XXI ВЕК

Н. В. КАРДАВА

КИБЕРПРОСТРАНСТВО КАК НОВАЯ ПОЛИТИЧЕСКАЯ РЕАЛЬНОСТЬ: ВЫЗОВЫ И ОТВЕТЫ

Автор рассматривает киберпространство как новое измерение политического пространства и как поле политического взаимодействия и противостояния различных политических акторов. Проанализированы основные исторические этапы возникновения угроз кибербезопасности и ответных мер по ее укреплению. Показано, что в современном мире киберпреступность, промышленный шпионаж, деятельность разведывательных служб и международный терроризм с использованием киберпространства тесно взаимосвязаны. При этом непрерывное и быстрое развитие киберугроз в киберпространстве постоянно порождает необходимость совершенствования кибербезопасности. Для России проблема кибербезопасности становится все более актуальной из-за деятельности иностранных разведывательных служб, хакеров, киберпреступников и международных террористов. В связи с этим в условиях сегодняшней России кибербезопасность становится одним из важнейших направлений обеспечения внутренней безопасности.

Ключевые слова: *политическое пространство, политические акторы, киберпространство, кибербезопасность, киберпреступность, международный терроризм, хакеры.*

В современном мире под влиянием быстрого развития информационных технологий формируются новые – «виртуальные» – измерения политических пространств, которые становятся все более значимыми для внутренней и международной политики. К числу таких «виртуальных» измерений относится *киберпространство*, *обозначающее особую область социальных взаимодействий, опосредованных совокупностью процессов, протекающих в компью-*

терных сетях мира, и превратившееся в еще одну среду обитания и деятельности человека. Помимо Интернета в киберпространство входят многие другие компьютерные сети, например транснациональные, через которые происходит передача данных о финансовых потоках, торгах на различных биржах и операциях по кредитным картам (Господарик, Пашковская 2016: 123). Кроме того, в киберпространстве функционируют системы управления разнообразными машинами и механизмами, например панели управления генераторами, лифтами, насосами, транспортными и энергетическими системами и др. Особую и весьма важную часть киберпространства представляют компьютерные сети управления военной техникой, в том числе беспилотниками (дронами), боевыми роботами, ракетами различного радиуса действия. Уже из этого краткого и далеко не полного перечисления следует, что киберпространство в настоящее время представляет собой жизненно важную область информационной, экономической, политической, военной деятельности отдельных людей, корпораций, государств и их союзов, наднациональных структур и образований.

В современном мире киберпространство, которое не знает государственных границ, становится важнейшим полем политической, экономической, информационной и культурной конкуренции. По существу, киберпространство благодаря быстрому развитию информационных технологий представляет собой политическое пространство нового («виртуального») типа, в котором сталкиваются интересы различных политических субъектов, разных государств и центров политической силы. Почти сразу же после своего возникновения киберпространство превратилось в пятое (после земли, моря, воздуха и космоса) поле битвы различных политических и военных сил и продолжает оставаться таковым. Более того, многие битвы между разведывательными организациями разных стран, их военными структурами, а также экономические и информационные сражения, включая экономический шпионаж и финансовые диверсии, развертываются именно в киберпространстве. Это обстоятельство определяет высокую значимость процессов, протекающих в киберпространстве, для современного политического анализа, теории и практики политической науки.

По мере развития киберпространства в нем возникали и усиливались различные угрозы, а также ответные меры по противодействию этим угрозам и их нейтрализации. Согласно определению Международного союза электросвязи, *кибербезопасность* представляет собой набор средств, стратегии и принципы обеспечения безопасности, гарантии безопасности, подходы к управлению рисками, действия и практический опыт, страхование и технологии, которые могут быть использованы для защиты киберсреды, ресурсов организации и пользователя.

Кибербезопасность включает меры по охране и действия, которые можно осуществить для защиты киберпространства как в гражданской, так и в военной области от угроз, которые связаны со сформировавшимися в нем взаимозависимыми сетями и информационной инфраструктурой или могут нанести данной инфраструктуре урон. Очевидно, что кибербезопасность не может рассматриваться изолированно от других аспектов и видов внутренней и международной безопасности, а киберпреступность тесно связана с другими видами преступности, такими как промышленный шпионаж, деятельность иностранных разведывательных служб, международный терроризм (Шрайер и др. 2013: 2). В то же время кибербезопасность имеет ярко выраженную специфику, которая определяется использованием быстро развивающихся информационных технологий, ее необходимо рассматривать как особую сферу внутренней и международной безопасности с собственными тенденциями развития и своими инструментами.

При этом одной из специфических черт кибербезопасности является то, что граница между киберпреступностью, использованием кибероружия и действиями различных политических акторов (например, спецслужб различных государств) является достаточно размытой и неопределенной. Отсюда возникает сложность идентификации источника и характера угроз для киберпространства, которая уже стала фактором многочисленных внутриполитических и международных конфликтов, взаимных обвинений и политической «борьбы без правил». Одним из наиболее серьезных и масштабных по своим последствиям конфликтов такого рода стало обвинение со стороны руководства Демократической партии США «русских хакеров» во взломе ее информационных ресурсов и вмешательстве

в президентскую кампанию Соединенных Штатов в 2016 г. Тем самым было продекларировано заявление о воздействии России на внутриполитическую ситуацию в США и растиражирована версия о поддержке Россией Д. Трампа, что якобы стало чуть ли не основным фактором его избрания президентом. Несмотря на отсутствие каких-либо серьезных доказательств вмешательства России в американские дела и надуманность самих обвинений во «вмешательстве», эти нападки, связанные с атаками в киберпространстве, стали одним из важнейших факторов как многочисленных внутриполитических конфликтов в США, так и резкого обострения российско-американских отношений. Таким образом, уже один этот факт говорит об огромном и всевозрастающем влиянии процессов в киберпространстве на внутреннюю и мировую политику, а также о растущем значении кибербезопасности в современных условиях, но прежде всего о том, что процессы, происходящие в киберпространстве, и даже сама угроза использования возможностей «кибератак» становятся важнейшим политическим ресурсом ключевых акторов современной политики.

Говоря о целенаправленном применении кибероружия в международной и внутренней политике, можно также привести следующие факты. Одно из первых масштабных применений кибероружия произошло в Иране в 2009–2010 гг. В отличие от обычных вредоносных программ, работающих в популярных операционных системах, примененный против Ирана вирус Stuxnet специально был создан для проникновения в промышленные компьютеры. Данный вирус парализовал ядерную программу Ирана, из-за чего производство урана в этой стране сократилось на 20 %. В результате ряда разоблачений и утечек информации можно утверждать, что этот вирус был разработан специалистами США и Израиля (Господарик, Пашковская 2016: 125).

По данным, опубликованным в ряде СМИ, Агентство национальной безопасности США установило прослушку кабинетов представительства Евросоюза в Вашингтоне, штаб-квартиры ООН в Нью-Йорке и Совета ЕС в Брюсселе. Прослушке также подвергались 38 посольств и миссий различных стран в Нью-Йорке и Вашингтоне. Самыми громкими дипломатическими скандалами стали прослушка телефонных переговоров президента Бразилии Дилмы

Русеф и канцлера Германии Ангелы Меркель, а также перехват защищенной спутниковой связи с Москвой Д. А. Медведева из Лондона во время саммита G20 в апреле 2009 г. (Господарик, Пашковская 2016: 127).

Киберугрозы оказали существенное влияние на политическую обстановку в мире: помимо упомянутой выше утечки писем Демократической партии США можно упомянуть раскрытие офшорных счетов Mossack Fonseca и деятельность группировки Fancy Bears. Предпосылками усиления современных угроз в киберпространстве стали такие факторы, как отставание средств защиты от киберугроз, обострение политической борьбы внутри отдельных стран и на международной арене, нехватка квалифицированных кадров в отрасли, а также рост технологических возможностей кибератак.

История киберугроз и кибербезопасности: основные этапы

История киберпреступлений и других киберугроз тесно связана с историей развития хакерства. *Хакер* – это высококвалифицированный специалист по информационным технологиям (IT-хакер), который понимает тонкости работы ЭВМ, ее программирования, изменения существующих и создания новых компьютерных программ. Различают два вида IT-хакеров: «белые хакеры» («white hat») и «черные хакеры» («black hat»). «Черными хакерами» называют киберпреступников, тогда как «белыми» – прочих специалистов по информационной безопасности (в частности, сотрудников крупных IT-компаний), не нарушающих закон. В то же время следует иметь в виду, что грань между «белыми» и «черными» хакерами достаточно условна, так как нередки примеры, когда пойманные с поличным «черные» хакеры оказывались «белыми» и наоборот. К хакерам иногда относят и так называемых *фрикеров*, отличие которых от хакеров состоит в том, что это злоумышленники, скрытно взламывающие телефонные автоматы, телефонные сети и сети мобильной связи. Обычно фрикинг осуществляется для бесплатных звонков, пополнения личного мобильного счета и т. п.

Можно выделить следующие основные периоды истории возникновения и первоначального развития хакерства (Николаева, Тумбинская 2014).

В период 1960-х гг. началось зарождение хакерства, появились первые компьютерные хакеры в Массачусетском технологическом институте (MIT). Некоторые члены группы начали обращать свой «пытливый ум» на использование нового университетского компьютера в собственных целях и манипулирования программами.

В 1970-е гг. фрикеры взламывали местные и международные телефонные сети, чтобы звонить бесплатно. «Отец» фрикеров, участник войны во Вьетнаме Джон Дрэйпер (известный как Cap'n Crunch) обнаружил, что игрушечный свисток-сувенир, который он нашел в коробке овсяных хлопьев Cap'n Crunch, издает звук с частотой 2600 герц, совпадающей с частотой электрического сигнала доступа в телефонную сеть дальней связи AT&T.

В 1980-е гг. появились хакерские доски сообщений и сообщества хакеров. Телефонные фрикеры начали заниматься компьютерным хакерством, возникли первые системы электронных досок объявлений (BBS), предшественников групп новостей Usenet и электронной почты. BBS с такими названиями, как «Sherwood Forest» и «Catch-22», стали местами встреч хакеров и фрикеров, обмена опытом по краже паролей и номеров кредитных карт. Начали формироваться хакерские группы. Первыми были Legion of Doom в США и Chaos Computer Club в Германии.

В 1983 г. широкой общественности был представлен первый фильм про хакеров «Военные игры» («War Games»). Главный персонаж – хакер – проникает в некий компьютер производителя видеоигр, который оказывается боевым симулятором ядерного конфликта, принадлежащего военным. В результате возникает реальная угроза ядерной войны, военные переходят в режим «DefCon 1» (Defense Condition 1 – высшая степень состояния боеготовности). Начинает формироваться образ хакера-кибергероя (и антигероя).

В том же 1983 году были арестованы шестеро подростков, называвших себя «бандой 414». В течение 9 дней они взломали 60 компьютеров, среди которых были машины Лос-Аламосской лаборатории ядерных исследований в США.

В 1984 г. началась публикация хакерского журнала «2600». Редактор этого журнала Эммануэль Гольдштейн взял псевдоним главного героя произведения Дж. Оруэла «1984». Название журналу, как легко догадаться, дала свистулька первого фрикера Cap'n Crunch

в 2600 герц. «2600», а также вышедший годом ранее онлайновый журнал «Phrack» публиковали обзоры и советы для хакеров и фрикеров.

В 1986 г. для того, чтобы решить проблему увеличения количества взломов государственных и корпоративных компьютеров или хоть как-то покончить с хакерством, Конгресс США впервые за свою историю принял закон «Computer Fraud and Abuse Act», который признал взлом компьютеров преступлением. Но имелось одно ограничение – данный закон не мог распространяться на несовершеннолетних.

2 ноября 1988 г. студент Корнеллского университета в США Роберт Моррис запустил в действие саморазмножающуюся программу под названием «Червь Морриса», которая вывела из строя около 6000 университетских и правительственных компьютеров по всей Америке, причинив огромный ущерб, который был оценен примерно в 96,5 млн долларов (Николаева, Тумбинская 2014).

Второй этап развития компьютерных преступлений начинается с середины 1990-х гг., в период, когда Интернет распространялся со стремительной скоростью. Это было время, когда персональные компьютеры и Всемирная сеть становились более доступными для всеобщего использования. В декабре 1995 г., по некоторым оценкам, было зарегистрировано 16 млн пользователей Интернета во всем мире, а уже к маю 2002 г. эта цифра возросла до 580 млн, что составляло почти 10 % от общего населения планеты (Там же).

Нужно отметить, что распространение Интернета по миру было неравномерным, например, более 95 % от общего числа интернет-соединений осуществлялись в США, Канаде, Европе, Австралии и Японии. Именно в это время в историю преступлений был введен новый вид преступлений, который носил название «взлом» (Там же).

Пропуская несколько более поздних этапов развития угроз в киберпространстве, можно констатировать, что количество кибератак на протяжении последних десятилетий непрерывно увеличивалось, а сами они становились все более изощренными. В то же время постоянно росла зависимость отдельных людей, фирм и корпораций, политических партий и других политических акторов, целых государств и наднациональных образований от Интернета

и других IT-сетей, необходимых для получения важнейших услуг и информации. Согласно сообщению компании McAfee, занимающейся вопросами безопасности, в 2011 г. было выявлено самое большое за всю историю количество скрытых угроз. В частности, сообщалось, что в настоящее время в мире блуждают не менее 70 млн различных элементов вредоносного программного обеспечения, а смартфоны превратились в одно из средств их распространения. Анализ показывает, что как минимум 70 % сообщений электронной почты – спам (World… 2012).

Параллельно с развитием киберпреступности развивались и системы защиты от нее, совершенствовалась кибербезопасность.

В 1988 г. использование Интернета населением находилось еще в стадии своего становления, и Регламент международной электросвязи (РМЭ), составленный в этом же году, еще не содержал четких положений, касающихся кибербезопасности. Однако в нем содержалось упоминание (статья 9) о недопустимости «технического ущерба», которое было добавлено для противодействия одному из первых элементов вредоносного программного обеспечения, компьютерному червю Морриса, блуждавшему в то время в киберпространстве. Спустя десятилетия значение защиты кибербезопасности чрезвычайно возросло и стало учитываться при пересмотре РМЭ. Существуют предложения добавить или изменить статьи в этом договоре, чтобы включить в него элементы, связанные с кибербезопасностью, в том числе меры по противодействию спаму (*Ibid.*).

Особый интерес представляет анализ укрепления кибербезопасности в самой развитой стране мира – Соединенных Штатах, которые первыми столкнулись с киберпреступностью, хакерами, хотя сами же во многом их и породили. Задача обеспечения безопасности информации в США начала решаться задолго до возникновения информационно-коммуникационных технологий (ИКТ) в их современном представлении как компьютерных и сетевых. Документы периода начала-середины XX в., принятые в США, имеют юридическую силу и по сей день. Например, положения закона «О связи» 1934 г. определяют полномочия президента страны по регулированию систем связи в интересах национальной обороны и безопасности. В настоящее время это касается в том числе и Интернета

(Карасев 2015: 13–14). В период 1960–1980-х гг. с развитием информационных систем и технологий в США был принят ряд законов по вопросам защиты компьютеров и информационных систем. В то время существовало лишь понятие «защита информации», решались задачи обеспечения конфиденциальности, доступности и целостности. Понятия «кибербезопасность» не существовало, и эта тематика не была предметом международных отношений, за исключением вопросов, связанных со шпионажем и электронной разведкой других государств (Там же).

В конце XX – начале XXI в. существенно изменились подходы к обеспечению безопасности киберпространства и использованию ИКТ. Теракты 11 сентября 2001 г., а также возрастающая угроза для экономики, во все большей степени зависящей от ИКТ, стали катализатором процесса модернизации системы кибербезопасности и безопасности объектов критически важной инфраструктуры. В первый президентский срок Дж. Буша-младшего политика его администрации по вопросам кибербезопасности была связана прежде всего с введением интегрированного подхода, который заключался в четком распределении ролей между ведомствами и агентствами при координирующей роли Министерства внутренней безопасности. Американская внешняя политика в киберпространстве в этот период была направлена на самостоятельные действия по обеспечению кибербезопасности, и, как следствие, международное сотрудничество в этой области почти не развивалось. В период второго президентского срока Дж. Буша-младшего политика кибербезопасности начала меняться, но ее трансформация на основе «Всеобъемлющей национальной инициативы кибербезопасности» произошла уже при президенте Б. Обаме, который в 2009 г. объявил обеспечение безопасности киберпространства, освоение и использование ИКТ в национальных интересах важнейшими государственными задачами (Там же).

В итоге в начале XXI в. в США была создана мощная система кибербезопасности, развитие и усложнение которой продолжается и сейчас. В то же время следует отметить, что США широко применяют созданные ими правовые, организационные и доктринальные инструменты использования ИКТ и политики кибербезопасности прежде всего для реализации своих глобальных политических

и экономических целей. В этой связи нельзя не заметить, что Соединенные Штаты активно продвигают свои взгляды на кибербезопасность и киберпространство, игнорируя подходы других государств к обеспечению информационной безопасности. Вместе с тем США, постоянно заявляющие о киберугрозах, исходящих от иностранных государств, прежде всего от России, не желают заключения международных соглашений в области обеспечения кибербезопасности и тем самым способствуют все большему усилению киберугроз, ведению кибервойн и т. п.

Россия и киберугрозы: новые вызовы для безопасности

В последние годы Россия не отстает от мировых показателей темпов роста киберпреступности. В 2011 г. российские хакеры заработали около 3,7 млрд долларов, а в 2013 г. удвоили данный показатель. В 2012 г. в России было зарегистрировано на 28 % больше высокотехнологичных преступлений в сравнении с предыдущим годом (Кофырин 2014). В 2013 г., согласно отчету Бюро специальных технических мероприятий (БСТМ) МВД РФ, количество зарегистрированных преступлений в сфере телекоммуникаций и компьютерных технологий увеличилось на 8,6 % и продолжает расти.

По данным «Лаборатории Касперского», в 2013 г. почти все компании Российский Федерации как минимум один раз в течение года подвергались внешним киберугрозам. Предприятия малого и среднего бизнеса в России теряют в среднем около 780 тыс. рублей вследствие каждой совершенной против них кибератаки. При этом бóльшая часть кибератак против российских предприятий и государственных учреждений совершается из-за рубежа.

Как известно, государственный переворот на Украине в 2014 г. и последовавшее за ним обострение международной политической ситуации радикально изменили отношения России не только с Украиной, но и с западными странами, в частности с Соединенными Штатами и Евросоюзом. На фоне введения США и ЕС экономических, торговых, военных и политических санкций в отношении России стала еще более актуальной проблема обеспечения кибербезопасности в РФ. Помимо политических санкций и кибервойны с использованием информационных технологий, которую ведут

спецслужбы западных государств, существуют также угрозы, исходящие от других игроков цифрового мира. Среди них следует выделить действия хакеров, взломщиков и кракеров, которые осуществляют свои акции не только внутри страны, но и из-за рубежа.

Чтобы противодействовать киберугрозам в отношении России, летом 2014 г. Федеральное собрание РФ приняло закон, обязывающий интернет-компании защищать данные о пользователях из Российской Федерации на территории страны. Такой порядок был введен в действие с 1 сентября 2016 г. Однако это не остановило американские спецслужбы в их стремлении получить сведения об интересующих их лицах, даже если эти сведения хранятся за рубежом. Поэтому необходимы разработка и внедрение дополнительных мер, направленных на противодействие киберугрозам и кибервойне, которую ведут США и другие западные государства против РФ. Среди таких мер могут быть, например, дополнительная и более надежная защита от взломов информационных ресурсов наиболее важных государственных организаций, прежде всего работающих в сфере обороны и национальной безопасности, а также ресурсов, стратегически важных для развития экономики российских корпораций и компаний.

Как известно, Вашингтон неоднократно обвинял Москву в попытке повлиять на выборы американского президента в 2016 г. По версии спецслужб США, российская разведка использовала две хакерские группировки – Fancy Bears и Cozy Bear – для взлома серверов Демократической партии. В то же время эти обвинения американской стороны не подкреплены никакими серьезными доказательствами и активно используются во внутриполитической борьбе, которая развернулась в США между республиканцами и демократами после избрания президентом Д. Трампа. Поэтому Россия отвергает обвинения в причастности к этим взломам.

Согласно данным совместного исследования Group-IB, Microsoft и ФРИИ, суммарный ущерб экономике России от киберпреступности уже к началу 2016 г. достиг 203,3 млрд рублей, что составляло 0,25 % от ВВП России и равнялось почти половине расходов федерального бюджета на здравоохранение в 2015 г. По некоторым оценкам, ущерб только от кибератак на российскую фи-

нансовую сферу за два года (2016–2017 гг.) составил более 117 млн долларов. В августе 2017 г. генпрокурор России Юрий Чайка заявил, что ущерб от киберпреступлений в РФ за первое полугодие 2017 г. превысил 18 млн долларов. Кроме того, он сообщил, что количество киберпреступлений в России за последние три года (2015–2017 гг.) увеличилось в шесть раз. Все это позволяет говорить о том, что российская экономика и российское государство сталкиваются с серьезными киберугрозами.

Отечественные СМИ также подвергаются постоянным кибератакам, причем в данном случае очевидно, что заказчиками (а нередко и исполнителями) данных киберпреступлений являются прежде всего резиденты США и стран ЕС; против России ведется настоящая информационная и кибервойна. В конце октября 2017 г. вирусной атаке подверглись информационное агентство «Интерфакс» и его проекты, включая базу данных СПАРК, а также информационное агентство ТАСС и новостное издание «Фонтанка.ру». Специалисты «Лаборатории Касперского» заявили, что СМИ стали жертвами целенаправленной атаки вируса-шифровальщика.

Все это заставило российских пользователей принять активные меры защиты против кибератак. В апреле 2017 г. «Лаборатория Касперского» зафиксировала некоторое уменьшение доли российских пользователей, подвергающихся киберугрозам и пренебрегающих компьютерной защитой. Об этом свидетельствует обновленный индекс информационной безопасности (Kaspersky Cybersecurity Index), рассчитанный компанией на основании проведенных ею опросов пользователей по итогам второй половины 2016 г. (Россияне... 2017).

В основу данного индекса легли три индикатора, отражающие отношение респондентов к киберугрозам:

• необеспокоенные (Unconcerned) – доля пользователей, которые не верят, что они могут стать жертвами киберпреступников;

• незащищенные (Unprotected) – доля пользователей, которые не установили защиту на свои компьютеры, планшеты и смартфоны;

• пострадавшие (Affected) – процент пользователей, которые стали жертвами киберпреступников.

Таким образом, индекс кибербезопасности в России за вторую половину 2016 г. выглядит так: 83 % – 37 % – 33 % (Unconcerned – Unprotected – Affected). Другими словами, подавляющее большинство российских пользователей (83 %) не верят, что киберугрозы могут как-либо затронуть их жизнь, причем этот показатель не изменился с первой половины 2016 г. Более трети пользователей (37 %) до сих пор пренебрегают защитными программами, при составлении первого индекса таких было чуть больше – 39 %. Наконец, 33 % опрошенных россиян признались, что сталкивались с киберугрозами. Этот показатель изменился в лучшую сторону по сравнению с первой половиной 2016 г., когда жертвами киберпреступников стали 42 % российских пользователей (Россияне… 2017).

Для сравнения: глобальный индекс кибербезопасности выглядит так: 74 % – 39 % – 29 %. Это несколько парадоксальное соотношение свидетельствует одновременно и о меньшей обеспокоенности россиян по сравнению с жителями мира в среднем, и о том, что жертв киберпреступников в России несколько больше, чем в среднем по миру. Возможно, этот парадокс объясняется более легкомысленным отношением части россиян к кибератакам.

В России в последние годы предпринимаются определенные шаги по усилению кибербезопасности. Во-первых, в 2016 г. появился Центр обнаружения, предупреждения и ликвидации последствий компьютерных атак (КЦОПЛ) госкорпорации «Ростех», в том же году был проведен тендер корпорации АФК «Система» по защите от кибератак, было заявлено намерение ФСО привлечь Государственную систему обнаружения, предупреждения и ликвидаций последствий компьютерных атак (ГосСОПКА) для создания и обеспечения работы закрытой государственной сети RSNet. Во-вторых, появился документ «Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА» (Бодрик 2017; 2018). Однако эти меры явно недостаточны, учитывая резко возросшее количество кибератак в России. Развитие рынка кибербезопасности в стране сдерживается главным образом нехваткой финансовых средств, а также не вполне продуманной и разработанной государственной системой киберзащиты.

Подводя итоги, следует отметить быстрый рост киберпреступности и количества кибератак как в России, так и во всем мире. Во многом это вызвано не только и не столько ростом киберпреступности со стороны индивидуальных хакеров, сколько тем обстоятельством, что киберпространство стало важнейшим полем политической и экономической борьбы, в которой участвуют спецслужбы различных стран (прежде всего США), политические партии, транснациональные корпорации, военные разведывательные службы и другие политические акторы. По существу, в киберпространстве идет кибервойна, кипят битвы, от исхода которых во многом зависит политический и экономический суверенитет государства (Kaplan 2016). Учитывая это обстоятельство, Российской Федерации, ее важнейшим государственным органам и корпорациям придется не только участвовать в отражении многочисленных кибератак, но и готовиться к формированию собственного киберпространства, своих сетей передачи особо важной, конфиденциальной информации, от которой зависит безопасность страны и ее граждан. Речь при этом идет не об отключении обычных пользователей от Всемирной паутины Интернет и не о цензуре в ней, а о создании особых сетей для обмена информацией между наиболее важными политическими и экономическими акторами. Эта весьма актуальная в современных политических условиях задача должна решаться быстро и динамично, так как без ее решения безопасности России и ее граждан может быть нанесен значительный и непоправимый ущерб.

Литература

Бодрик, А.

2017. Кибербезопасность России: итоги 2016 года и стратегии для 2017-го. *IT Week. Безопасность* 10 января. URL: https://www.itweek.ru/security/article/detail.php?ID=191370 (дата обращения: 25.04.2018).

2018. Кибербезопасность России: итоги 2017 года и стратегии для 2018-го. *PC Week* 2(938) 27 марта. URL: https://www.itweek.ru/security/article/detail.php?ID=199494 (дата обращения: 25.04.2018).

Господарик, Ю. П., Пашковская, М. В. 2016. *Международная экономическая безопасность:* учеб. М.: Моск. фин.-пром. ун-т «Синергия». 417 с.

Карасев, П. А. 2015. *Политика безопасности США в глобальном информационном пространстве:* дис. … канд. полит. наук. М.: ИМЭМО РАН. 215 с.

Кофырин, Н. 2014. Киберпреступность в России. *Эхо Москвы* 29 марта. URL: http://echo.msk.ru/blog/nikolay_kofyrin/1289342-echo/ (дата обращения: 25.04.2018).

Николаева, А. Б., Тумбинская, М. В. 2014. Киберпреступность: история развития, проблемы практики расследования. *Труды SORUCOM-2014. Третья международная конференция «Развитие вычислительной техники и ее программного обеспечения в России и странах бывшего СССР: история и перспективы (Sorucom-2014)». 13–17 октября.* Казань: Казанский нац. исслед. техн. ун-т им. А. Н. Туполева. С. 253–258.

Россияне стали меньше сталкиваться с киберугрозами: «Лаборатория Касперского» обновила индекс информационной безопасности. 2017. *Лаборатория Касперского* 27 апреля. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-index (дата обращения: 25.04.2018).

Шрайер, Ф., Викс, Б., Винклер, Т. Х. 2013. *Кибербезопасность: дорога, которую предстоит пройти.* Женева: Жен. центр демокр. контроля над воор. силами (DCAF). 52 с.

Kaplan, F. 2016. *Dark Territory. The Secret History of Cyber War*. New York; London; Toronto; Sydney; New-Delhi: Simon & Schuster. 342 pp.

World Conference on International Telecommunications (ITU–SG WCIT-12). 2012. WCIT Background Brief. Dubai, UAE 3–14 December. URL: https://www.itu.int/en/wcit-12/Documents/WCIT-background-brief6-R.pdf (дата обращения: 25.04.2018).