security and Human Factors. — Bournemouth University Poole, United Kingdom. — 2020. — 3 p. — URL: https://arxiv.org/ftp/arxiv/papers/2012/2012.08968.pdf.
21. Notorious hackers claim responsibility for Labour cyber attacks and threaten to target Corbyn's family [Электронный ресурс] // Independent. — 2019. — URL: https://www.independent.co.uk/news/uk/politics/labour-cyber-attack-lizard-squad-ddos-corbyn-general-election-a9202006.html (дата обращения: 24.12.20).
22. *Wray S.* On electronic civil disobedience, Electronic Civil Disobedience: and Other Unpopular Ideas [Электронный ресурс] // Peace Review. — A Journal of Social Justice. — Vol. 11. — Iss. 1: Media and Democratic Action — 1999. — P. 107–111. — URL: https://www.tandfonline.com/doi/abs/10.1080/10402659908426237 (дата обращения: 24.12.20).
23. Stratégie nationale pour la sécurité du numérique de France, 2015, p. 38, [Электронный ресурс] // ANSSI [Офиц. сайт]. — URL: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (дата обращения: 24.12.20).
24. Sudan's Bashir bans protests in latest emergency measures [Электронный ресурс] // REUTERS. — 2019. — URL: https://br.reuters.com/article/us-sudan-protests-emergency/sudans-bashir-bans-protests-in-latest-emergency-measures-idUSKCN1QE26C (дата обращения: 24.12.20).
25. Taiwan says China behind cyberattacks on government agencies, emails [Электронный ресурс] // Reuters. — 2020. — URL: https://www.reuters.com/article/us-taiwan-cyber-china-idUSKCN25F0JK (дата обращения: 24.12.20).
26. Taiwan's citizens battle pro-China fake news campaigns as election nears [Электронный ресурс] // The Guardian. — 2019. — URL : https://www.theguardian.com/world/2019/dec/30/taiwan-presidential-election-referendum-on-ties-with-china.
27. The great Catalonian cyberwar of 2017 [Электронный ресурс] // The Washington Post. — 2017. — URL: https://www.washingtonpost.com/news/democracy-post/wp/2017/10/18/the-great-catalonian-cyberwar-of-2017/ (дата обращения: 24.12.20).

28. The Perfect Weapon: How Russian Cyberpower Invaded the U.S. [Электронный ресурс] // The New York Times. — 2016. — URL: https://www.nytimes.com/2016/12/21/world/russia-hack-presidential-election.html (дата обращения: 24.12.20).
29. Threat Advisories and Attack Reports OpCatalonia [Электронный ресурс] // Radware. — 2017. — URL: https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opcatalonia/%20 (дата обращения: 24.12.20).
30. Threat Research, Election Cyber Threats in the Asia-Pacific Region [Электронный ресурс] // FireEye. — 2020. — URL: https://www.fireeye.com/blog/threat-research/2020/11/election-cyber-threats-in-the-asia-pacific-region.html (дата обращения: 24.12.20).
31. Top-secret NSA report details Russian hacking effort days before 2016 election [Электронный ресурс] // The Intercept. — 2017. — URL : https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.
32. Wired, Everything We Know About Russia's Election-Hacking Playbook [Электронный ресурс] // Wired. — 2017. — URL: https://www.wired.com/story/russia-election-hacking-playbook/ (дата обращения: 24.12.20).
33. #OpNicaragua: El Ministerio de Relaciones Exteriores de Costa Rica y el Gobierno de Nicaragua son atacados por los hackers internacionales [Электронный ресурс] // EnHacke. — 2019. — URL: https://www.enhacke.com/2019/03/17/opnicaragua-el-ministerio-de-relaciones-exteriores-de-costa-rica-y-el-gobierno-de-nicaragua-son-atacados-por-los-hackers-internacionales/ (дата обращения: 24.12.20).
34. #OpSudan: Hacktivists Around The World Prepare for Massive Cyber Attacks Against The Government of Sudan [Электронный ресурс] // The Creators Tribune. — 2019. — URL: https://creatorstribune.com/2019/04/06/opsudan-hacktivists-around-the-world-prepare-for-massive-cyber-attacks-against-the-government-of-sudan/ (дата обращения: 24.12.20).