М.В. Смекалова*

ЭВОЛЮЦИЯ ДОКТРИНАЛЬНЫХ ПОДХОДОВ США К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЕ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Федеральное государственное бюджетное учреждение науки
«Институт Соединенных Штатов Америки и Канады
Российской академии наук»
123995, Москва, Хлебный пер., 2/3

Интернет-технологии за время своего существования создали как массу новых возможностей для экономического развития, так и целый ряд опасностей для мирового сообщества. Вызовы и угрозы, исходящие из информационного пространства, были включены в приоритетные направления работы ведущих государств мира в начале 2000-х годов. США одними из первых стали прорабатывать законодательные основы киберполитики, нацеленной прежде всего на обеспечение безопасности страны после терактов 2001 г. С течением времени был принят не один десяток законодательных актов, создан ряд комитетов и агентств, ответственных за обеспечение информационной безопасности страны. В статье изучена эволюция доктринальных подходов США к обеспечению информационной безопасности (в американских документах — кибербезопасности) в годы пребывания у власти трех президентов: Дж. Буша-мл. (при котором появилась первая Национальная стратегия кибербезопасности), Б. Обамы и Д. Трампа. Прослежено, как со временем менялись приоритеты американской политики в данной области, а также рассмотрено развитие отношений США с другими ведущими игроками в киберсфере, прежде всего Российской Федерацией и КНР. Особое внимание уделено политике Вашингтона, направленной на обеспечение безопасности критической информационной инфраструктуры (КИИ). Указывается, что, несмотря на принятие целого ряда регулирующих нормативных актов, уровень безопасности объектов КИИ остается достаточно низким. В целом анализ доктринальных документов позволил выделить несколько ключевых особенностей, характеризующих развитие политики США в области кибербезопасности в последние годы. В частности, усиливается тенденция к проведению односторонних действий, связанных с оказанием санкционного давления на те или иные страны и их

* *Смекалова Мария Владимировна* — аспирант Института США и Канады Российской академии наук (e-mail: mashasmekalova@gmail.com).

компании. При этом проблематика кибербезопасности зачастую рассматривается не как самостоятельное направление, а лишь как инструмент для достижения иных, более широких внешне- и внутриполитических целей. Автор приходит к выводу, что в целом политика США в области обеспечения информационной безопасности носит скорее реактивный характер, что не может не отражаться на ее эффективности.

Ключевые слова: Соединенные Штаты Америки, США, информационная безопасность, кибербезопасность, киберугрозы, киберстратегия, критическая информационная инфраструктура, КИИ, санкции.

С начала XXI в. проблемы, связанные с киберсферой, все больше определяют международную повестку дня. В российских документах принято использовать понятие «информационно-коммуникационные технологии» (ИКТ)[1], однако именно термины с приставкой «кибер-» наиболее употребимы в зарубежном академическом и политическом дискурсе. Подобное проникновение характеристики произошло не только в связи с беспрецедентным развитием ИКТ, но также ввиду приобретения ими политического характера и их широкого распространения в межгосударственных отношениях. Важным трендом стало растущее внимание ведущих государств к проблематике киберугроз национальной безопасности. Основным актором, инициировавшим данный тренд, можно считать Соединенные Штаты Америки, которые посредством обвинений России[2] в кибератаках и вмешательстве в американские внутренние дела вывели проблематику кибербезопасности на первые страницы газет и журналов[3]. При этом в США разрабатывались и прини-

---

[1] См., например: Доктрина информационной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Официальный сайт Президента России. Доступ: http://kremlin.ru/acts/bank/41460 (дата обращения: 05.05.2019); Материалы Седьмой научной конференции Международного исследовательского консорциума информационной безопасности // Институт проблем информационной безопасности МГУ. Доступ: http://www.iisi.msu.ru/UserFiles/File/publications/VII%20Forum.pdf (дата обращения: 05.05.2019).

[2] Fact Sheet President Donald J. Trump is Standing up to Russia's Malign Activities // The White House. Available at: https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-standing-russias-malign-activities/ (accessed: 01.05.2019).

[3] См., например: Потери компаний от кибератак в мире в 2019 году могут достигнуть $2,5 трлн // Коммерсант. 26.04.2019. Доступ: https://www.kommersant.

мались документы, призванные определить политику государства в информационном пространстве. Часть этих документов предваряла кризисные явления последних лет, в то время как новые стратегии носили реактивный характер.

В российских и зарубежных исследованиях традиционно много внимания уделяется выявлению и анализу ключевых факторов, определяющих действия ведущих государств в киберсреде [Стрельцов, Смирнов, 2017; Гаврилова и др., 2015]. Глобальные аспекты информационной безопасности отразили в своих работах П.А. Шариков и Е.С. Зиновьева [Шариков, 2015; Зиновьева, 2016]. К. Павлик, К. Куигли и Дж. Рой исследовали влияние развития интернет-технологий на законодательную политику государств [Pavlik, 2017; Quigley, Roy, 2012]. В свою очередь Н.П. Ромашкина особое внимание уделяет киберрискам с точки зрения международной стабильности и предотвращения ядерной войны [Ромашкина, 2016, 2018].

Проблематика киберрисков, прежде всего в контексте обеспечения безопасности объектов критической информационной инфраструктуры (КИИ) и деятельности крупных предприятий, вообще является очень динамично развивающимся направлением исследований. Так, последствия атак на объекты КИИ изучает группа британских экспертов [Ani et al., 2018]. На примере работы американских электростанций они доказывают, что законодательное регулирование защиты объектов КИИ не всегда приводит к минимизации рисков [Clark-Ginsberg, Slayton, 2019]. Угрозы, с которыми сталкиваются корпорации в наши дни, подробно рассмотрены в работах С. Романовского и Х. Катцана [Romanovsky, 2016; Katzan, 2016]. Ряд исследователей подчеркивают сложность определения финансового ущерба от предстоящих атак и сферы киберпреступности в целом [Riek, Böhme, 2018]. В связи с этим интересны подходы ученых к оценке рынка страхования от киберинцидентов и ценообразования подобных услуг [Romanovsky et al., 2019]. Особое внимание западные ученые уделяют важности угроз, исходящих от шифрования сообщений в мессенджерах [Endeley, 2018].

При этом перечисленные проблемы разбираются по-прежнему чаще всего с технической точки зрения (в этом отношении

ru/doc/3957187 (дата обращения: 10.05.2019); Cybercrime costs the world economy hundreds of billions // Time Magazine. 09.06.2014. Available at: http://time.com/2849814/cybercrime-costs-the-world-economy-hundreds-of-billions/ (accessed: 10.05.2019).

обращают на себя внимание доклады экспертов «Лаборатории Касперского», CISCO, Group-IB, а также аналитических центров — RAND Corporation[4], EastWest Institute[5], Российского совета по международным делам[6]).

В то же время проблемы политического реагирования на кибератаки и предпринимаемых властями США действий по защите объектов КИИ остаются сравнительно менее изученными в научном сообществе. Особого внимания заслуживают работы отечественных исследователей А.И. Смирнова и В.П. Шерстюка [Смирнов, 2005; Научные и методологические проблемы информационной безопасности, 2004], которые внесли значительный вклад в изучение позиции США в международных институтах по вопросам формулирования норм поведения в информационном пространстве и сопоставимости американской позиции с российской. П.А. Карасёв исследует формирование киберполитики США и ее военные аспекты [Карасев, 2013].

Цель данной статьи — проанализировать заявленные в ключевых американских доктринальных документах подходы к вопросам обеспечения кибербезопасности и защиты объектов КИИ. Автор ставит задачу выяснить, можно ли говорить о существовании согласованной линии в политике США в отношении информационного пространства, а также какой характер носит эта политика — проактивный или реактивный. Можно ли предположить, что разработка документов, регулирующих деятельность в киберсреде, нацелена исключительно на политическое позиционирование страны на международной арене и лишь подстраивается под сложившуюся внешнеполитическую обстановку? По мнению автора, на данном этапе в американском истеблишменте прослеживается четкое стремление к проведению жесткой политики относительно информационного пространства, попытки не только обезопасить государство от

---

[4] Blumenthal M.S. Why AV safety and cybersecurity need to be pursued in tandem // RAND Corporation. Available at: https://www.rand.org/blog/2019/03/why-av-safety-and-cybersecurity-need-to-be-pursued.html (accessed: 28.04.2019).

[5] McConnell B.W. Five ways to increase the security of cyber products and services // EastWestInstitute. Available at: https://www.eastwest.ngo/idea/five-ways-increase-security-cyber-products-and-serviceshttps://www.congress.gov/bill/116th-congress/senate-bill/482 (accessed: 28.04.2019).

[6] МакКоннелл Б., Шариков П., Смекалова М. Предложения по российско-американскому сотрудничеству в сфере кибербезопасности // Российский совет по международным делам. Доступ: https://russiancouncil.ru/activity/policybriefs/predlozheniya-po-rossiysko-amerikanskomu-sotrudnichestvu-v-sfere-kiberbezopasnosti/ (дата обращения: 10.05.2019).

любого рода вмешательства с использованием ИКТ, но и заранее объяснить потенциальные свои шаги в будущем. Действия руководства США на практике сводятся к разработке новых программных документов и созданию специализированных органов власти. При этом, несмотря на заявленные амбициозные цели, сложно говорить об эффективности принимаемых мер, так как угрозы, исходящие из информационного пространства, растут с каждым годом, а уровень защищенности объектов КИИ остается низким.

* * *

На правах пионера интернет-технологий США регулярно обновляют государственные документы, прямо или косвенно связанные с обеспечением кибербезопасности страны. Частая смена декларируемых приоритетов происходит не только ввиду прихода к власти новых администраций, но и в первую очередь в связи с беспрецедентным распространением ИКТ и постоянным технологическим развитием, стремительно опережающим действия государств.

Старт формулированию официальных подходов в рассматриваемой сфере был дан еще в 2003 г., в годы администрации Дж. Буша-мл., когда появилась Национальная стратегия кибербезопасности[7]. После террористических атак 11 сентября 2001 г. первоочередной задачей была объявлена борьба с терроризмом, при этом особое внимание уделялось защите инфраструктуры в киберпространстве как «нервной системы» государства. В предисловии к документу Дж. Буш-мл. объявил о необходимости защиты от вмешательства в функционирование информационных систем США, а также снижения уязвимостей на объектах КИИ. Интересно, что в видении президента основополагающим аспектом обеспечения кибербезопасности выступало государственно-частное партнерство. В качестве стратегических целей были обозначены предотвращение кибератак против объектов КИИ, снижение уровня уязвимости к кибератакам как таковым, а также минимизация ущерба и времени на восстановление. Центральным органом, ответственным за выполнение положений стратегии, было названо Министерство внутренней безопасности, созданное в 2002 г. В документе подчеркивалась важность

[7] The National Strategy to Secure Cyberspace. February 2003 // The White House. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed: 16.05.2019).

сотрудничества между государствами со схожим восприятием процессов и проблем киберпространства.

Таким образом, вопросы обеспечения кибербезопасности не только впервые появились в доктринальных документах США, но и приобрели четкие очертания: были обозначены основные участники этого процесса, выделены угрозы и поставлены первые задачи. Можно говорить о том, что на основе именно этой доктрины Дж. Буша-мл. выстраивалась дальнейшая политика защиты киберпространства США. Важно отметить, что обозначенный государственный документ был разработан в качестве реакции на сложившиеся угрозы и мировое технологическое развитие.

Внимание к вопросам кибербезопасности лишь усилилось с приходом администрации Б. Обамы: президент нередко заявлял, что это направление — один из приоритетов развития страны. В рамках Всеобъемлющей национальной инициативы кибербезопасности[8] (документ был принят при Дж. Буше-мл. в 2008 г., но реализовывался Б. Обамой) он призвал провести инвентаризацию государственных действий по защите информации и инфраструктуры. Была создана должность координатора государственной политики в области кибербезопасности, ответственного за организацию межведомственного взаимодействия. До этого соответствующими вопросами занимались различные ведомства, и новая должность должна была способствовать разработке консолидированной политики[9]. В целом стратегия Б. Обамы носила гораздо более глобалистский характер, чем у его предшественника: значительно большее внимание уделялось международному сотрудничеству в вопросах обеспечения кибербезопасности.

Эта тенденция получила наиболее яркое воплощение в 2011 г. с принятием Белым домом Международной стратегии для киберпространства[10], призванной способствовать созданию платформы для международного сотрудничества в сфере обеспечения

---

[8] Comprehensive National Cyberspace Initiative // The White House. Available at: https://fas.org/irp/eprint/cnci.pdf (accessed: 14.04.2019).

[9] Карасев П. Новые стратегии США в области кибербезопасности // Российский совет по международным делам. Доступ: http://russiancouncil.ru/analytics-and-comments/analytics/novye-strategii-ssha-v-oblasti-kiberbezopasnosti/ (дата обращения: 20.05.2019).

[10] International Strategy for Cyberspace // President of the United States. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed: 01.05.2019).

кибербезопасности на основе американской трактовки данного понятия, которую открыто не разделяла Россия[11]. Помимо этого ориентация на расширение международного взаимодействия в киберсфере проявилась в последующие годы в активной работе представителей США в деятельности Группы правительственных экспертов ООН. Вашингтон также развивал двусторонние переговорные процессы.

В этой связи особенно интересно рассмотреть соглашения США с Российской Федерацией и КНР как одними из основных игроков в глобальной борьбе за обеспечение информационной безопасности. Эти документы стали логичным продолжением политики Белого дома по своевременному реагированию на тренды в киберповестке дня. В то время как российско-американский документ в первую очередь касается вопросов национальной безопасности США, соглашение с Китаем сфокусировано на кибершпионаже и проблемах производства информационных технологий.

В 2013 г. на полях саммита «Группы восьми» состоялась встреча В. Путина и Б. Обамы, в ходе которой среди прочих вопросов обсуждались проблемы кибербезопасности. Результаты встречи[12] стали прорывом в политике по укреплению доверия между двумя странами. Главы государств договорились создать новую рабочую группу под эгидой Российско-американской президентской комиссии по развитию сотрудничества, в цели которой входили оценка возникающих киберугроз и предложение конкретных действий по реагированию на них. Для повышения прозрачности действий стороны договорились о следующих шагах:

1) обеспечить регулярный обмен данными между Центрами реагирования на компьютерные инциденты (стороны должны уведомлять друг друга в случае обнаружения злонамеренных действий, исходящих с территории второго государства);

---

[11] Официальная позиция Российской Федерации сводится к поддержке концепции «международной информационной безопасности» (МИБ), включающей более широкое наполнение. Согласно официальной трактовке международная информационная безопасность — это такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

[12] Встреча с Президентом США Бараком Обамой // Официальный сайт Президента России. Доступ: http://kremlin.ru/events/president/news/18355 (дата обращения: 18.05.2019).

2) использовать Центры снижения ядерных рисков для круглосуточной связи в целях сокращения угрозы эскалации в результате киберинцидентов;

3) к существующей «горячей линии» между Кремлем и Белым домом подсоединить прямую связь между координатором по вопросам кибербезопасности США и заместителем секретаря Совета безопасности РФ (линия может быть использована при необходимости оперативной реакции и принятия решения по ситуациям, возникающим в результате киберинцидента).

Руководителями рабочей группы были назначены заместитель секретаря Совета безопасности РФ Н.В. Климашин и специальный помощник Б. Обамы М. Дэниел[13]. На первом заседании группы, которое состоялось осенью 2013 г. в Вашингтоне[14], стороны обсудили общие подходы к вопросам интернет-безопасности и важность своевременного реагирования на инциденты.

Однако позитивная динамика взаимодействия по вопросам киберпроблематики сменилась кризисом в двусторонних отношениях, последовавшим за обвинениями в адрес России во вмешательстве во внутренние дела США и попытках оказать влияние на исход президентских выборов 2016 г. посредством использования киберинструментов. Несмотря на то что официального отказа от договоренностей 2013 г. не было, текущая повестка межгосударственного сотрудничества не позволяет говорить об изменении ситуации к лучшему и активному выполнению принятых сторонами на себя обязательств.

В целом похожую траекторию можно наблюдать и в развитии американо-китайского взаимодействия в киберсфере. В 2015 г. президент США Б. Обама встретился с председателем КНР Си Цзиньпином для обсуждения целого ряда вопросов двусторонних отношений[15]. В повестку дня вошли и проблемы обеспечения кибербезопасности, которым стороны уделили особое внимание. Главы двух государств пришли к консенсусу по следующим проблемным точкам:

---

[13] Сопредседателем российско-американской группы по кибербезопасности со стороны США назначен спецпомощник президента Майкл Дэниел // ТАСС. 21.10.2013. Доступ: https://tass.ru/politika/693170 (дата обращения: 18.05.2019).

[14] U.S.-Russia Bilateral Presidential Commission: 2013 Joint Annual Report // U.S. Department of State Archive. Available at: https://2009-2017.state.gov/p/eur/ci/rs/usrussiabilat/219086.htm#8 (accessed: 20.05.2019).

[15] President Xi Jinping's State Visit to the United States // Obama White House Archives. Available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed: 20.05.2019).

1) Вашингтон и Пекин договорились оперативно предоставлять друг другу информацию и помощь в случае выявления злонамеренных действий;

2) две страны должны сотрудничать в вопросах расследования киберпреступлений в той степени, в которой это позволяют внутреннее законодательство и существующие международные договоренности;

3) ни одна из сторон не будет осознанно осуществлять или поддерживать кражу интеллектуальной собственности с помощью интернета, включая детали торговых взаимоотношений или конфиденциальную информацию, связанную с ведением бизнеса, в целях получения конкурентных преимуществ для отдельных компаний или секторов экономики;

4) государства поддержали инициативы по разработке всеобъемлющих норм поведения в информационном пространстве, приветствуя успехи Группы правительственных экспертов ООН 2015 г., также была достигнута договоренность о создании совместной группы экспертов для дальнейших переговоров;

5) США и КНР приняли решение создать совместный высокоуровневый диалоговый механизм по борьбе с киберпреступностью и связанными проблемами. Посредством данного механизма планировалось отслеживать своевременность ответов на запросы о помощи и т.д. Встречи диалога должны были проходить на регулярной основе два раза в год[16].

Главы двух государств договорились создать «горячую линию» для реагирования на киберинциденты. Заседания рабочей группы проводились в намеченном порядке, а отчеты о проделанной работе, пусть и не раскрывающие никаких деталей повестки, появлялись на сайте Министерства юстиции США[17]. Уже при новой администрации, в 2017 г., состоялся первый американо-китайский Диалог по вопросам правоохранения и кибербезопасности[18], на котором стороны вновь подчеркнули приверженность договоренностям, достигнутым в 2015 г.

---

[16] Ibidem.

[17] См., например: First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes // The United States Department of Justice. Available at: https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0 (accessed: 20.05.2019); Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue // Department of Homeland Security. Available at: https://www.dhs.gov/news/2016/06/15/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue (accessed: 20.05.2019).

[18] First U.S.-China Law Enforcement and Cybersecurity Dialogue // Department of Homeland Security. 06.11.2017. Available at: https://www.dhs.gov/news/2017/10/06/first-us-china-law-enforcement-and-cybersecurity-dialogue (accessed: 20.05.2019).

Несмотря на существенный прогресс в переговорах прежней администрации США с китайскими коллегами, общая динамика всё же ухудшилась осенью 2018 г., когда представители Агентства национальной безопасности США заявили[19] о хакерских атаках со стороны Китая и нарушениях достигнутых ранее договоренностей.

Исходя из проанализированных документов и общей повестки внешнеполитических инициатив Б. Обамы, можно констатировать стремление его администрации к налаживанию диалога с ключевыми конкурентами и партнерами в вопросах кибербезопасности. С приходом администрации Д. Трампа негативные тренды, проявившиеся в российско-американских и китайско-американских связях, вышли на беспрецедентный уровень. В то время как напряжение в отношениях с Москвой было во многом продиктовано ситуацией вокруг предполагаемого вмешательства России в ход президентских выборов в США в 2016 г., на взаимоотношения с КНР в киберсфере повлияла начавшаяся между двумя странами торговая война, которая затронула и вопросы кибербезопасности. Описанная напряженность нашла отражение в доктринальных документах, принятых новой администрацией США.

В мае 2018 г. была опубликована Стратегия кибербезопасности[20] Министерства внутренней безопасности США, рассчитанная на пять лет и перечисляющая ключевые цели и задачи, стоящие перед ведомством до 2023 г.

В документе определены пять основных направлений деятельности:

1) выявление и оценка рисков;

2) сокращение уязвимостей (в рамках этого направления поставлена цель защищать информационные системы федерального правительства и объекты КИИ);

3) сокращение угроз, включая предотвращение и прекращение использования киберпространства в неправомерных (преступных) целях;

4) минимизация последствий — эффективное реагирование на инциденты;

---

[19] U.S. accuses China of violating bilateral anti-hacking deal // Reuters. 09.11.2018. Available at: https://www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE02E (accessed: 25.05.2019).

[20] DHS Cybersecurity Strategy // Department of Homeland Security. 17.05.2018. Available at: https://www.dhs.gov/publication/dhs-cybersecurity-strategy (accessed: 24.04.2019).

5) повышение общего уровня кибербезопасности путем управления рисками и грамотных действий со стороны Министерства.

Не последнее место в документе занимают вопросы финансирования и международного сотрудничества. Авторы Стратегии считают, что для реализации государственных задач в сфере кибербезопасности необходимо активное взаимодействие государств. На протяжении последних 20 лет основной международной площадкой для обсуждения вопросов в этой сфере выступала ООН. На фоне громких расследований предполагаемого вмешательства России во внутренние дела США с помощью ИКТ эта проблематика отошла на второй план, однако осенью 2018 г. Вашингтон вновь выдвинул вопрос международного сотрудничества на повестку дня, предложив собственную резолюцию о Продвижении ответственного поведения государств в киберпространстве в контексте международной безопасности[21].

Кроме того, в рассматриваемой Стратегии отмечается, что обеспечение кибербезопасности не должно быть самоцелью: минимизация рисков в этой сфере приводит к стимулированию международной торговли, укреплению безопасности и поощрению свободы слова и инноваций. Разработавшее документ Министерство внутренней безопасности продвигает прагматичный подход: результаты приложенных усилий должны быть пропорциональны затраченным ресурсам[22].

В сентябре 2018 г. была опубликована Национальная киберстратегия США[23], подготовленная администрацией Д. Трампа. Ключевая угроза, выделенная в документе, — угроза свободе и демократии в США. К источникам рисков авторы стратегии отнесли Россию, КНР, Иран, Северную Корею и международный терроризм. Подборка аргументов носит уже привычный характер: в адрес Москвы и Пекина регулярно звучат обвинения в кибератаках, Китай выступает в качестве основного конкурента США на международной арене, а Иран и международный терроризм

---

[21] Advancing responsible State behaviour in cyberspace in the context of international security // United Nations General Assembly. Available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266 (accessed: 20.04.2019).

[22] DHS Cybersecurity Strategy // Department of Homeland Security. 17.05.2018. Available at: https://www.dhs.gov/publication/dhs-cybersecurity-strategy (accessed: 24.04.2019).

[23] National Cyber Strategy of the United States of America // The White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed: 17.04.2019).

уже несколько лет отнесены к рангу официальных угроз[24]. Документ предлагает объединять политические и технократические действия, поддерживать распространение влияния США в мире и содействовать процветанию страны.

Согласно новой стратегии ключевая задача состоит в повышении надежности и устойчивости информационных систем. Под последней в документах Министерства внутренней безопасности США подразумеваются постоянная готовность к неблагоприятным событиям, способность реагировать на них и возвращаться к штатному режиму работы в кратчайшие сроки[25]. Кроме того, устойчивость базируется на четырех основных принципах: быстрая адаптация к чрезвычайной ситуации; качественная подготовка к ней и ее прогнозирование; поддержание работы объекта без потери функционала; полное восстановление мощностей в кратчайшие сроки.

Для реализации данной задачи американские власти в том числе планируют пересмотреть список компаний, поставляющих программное обеспечение государственным учреждениям страны. После нашумевшей истории с запретом на закупки продукции «Лаборатории Касперского»[26] для государственных нужд под официальное давление попали китайские компании. Ситуация с ними лишь продолжает набирать обороты. В мае 2019 г. Д. Трамп подписал президентский указ «Об обеспечении безопасности ИКТ и цепочки поставок сервисов»[27], направленный против китайской компании-гиганта «Huawei». Этот шаг стал закономерным продолжением нового витка торговой войны, развернувшегося в начале 2019 г.

---

[24] См., например: National Security Strategy of the United States of America, December 2017 // The White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed: 14.04.2019).

[25] Cyber Resilience and Response. 2018 Public-Private Analytic Exchange Program // Department of Homeland Security, Office of the Director of National Intelligence. Available at: https://www.dni.gov/files/PE/Documents/2018_Cyber-Resilience.pdf (accessed: 14.04.2019).

[26] Trump signs into law U.S. government ban on Kaspersky Lab software // Reuters. 13.12.2017. Available at: https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4 (accessed: 16.04.2019).

[27] Executive Order on Securing the Information and Communications Technology and Services Supply Chain // The White House. Available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (accessed: 16.05.2019).

Интересно, что новая стратегия администрации Д. Трампа дает больше полномочий правоохранительным органам в том, что касается доступа к информации, необходимой для следствия. Похожие положения содержатся в российском законодательстве и в свое время получили ряд негативных откликов в общественно-политических и отраслевых СМИ[28]. Можно предположить, что с распространением и учащением кейсов компьютерных преступлений различного рода[29] всё больше государств будут прибегать к подобным законодательным инициативам.

В этой связи обращает на себя внимание так называемый CLOUD Act[30], разрешающий американским правоохранительным органам получать доступ к серверам американских компаний, расположенных за пределами США, без уведомления властей государства и получения от них официального разрешения. Из текста закона следует, что правоохранительные органы других стран также смогут получать доступ к информации, размещенной на американских серверах, отправив запрос непосредственно в компанию (в обход стандартной процедуры политического запроса и действий в рамках договоров о взаимной правовой помощи). Важно, что при этом речь идет исключительно о данных, предоставленных посредством электронной коммуникации или размещенных на облачных сервисах. Другие виды персональной или корпоративной информации этот закон не охватывает.

Государства, высказавшие желание пользоваться CLOUD Act, должны будут заключить соответствующее дополнительное соглашение с США. В тексте закона указано, что подобные документы не будут подписываться с государствами, не уважающими базовые права человека. Для заключения дополнительных соглашений министру юстиции и государственному секретарю США придется убедить Конгресс в том, что вторая сторона принимает надлежащие меры по обеспечению безопасности и защите прав человека.

---

[28] Why Russia's anti-terrorism laws are controversial // The Economist. 20.07.2016. Available at: https://www.economist.com/the-economist-explains/2016/07/20/why-russias-anti-terrorism-laws-are-controversial (accessed: 19.04.2019).

[29] По данным «Ростелекома», в 2018 г. в России было зафиксировано на 89% больше кибератак, чем по итогам 2017 г. / Количество кибератак в России удвоилось // Ведомости. 17.04.2019. Доступ: https://www.vedomosti.ru/technology/articles/2019/04/17/799417-kolichestvo-kiberatak (дата обращения: 19.04.2019).

[30] CLOUD Act // The Congress of the United States of America. Available at: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text (accessed: 15.04.2019).

Заместитель министра юстиции США Р. Даунинг назвал этот закон моделью для международного сотрудничества, стоящей выше двусторонних договоров о правовой взаимопомощи[31]. Он также указал, что цель закона — сформировать сообщество уважающих права друг друга государств-единомышленников, действующих на основе верховенства закона. По мнению министра, использование CLOUD Act приведет к сокращению количества конфликтных точек в законодательствах государств. Принятие этого закона призвано способствовать защите данных граждан, но на текущий момент отсутствует ясность, как документ будет реализован.

Наконец, при анализе попыток США обезопасить страну и граждан от киберугроз следует отдельно рассмотреть вопрос защиты объектов КИИ, от которых зависят как безопасность страны, так и функционирование экономики.

* * *

По мнению Ч. Барри из Института национальной стратегии Университета национальной обороны США, до сих пор не было сформулировано единого определения объекта КИИ[32]. В официальных документах США говорится, что к ним относятся те важнейшие физические или виртуальные системы либо активы, разрушение или ограничение дееспособности которых приведет к ослаблению уровня безопасности страны и национальной экономики, негативно отразится на здоровье и защищенности граждан[33].

В 2013 г. Министерство внутренней безопасности США подготовило План защиты государственной инфраструктуры[34],

---

[31] Johnson D.B. The CLOUD Act, one year on // The Business of Federal Technology. Available at: https://fcw.com/articles/2019/04/08/cloud-act-turns-one.aspx (accessed: 20.04.2019).

[32] Потенциал использования ИКТ в военно-политических целях в контексте стратегической стабильности: Семинар — круглый стол № 2. Чарльз Барри // Приложение к журналу «Международная жизнь». XI Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Доступ: https://interaffairs.ru/virtualread/ikt/files/assets/downloads/publication.pdf (дата обращения: 20.04.2019).

[33] Впервые было использовано в USA PATRIOT Act, 2001. H.R.3162 — Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 // The Congress of the United States of America. Available at: https://www.congress.gov/bill/107th-congress/house-bill/3162/text/enr (accessed: 01.05.2019).

[34] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience // Department of Homeland Security. Available

часть которого посвящена объектам КИИ. Другим значимым документом в этом направлении стал Указ президента США Б. Обамы № 13636 «Укрепление кибербезопасности критической инфраструктуры», подписанный в феврале 2013 г.[35] Документ призывает к тесному сотрудничеству владельцев и операторов объектов КИИ для обеспечения наиболее адекватных подходов к защите и методов реагирования, выстроенных исходя из имеющихся рисков. По мнению Б. Обамы, федеральное правительство США должно быть активно вовлечено в процесс обмена информацией в том, что касается киберугроз, и поощрять инициативы, связанные с оперативным восстановлением работы после киберинцидентов. План защиты государственной инфраструктуры полностью поддерживает заданную линию. В свою очередь в Национальной киберстратегии США (2018) уделено особое внимание защите транспортной и морской инфраструктуры и операциям в космосе, что стало важным дополнением к классическому списку объектов критического значения[36].

Впрочем, по некоторым данным, уровень их защиты не повысился с момента подписания Д. Трампом соответствующего указа в мае 2017 г.[37] Согласно этому документу правительственные органы должны использовать все рычаги для обеспечения защиты, однако даже процесс определения критических функций, запущенный Министерством внутренней безопасности США, по-прежнему находится на начальных этапах[38]. Кроме

---

at: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience (accessed: 15.05.2019).

[35] National Archives and Records Administration. Executive Order 13636 — Improving Critical Infrastructure Cybersecurity // Federal Register. Available at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed: 25.05.2019).

[36] National Cyber Strategy of the United States of America // The White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed: 25.05.2019).

[37] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure // The White House. Available at: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (accessed: 27.05.2019).

[38] Marks J. The Cybersecurity 202: Trump's efforts failed to make critical infrastructure safer from cyberattacks, experts say // The Washington Post. 05.05.2019. Available at: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/05/the-cybersecurity-202-trump-s-efforts-failed-to-make-critical-infrastructure-safer-from-cyberattacks-experts-say/5c7d6c5b1b326b2d177d5fbd/?noredirect=on&utm_term=.b74f21316b02 (accessed: 27.05.2019).

того, возможности атакующих развиваются гораздо быстрее, чем повышается уровень защищенности объектов.

В ноябре 2018 г. был принят подготовленный Министерством внутренней безопасности США «Закон об Агентстве кибербезопасности и безопасности объектов инфраструктуры» № 115-218[39]. Согласно этому документу Директорат национальной защиты и кибербезопасности Министерства внутренней безопасности США переформируется в Агентство по кибербезопасности и безопасности инфраструктуры. Функционал нового ведомства не изменился: в сферу его ответственности вошли вопросы, связанные с обеспечением общей и кибербезопасности объектов КИИ, а также федеральные программы в этой сфере. Но важно отметить, что сформированное агентство вышло из-под контроля Министерства, став самостоятельным исполнительным органом.

Наконец, в 2018 г. был создан Национальный центр управления рисками, в цели которого входит защита от атак объектов КИИ, включая банковские системы и электросети.

Впрочем, недавние оценки деятельности Министерства внутренней безопасности в данной области носят достаточно критический характер. В частности, отмечается, что ведомство не прикладывает должных усилий к обеспечению защиты оборудования для голосования[40]. Указывается, что среди причин такого положения дел — недостаток кадров в Агентстве по кибербезопасности и безопасности инфраструктуры.

Более конкретные меры были приняты Д. Трампом в марте 2019 г. Президент обязал федеральные органы власти определить формат реагирования на угрозы для КИИ, исходящие от электромагнитных импульсов, интенсивных звуковых волн, спровоцированных в том числе кибератаками. Широкомасштабный электромагнитный импульс может нанести серьезный вред экономике, приостановить работу теплоэлектростанций, транспортной инфраструктуры и т.д., а также грозит крупными людскими потерями[41]. Министерство внутренней безопасности

---

[39] H.R.3359 — Cybersecurity and Infrastructure Security Agency Act of 2018 // The Congress of the United States of America. Available at: https://www.congress.gov/bill/115th-congress/house-bill/3359 (accessed: 27.05.2019).

[40] Progress made, but additional efforts are needed to secure the election infrastructure // Department of Homeland Security. 28.02.2019. Available at: https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf (accessed: 25.05.2019).

[41] President Trump signs EMP order to protect critical infrastructure // The Heartland Institute. Available at: https://www.heartland.org/news-opinion/news/president-trump-signs-emp-order-to-protect-critical-infrastructure (accessed: 27.05.2019).

США должно разработать список национальных критически важных систем и в течение года определить уязвимые объекты.

Прямую связь с защитой КИИ имеет подписанный президентом указ о состоянии чрезвычайного экономического положения и запрете использования технологий и сервисов зарубежных противников, ставящих государственную безопасность США под угрозу[42]. Речь идет о китайском оборудовании, которое несет в себе риски шпионажа на объектах интернет- и телекоммуникационной инфраструктуры[43]. Данный шаг действительно подчеркивает решимость президента прикладывать максимум усилий к защите объектов КИИ, но в то же время лежит в русле агрессивной риторики, характерной для китайско-американского противостояния, в том числе в киберсфере, о чем говорилось ранее в статье.

В последние годы одной из наиболее распространенных форм борьбы США с киберпреступлениями, направленными против объектов КИИ, и реакции на действия других государств в киберсфере стали санкции. Как правило, они также носят реактивный характер и преследуют цель «наказать» ту или иную страну за уже осуществленные ею действия. Согласно принятому в феврале 2019 г. закону «О защите американской безопасности от агрессии Кремля» (DASKAA)[44] в Государственном департаменте создается отдел по политике поведения в киберпространстве и цифровой экономике. Он специализируется на поддержании международной кибербезопасности, борьбе с киберпреступностью и обеспечении доступа к интернету. Глава отдела должен выступать лидирующим звеном в борьбе с использованием террористами киберинструментов, давать рекомендации госсекретарю, совместно с другими ведомствами реагировать на киберинциденты общенационального масштаба, заниматься анализом киберугроз. Кроме того, американские дипломаты также должны быть вовлечены в процесс укрепления кибербезопасности.

---

[42] Executive Order on Securing the Information and Communications Technology and Services Supply Chain // The White House. Available at: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (accessed 27.05.2019).

[43] Huawei hits back over Trump's national emergency on telecoms 'threat' // The Guardian. Available at: https://www.theguardian.com/us-news/2019/may/15/donald-trump-national-emergency-telecoms-threats-huawei (accessed 27.05.2019).

[44] Defending American Security from Kremlin Aggression Act of 2019 // The Congress of the United States of America. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/482 (accessed 02.06.2019).

В законе указано, что отдел должен сотрудничать с другими подразделениями Госдепартамента в противостоянии действиям, осуществляемым Россией или от лица России и нацеленными на подрыв кибербезопасности США или демократии государства.

Закон охватывает в том числе вопрос борьбы с киберпреступлениями международного характера. Заведомое причинение или попытки причинения вреда компьютеру, связанному с объектами КИИ, признается противозаконным, если оно приводит к нарушению работы этого компьютера или объекта. Лица, виновные в такого рода преступлениях, должны заплатить штраф и отбыть тюремное наказание сроком до 20 лет. Условное наказание за атаки на объекты КИИ не предусмотрено.

Важно отметить, что в вопросе реагирования на киберинциденты любой ответ государства или компании носит асимметричный характер. Маловероятно, что введение санкций в качестве наказания станет эффективной мерой воздействия. Кроме того, подобная реакция должна быть обоснована результатами технического расследования произошедших инцидентов. На данном этапе санкционная политика сводится к внедрению все новых ограничений и созданию дополнительных контролирующих институтов власти, что не гарантирует снижения рисков атак и киберпреступлений в будущем.

* * *

За два десятилетия проблематика кибербезопасности и огромная сфера деятельности, которая за ней кроется, превратились в одну из важнейших составляющих современной государственной и межгосударственной политики. Начав разработку политики обеспечения кибербезопасности на заре XXI в., правительство США приняло десятки документов, регулирующих работу в киберпространстве. Несмотря на активную политическую позицию по этому вопросу, США не удалось и, можно предполагать, не удастся полностью обезопасить себя от киберрисков, количество и комплексность которых растут день ото дня. В то же время можно выделить несколько отличительных особенностей, характеризующих эволюцию официальных подходов трех американских администраций как к проблемам обеспечения национальной кибербезопасности и защиты критической информационной инфраструктуры, так и к взаимодействию с другими акторами в этой сфере.

В целом предпринимаемые США шаги в области кибербезопасности носят скорее реактивный характер, отражая их ответ, иногда запоздалый, как на действия других государств, так и на глобальные вызовы. К числу последних следует отнести, в частности, то обстоятельство, что в связи с повсеместным распространением интернета стали всё больше размываться границы внутри- и внешнеполитических проблем и угроз. Кроме того, постоянно растут угрозы политически мотивированных атак на объекты КИИ.

При этом подходы американских властей к политике в сфере кибербезопасности характеризуются значительной оппортунистичностью, в большей степени зависят от текущей внешнеполитической ситуации, нежели отражают осознанное и последовательно эволюционирующее понимание путей решения этой насущной проблемы. Во многом по этой причине в настоящий момент затруднительно оценить эффективность более двух десятков законодательных инициатив, принятых двумя последними администрациями.

Наконец, можно отметить еще одну тенденцию: проблематика кибербезопасности зачастую рассматривается руководством США не как самостоятельное направление деятельности, а как средство решения более широких внешнеполитических задач, возможность оказания давления на других акторов с целью изменить поведение последних. В этой связи, в частности, обращает на себя внимание тот факт, что необходимость защиты объектов КИИ и, шире, поддержания национальной безопасности в киберсфере используется в качестве аргумента и повода для введения новых санкций в отношении других государств и их компаний.

СПИСОК ЛИТЕРАТУРЫ

1. Гаврилова М.С., Демидов О.В., Козик А.Л., Стрельцов А.А. Применение международного права в киберпространстве // Индекс безопасности. 2015. Т. 21. № 4. С. 99–116.

2. Зиновьева Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО-Университета. 2016. № 4 (49). С. 235–247.

3. Карасев П.А. Стратегия информационной (кибер)безопасности США в XXI веке // Вестник Московского университета. Серия 12. Политические науки. 2013. № 2. С. 89–102.

4. Материалы Седьмой научной конференции Международного исследовательского консорциума информационной безопасности. М., 2013. Доступ: http://www.iisi.msu.ru/UserFiles/File/publications/VII%20Forum.pdf (дата обращения: 02.02.2019).

5. Научные и методологические проблемы информационной безопасности: Сборник статей / Под ред. В.П. Шерстюка. М.: МЦНМО, 2004.

6. Ромашкина Н.П. Информационная безопасность как часть проблемы обеспечения стратегической стабильности // Стратегическая стабильность. 2018. № 1 (82). С. 8–13.

7. Ромашкина Н.П. Проблемы международной информационной безопасности: компромисс между Россией и Западом? // Европейская безопасность: события, оценки, прогнозы. 2016. Вып. 41 (57). С. 9–12.

8. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: Парад, 2005.

9. Стрельцов А.А., Смирнов А.И. Российско-американские отношения в области международной информационной безопасности: приоритетные направления сотрудничества // Международная жизнь. 2017. № 11. С. 71–81.

10. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. М.: Весь мир, 2015.

11. Ani U.D., Daniel N., Oladipo F., Adewumi S.E. Securing industrial control system environments: The missing piece // Journal of Cyber Security Technology. 2018. Vol. 2. No. 3–4. P. 131–163. DOI: 10.1080/23742917.2018.1554985.

12. Ani U.P.D., He H., Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective // Journal of Cyber Security Technology. 2017. Vol. 1. No. 1. P. 32–74. DOI: 10.1080/23742917.2016.1252211.

13. Clark-Ginsberg A., Slayton R. Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards // Science and Public Policy. 2019. Vol. 46. Iss. 3. P. 339–346. DOI: 10.1093/scipol/scy061.

14. Endeley R. End-to-end encryption in messaging services and national security — case of WhatsApp messenger // Journal of Information Security. 2018. Vol. 9. No. 1. P. 95–99. DOI: 10.4236/jis.2018.91008.

15. Katzan H. Contemporary issues in cybersecurity // Journal of Cybersecurity Research (JCR). 2016. Vol. 1. No. 1. P. 1–6. DOI: 10.19030/jcr.v1i1.9745.

16. Pavlik K. Cybercrime, hacking, and legislation // Journal of Cybersecurity Research (JCR). 2017. Vol. 2. No. 1. P. 13–16. DOI: 10.19030/jcr.v2i1.9966.

17. Quigley K., Roy J. Cyber-security and risk management in an interoperable world: An examination of governmental action in North America // Social Science Computer Review. 2012. Vol. 30. No. 1. P. 83–94. DOI: 10.1177/0894439310392197.

18. Riek M., Böhme M. The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates // Journal of Cybersecurity. 2018. Vol. 4. Iss. 1. DOI: 10.1093/cybsec/tyy004.

19. Romanosky S. Examining the costs and causes of cyber incidents // Journal of Cybersecurity. 2016. Vol. 2. No. 2. P. 121–135. DOI: 10.1093/cybsec/tyw001.

20. Romanosky S., Ablon L., Kuehn A., Jones T. Content analysis of cyber insurance policies: How do carriers price cyber risk? // Journal of Cybersecurity. 2019. Vol. 5. Iss. 1. DOI: 10.1093/cybsec/tyz002.

M.V. Smekalova

EVOLUTION OF U.S. POLICY APPROACHES TO ENSURING CYBERSECURITY AND DEFENSE OF CRITICAL INFORMATION INFRASTRUCTER

Institute for the US and Canadian Studies, Russian Academy of Sciences
2/3 Khlebnyi pereulok, Moscow, 123995

Rapid development of the Internet technologies has brought both unprecedented opportunities for economic development and a number of dangers for international community. In the early 2000s, challenges and threats emanating from the cyberspace were prioritized by leading world powers. The United States were among the first to elaborate legal framework for cyberpolicy aiming at providing national security after terrorist attacks of 2001. As time passed, dozens of legislation acts were adopted, and a number of agencies and committees responsible for ensuring information security emerged. The article examines the evolution of the U.S. conceptual approaches to information security (cybersecurity of the U.S. official documents) during the presidency of George Bush Jr. (during his tenure in office, the first National Strategy to Secure Cyberspace was accepted), Barack Obama and Donald Trump. The author traces priority changes that took place in this area as well as analyzes U.S. relationships with other major actors in the cybersphere, especially Russia and China. A particular attention is paid to the U.S. policy directed at ensuring security of critical information infrastructures (CII). The author emphasizes that, although a set of regulating document has been adopted, the security level of CII objects remains relatively low. In general, the analysis of national policy documents allowed the author to outline several tendencies, characterizing development of the U.S. policy in cybersphere in recent years. In particular, there is an increasing tendency towards unilateralism relating to the sanctions measures against particular countries and their companies. In this context, the cybersecurity issues are often considered not as an end in itself but as means of achieving wider goals of external and internal policy. The author concludes that the U.S. cybersecurity policy is reactive in nature, which directly affects its effectiveness.

Keywords: the United States of America, the U.S., information security, cybersecurity, cyberthreats, cyberstrategy, critical information infrastructure (CII), sanctions.

About the author: *Maria V. Smekalova* — PhD Candidate at the Institute for the US and Canadian Studies, Russian Academy of Sciences (e-mail: mashasmekalova@gmail.com).

REFERENCES

1. Gavrilova M.S., Demidov O.V., Kozik A.L., Strel'tsov A.A. 2015. Primenenie mezhdunarodnogo prava v kiberprostranstve [The application of international law in cyberspace]. *Indeks bezopasnosti*, vol. 21, no. 4, pp. 99–116. (In Russ.)

2. Zinov'eva E.S. 2016. Perspektivnye tendentsii formirovaniya mezhdunarodnogo rezhima po obespecheniyu informatsionnoi bezopasnosti [Emerging trends in development of international information security regime]. *MGIMO Review of International Relations*, no. 4 (49), pp. 235–247. (In Russ.)

3. Karasev P.A. 2013. Strategiya informatsionnoi (kiber)bezopasnosti SShA v XXI veke [The strategy of U.S. information (cyber)security in the 21st century]. *Moscow University Bulletin. Series 12. Political Science*, no. 2, pp. 89–102. (In Russ.)

4. *Materialy Sed'moi nauchnoi konferentsii Mezhdunarodnogo issledovatel'skogo konsortsiuma informatsionnoi bezopasnosti* [Proceedings of the Seventh Scientific Conference of the International Information Security Research Consortium]. 2013. Moscow. Available at: http://www.iisi.msu.ru/UserFiles/File/publications/VII%20Forum.pdf (accessed: 02.02.2019). (In Russ.)

5. Sherstyuk V.P. (ed.). 2004. *Nauchnye i metodologicheskie problemy informatsionnoi bezopasnosti* [Scientific and methodological issues of information security]. Moscow, MTsNMO Publ. (In Russ.)

6. Romashkina N.P. 2018. Informatsionnaya bezopasnost' kak chast' problemy obespecheniya strategicheskoi stabil'nosti [Information security as a part of strategical stability maintenance problem]. *Strategicheskaya stabil'nost'*, no. 1 (82), pp. 8–13. (In Russ.)

7. Romashkina N.P. 2016. Problemy mezhdunarodnoi informatsionnoi bezopasnosti: kompromiss mezhdu Rossiei i Zapadom? [Issues of international information security: A compromise between Russia and the West?]. *Evropeiskaya bezopasnost': sobytiya, otsenki, prognozy*, iss. 41 (57), pp. 9–12. (In Russ.)

8. Smirnov A.I. 2005. *Informatsionnaya globalizaciya i Rossiya: vyzovy i vozmozhnosti* [Globalization of information and Russia: Challenges and opportunities]. Moscow, Parad Publ. (In Russ.)

9. Strel'tsov A.A., Smirnov A.I. 2017. Rossiisko-amerikanskie otnosheniya v oblasti mezhdunarodnoi informatsionnoi bezopasnosti: prioritetnye napravleniya sotrudnichestva [U.S.-Russian relations in the field of international information security: Priority areas of cooperation]. *International affairs*, no. 11, pp. 71–81. (In Russ.)

10. Sharikov P.A. 2015. *Problemy informatsionnoi bezopasnosti v politsentrichnom mire* [Issues of information security in a polycentric world]. Moscow, Ves' mir Publ. (In Russ.)

11. Ani U.D., Daniel N., Oladipo F., Adewumi S.E. 2018. Securing industrial control system environments: The missing piece. *Journal of Cyber Security Technology*, vol. 2, no. 3-4, pp. 131–163. DOI: 10.1080/23742917.2018.1554985.

12. Ani U.P.D., He H., Tiwari A. 2017. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 32–74. DOI: 10.1080/23742917.2016.1252211.

13. Clark-Ginsberg A., Slayton R. 2019. Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, vol. 46, iss. 3, pp. 339–346. DOI: 10.1093/scipol/scy061.

14. Endeley R. 2018. End-to-end encryption in messaging services and national security — case of WhatsApp messenger. *Journal of Information Security*, vol. 9, no. 1, pp. 95–99. DOI: 10.4236/jis.2018.91008.

15. Katzan H. 2016. Contemporary issues in cybersecurity. *Journal of Cybersecurity Research (JCR)*, vol. 1, no. 1, pp. 1–6. DOI: 10.19030/jcr.v1i1.9745.

16. Pavlik K. 2017. Cybercrime, hacking, and legislation. *Journal of Cybersecurity Research (JCR)*, vol. 2. no. 1, pp. 13–16. DOI: 10.19030/jcr.v2i1.9966.

17. Quigley K., Roy J. 2012. Cyber-security and risk management in an interoperable world: An examination of governmental action in North America. *Social Science Computer Review*, vol. 30, no. 1, pp. 83–94. DOI: 10.1177/0894439310392197.

18. Riek M., Böhme M. 2018. The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, vol. 4, iss. 1. DOI: 10.1093/cybsec/tyy004.

19. Romanosky S. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135. DOI: 10.1093/cybsec/tyw001.

20. Romanosky S., Ablon L., Kuehn A., Jones T. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, vol. 5, iss. 1. DOI: 10.1093/cybsec/tyz002.