ЧАЛДАЕВА Лариса Алексеевна – *доктор экономических наук, профессор; профессор кафедры экономики организации Финансового университета при Правительстве РФ (125993, Россия, г. Москва, ГСП-3, Ленинградский пр-кт, 49; Chaldaeva45@mail.ru)*

КИЛЯЧКОВ Анатолий Анатольевич – *кандидат технических наук, старший научный сотрудник; эксперт Центра исследования проблем безопасности РАН (119334, Россия, г. Москва, ул. Гарибальди, 21-б; AAKil@mail.ru)*

ЯКОРЕВ Анатолий Александрович – *директор Института международного сотрудничества, комплаенса и защиты бизнеса (123007, Россия, г. Москва, 2-й Хорошевский пр-д, 9, корп. 1); заместитель председателя по международному сотрудничеству МОО «Национальный комитет общественного контроля» (cybericle@mail.ru)*

К ВОПРОСУ О ФОРМИРОВАНИИ ГОСУДАРСТВЕННЫХ ФУНКЦИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ РОССИИ

Аннотация. *В работе рассмотрены признаки формирования государственных функций РФ по обеспечению безопасности в киберпространстве. Вопросами защиты государственных интересов занимаются все госструктуры, а также специально созданные для этого институты. В кредитно-финансовой сфере вопросами кибербезопасности занимается департамент Банка России. Остальной корпоративный сегмент обеспечивает свою кибербезопасность самостоятельно, так же как и население России. Переход программно-аппаратного обеспечения на отечественные разработки происходит неравномерно с серьезным отставанием аппаратного сегмента.*

Ключевые слова: *цифровое пространство, формирование виртуального государства, обеспечение безопасности населения и государства, формирование функций государства в киберпространстве*

Наряду с выполнением экономико-организационных функций, формирование которых в виртуальном пространстве РФ было рассмотрено в предыдущей статье [Чалдаева, Килячков, Якорев 2020], государство выполняет функции по охране общественного порядка, а также по обеспечению безопасности населения и собственной безопасности как института политической системы общества[1]. В настоящей работе будут рассмотрены признаки формирования у Российской Федерации этих государственных функций в киберпространстве. Необходимость изучения данного процесса адекватно оценивается высшим руководством страны. Так, премьер-министр России М.В. Мишустин, выступая в конце января на форуме *Digital Almaty* в Казахстане, сказал, что происходящая в мире цифровая трансформация требует переосмысления роли государства и органов власти[2].

Внутренняя функция государства по обеспечению безопасности и охране общественного порядка предполагает защиту прав и законных интересов граждан, юридических лиц и государства. При рассмотрении признаков формирования государственных функций в виртуальном пространстве необходимо ответить на следующие вопросы: 1) что является объектом охраны в цифровом пространстве; 2) какой государственный институт выполняет эти функции и 3) как эти функции осуществляются.

---

[1] Автономов А. С., Попов В. А. 2007. Государство. – *Большая российская энциклопедия*. Т. 7. М. С. 542. Доступ: https://bigenc.ru/ethnology/text/2373590 (проверено 24.05.2020).

[2] Едовина Т. 2020. Деньги на цифру. Куда ведет цифровая трансформация в России. – *Деньги*. Приложение № 1. 13 февраля 2020. С. 14. Доступ: https://www.kommersant.ru/doc/4243128 (проверено 24.05.2020).

Объект охраны в цифровом пространстве. Очевидно, что в цифровом пространстве основной ценностью является информация. Актуальность данного вопроса получила неожиданную и мощную поддержку в результате пандемии коронавируса, противоэпидемическая защита от которого потребовала тотального перехода сотрудников компаний к работе с удаленных рабочих мест.

Для граждан несанкционированный доступ к персональному компьютеру, электронной переписке[1] или кража информации влечет за собой в лучшем случае назойливую таргетированную рекламу[2] или несанкционированное использование вычислительных ресурсов[3]. Возможны существенно более негативные варианты последствий кибератак, когда похищенные данные используются для вымогательства[4], присвоения финансовых средств[5], компрометации личности[6] или шпионажа. В 2019 г. выяснилось, что популярный мессенджер *WhatsApp* является одним из наиболее опасных приложений[7]. Неизвестные лица заражали телефон жертвы, используя уязвимость этого приложения, просто позвонив ему на телефон. После этого злоумышленники могли получить от телефона зашифрованные данные, изображение на экране, личные сообщения, местоположение и т.п. Кроме того, преступники могли включить на телефоне камеру или микрофон. Следует отметить, что значительная часть выявленных жертв этого мошенничества являлись высокопоставленными государственными чиновниками и военачальниками различных государств[8].

Для юридических лиц кража информации сопряжена с финансовыми и имиджевыми потерями, хищениями коммерческой информации, промышленным кибершпионажем и т.д. Так, по результатам исследований[9], проведенных в 2019 г., в 59% опрошенных российских компаний происходила утечка данных. Причем чаще всего похищалась коммерческая (35%), техническая (25%) и финансовая (19%) информация, а также персональные данные (23%). Причем 63% опрошенных компаний скрыли инцидент, 27% сообщили о нем пострадавшим и принесли извинения, 15% сообщили регулятору, но ни одна компания не сделала официального заявления в СМИ. В качестве вопиющего примера подобной утечки можно привести продажу в начале 2020 г. базы данных обо

---

1 Joseph Cox. How Big Companies Spy on Your Emails. Motherboard. – *VICE*. 10.02.2020. URL: https://www.vice.com/en_us/article/pkekmb/free-email-apps-spying-on-you-edison-slice-cleanfox (accessed 24.05.2020).

2 Перкалин А. Самые распространенные мобильные угрозы в 2019 году. – *Лаборатория Касперского*. 25.02.2020. Доступ: https://www.kaspersky.ru/blog/mobile-virusology-2019/26401/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest (проверено 24.05.2020).

3 Булавас В., Лопатин Е. Майнеры на подъеме. – *SL SecureList. Лаборатория Касперского*. 04.09.2017. Доступ: https://securelist.ru/miners-on-the-rise/80257/ (проверено 04.04.2020).

4 Mamedov O., Sinitsyn F., Ivanov A. Bad Rabbit ransomware. – *SL SecureList. Лаборатория Касперского*. 24.10.2017. Доступ: https://securelist.com/bad-rabbit-ransomware/82851/ (проверено 24.05.2020).

5 Дементьева К. ЦБ придаст переводам обратную силу. – *Коммерсантъ*. № 31. 20.02.2020. С. 7. Доступ: https://www.kommersant.ru/doc/4260923?utm_source=newspaper&utm_medium=email&utm_campaign=newsletter (accessed 24.05.2020).

6 Secret Sharing app Whisper Left Users' Locations Fetishes Exposed on the Web. – *Washington Post*. 10.03.2020. URL: https://www.washingtonpost.com/technology/2020/03/10/secret-sharing-app-whisper-left-users-locations-fetishes-exposed-web/ (accessed 31.03.2020).

7 Кадочникова С. Звонит по тебе. – *Информационный канал Subscribe.Ru*. 27.11.2019. Доступ: https://subscribe.ru/digest/inet/protection/n260382991.html?utm_source=subscribe-newsletters&utm_medium=email&utm_campaign=subscribe-newsletters (проверено 04.04.2020).

8 Bing C., Satter R. Exclusive: Government officials around the globe targeted for hacking through WhatsApp-sources. – *Reuters*. 31.10.2019. Доступ: https://www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup/exclusive-whatsapp-hacked-to-spy-on-top-government-officials-at-u-s-allies-sources-idUSKBN1XA27H (accessed 04.04.2020).

9 Исследование уровня информационной безопасности в компаниях России и СНГ за 2019 год. – *СерчИнформ*. Доступ: https://searchinform.ru//research-2019/ (проверено 24.05.2020).

всех экспортно-импортных операциях российских компаний за 2012–2019 гг. Она содержала полные декларации всех участников внешнеэкономической деятельности России с указанием ИНН, информации о товарах и страны их происхождения, номеров транспортных средств и персональных данных представителей компаний – физических лиц[1].

В масштабах государства кража информации, искажение управленческих решений и другие кибератаки сопряжены с большими экономическим и имиджевыми потерями, снижением обороноспособности, снижением устойчивости работы телекоммуникационных сетей, нарушением внутренней стабильности и гражданского мира, дискредитацией политических деятелей и государственных чиновников[2] и т.п. Министр иностранных дел РФ Сергей Лавров, выступая осенью 2019 г. перед студентами и профессорско-преподавательским составом МГИМО и Дипломатической академии МИД РФ, заявил: «У нас тоже есть основания, причем более солидные, подозревать, что западные коллеги проявляют повышенное внимание к нашим интернет-ресурсам... И это не раз проявляется. Об этом говорили и представители Центрального банка России, Сбербанка, и других государственных структур»[3]. В качестве яркого примера использования виртуального пространства в шпионских целях можно привести сообщение, появившееся в печати в начале 2020 г., что авторитетный и пользовавшийся хорошей репутацией производитель шифровального оборудования *Crypto AG* передавал американской и германской разведке секретную переписку официальных лиц из разных стран мира[4]. Другим примером использования цифрового пространства против суверенных государств являются кибератаки, совершенные в 2019 г. группировкой *Calypso,* на государственные учреждения различных стран. На Россию пришлось 12% общего числа выявленных атак, на Индию – 34%, Бразилию и Казахстан – по 18%, Таиланд – 12%, Турцию – 6%. Основной целью атаки был шпионаж[5]. Хакерские группировки различных стран, наиболее известные из которых приведены в табл. 1, зачастую работают в интересах или по заданию национальных спецслужб. Необходимо отметить, что в интернет-протоколах государственных структур РФ для защиты информации применяются отечественные алгоритмы криптозащиты, прошедшие стандартизацию ФСБ[6].

---

1 По требованию Северного транспортного прокурора суд признал информацию, размещенную в сети Интернет, запрещенной. – *Московская региональная транспортная прокуратура*. 12.03.2020. Доступ: http://www.mmtproc.ru/news/1/13308/ (проверено 04.04.2020).

2 Stanton C. How Should Countries Tackle Deepfakes? – *Carnegie Endowment for International Peace*. 28.01.2019. URL: https://carnegieendowment.org/2019/01/28/how-should-countries-tackle-deepfakes-pub-78221 (accessed 24.05.2020).

3 Лавров: Россия подозревает Запад во вмешательстве в работу сайтов российских госструктур. – *ТАСС*. 02.09.2019. Доступ: https://tass.ru/politika/6831491 (проверено 04.04.2020).

4 Miller G. The Intelligence Coup of the Century. – *The Washington Post*. 11.02.2020. URL: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ (accessed 04.04.2020).

5 Тишина Ю. Хакеры встроились в госструктуры. Атакам группировки из Азии подверглись российские организации. – Коммерсантъ. № 200. 31.10.2019. С. 1. Доступ: https://www.kommersant.ru/doc/4142712?utm_source=newspaper&utm_medium=email&utm_campaign=newsletter (проверено 04.04.2020).

6 Тишина Ю. Россвязь прозванивает «Кузнечика». Отечественную криптозащиту протестируют на виртуальных сим-картах. – Коммерсантъ. № 31. 20.02.2020. С. 1. Доступ: https://www.kommersant.ru/doc/4260869?utm_source=newspaper&utm_medium=email&utm_campaign=newsletter (проверено 04.04.2020).

Таблица 1

Краткая характеристика наиболее известных хакерских группировок

Страна локализации	Хакерские группы	Регион (страна) киберактивности				
		США и Латинская Америка	Европа	Юго-Восточная Азия	Ближний Восток и Африка	Россия
США	*Slingshot, Equation*			+	+	+
Китай	*APT15, Thrip, TEMP, Periscope, Tick, APT17, PutterPanda, APT10, PlugX, MustangPanda*	+	+	+		+
Россия	*APT28, Dragonfly, Turla, BlackEnergy*	+	+	+		+
КНДР	*Lazarus, DarkHotel, Andariel, Kimsuky, APT37*	+	+	+	+	
Иран	*Charming Kitten, Team, MuddyWater, Chafer, OilRig, APT34, APT33*	+		+	+	
Вьетнам	*APT32*			+		
Индия	*Sidewinder*			+		
Пакистан	*Gorgon Group*	+	+			
Украина	*Prikormka*					+

Источник: [Грунтов 2019: 4].

Виртуальное пространство государств может быть использовано для совершения диверсионных атак. Так, по сообщению газеты *The New York Times,* еще с 2012 г. спецслужбы США занимались глубоким внедрением вредоносного программного обеспечения на объектах российской энергетической системы. Целью подобных действий является отключение некоторых элементов энергетической системы России при возникновении серьезного конфликта[1]. Именно поэтому в феврале 2020 г. на расширенном заседании коллегии ФСБ Владимир Путин поручил ведомству расширять возможности государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак. «Сейчас в ряде стран уже созданы специальные центры для проведения таких акций, разрабатываются стратегии превентивного применения киберсредств. По мере бурного развития цифровых технологий мощность такого информационного оружия, безусловно, будет только нарастать. Нам нужно это не просто учитывать, а соответствующим образом, с опережением строить свою работу по защите интересов России», – сказал президент[2].

Таким образом, в цифровом пространстве основной ценностью является

[1] U.S. Escalates Online Attacks on Russia's Power Grid. – *The New York Times*. 15.06.2019. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html (accessed 04.04.2020).

2 Заседание коллегии ФСБ. – *Президент России. Официальный сайт*. 20.02.2020. Доступ: http://kremlin.ru/events/president/news/62834 (проверено 04.04.2020).

информация, которую необходимо не только аккумулировать, хранить и обрабатывать, но и обеспечивать ее безопасность. Причем термин «информация» следует понимать в широком смысле – не только как данные, но и как управленческие решения, информационные потоки, медиаконтент и т.п.; а безопасность информации – это не только ее защита от хищения, но и предотвращение искажений и компрометации.

Структуры, обеспечивающие безопасность киберпространства. Защита существующего политического строя и правовой системы государства включает в себя борьбу с негативным влиянием виртуального пространства на события, происходящие в реальном мире. Она включает в себя борьбу с распространением ложной и панической информации, с призывами свержения существующей политической и правовой системы. Возможность использования медийного пространства в качестве нового театра военных действий продемонстрировало Министерство обороны США, которое приступило к разработке новой стратегии боевых действий, предполагающей координацию протестного потенциала «пятой колонны» для дестабилизации общества с одновременным нанесением ударов по наиболее важным объектам страны[1]. История «цветных революций» показывает, что для этого активно используются возможности медийного цифрового пространства. Поэтому Стратегия национальной кибербезопасности Соединенных Штатов Америки формулирует требование открытого Интернета как одного из основных стандартов, обеспечивающих продвижение американского влияния в мире[2]. Эти обстоятельства заставили высшее военное руководство РФ заявить о переносе военных действий в информационную сферу[3].

Само цифровое пространство может быть не только театром военных действий, но и объектом нападения. Летом 2014 г. соответствующие ведомства во главе с Минкомсвязью провели киберучения. Целью учений было выявление угроз внешнего воздействия на Рунет и оценка вероятности потери его целостности и работоспособности (другими словами, суверенитета и территориальной целостности российского виртуального пространства). Кроме того, оценивалась защищенность отечественных ресурсов от внешних киберугроз. В результате учений была выявлена недостаточная устойчивость работы Интернета на территории РФ в случае внешнего воздействия. Таким образом, в нашей стране могла возникнуть ситуация, подобная сирийскому инциденту 2012 г., когда в результате подобного внешнего кибервоздействия была нарушена маршрутизация трафика, что на двое суток заблокировало работу Интернета на территории страны[4]. В результате принятых мер, включающих в т.ч. и выполнение требований закона «о суверенном Интернете»,[5] Россия в 2019 г. заняла 11-е

---

[1] Генштаб России объяснил суть американского «Троянского коня». – *РИА Новости*. 02.03.2019. Доступ: https://ria.ru/20190302/1551501526.html (проверено 04.04.2020).

[2] National Cyber Strategy of the United States of America. September 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed 01.04.2020).

[3] Генштаб предупредил о переносе военных действий в информационную сферу. – *РИА Новости*. 02.03.2019. Доступ: https://ria.ru/20190302/1551498511.html (проверено 04.04.2020).

[4] Анненков А. Еще к вопросу об устойчивости Рунета к неблагоприятным внешним воздействиям. – *D-russia.ru:* онлайн-издание. 16.09.2014. Доступ: http://d-russia.ru/eshhe-k-voprosu-ob-ustojchivosti-runeta-k-neblagopriyatnym-vneshnim-vozdejstviyam.html (проверено 04.04.2020); Анненков А. Игорь Щеголев: «Учения подтвердили недостаточную устойчивость Рунета при недружественных «целенаправленных действиях». – *D-russia.ru:* онлайн-издание. 17.10.2014. Доступ: http://d-russia.ru/ucheniya-podtverdili-nedostatochnuyu-ustojchivost-runeta-pri-nedruzhestvennyx-celenapravlennyx-dejstviyax.html (проверено 04.04.2020).

[5] Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"». Доступ: http://www.consultant.ru/document/cons_doc_LAW_323815/ (проверено 02.04.2020).

место (из 224) в рейтинге устойчивости национальных сегментов Интернета[1]. Для дальнейшего повышения устойчивости функционирования Рунета в 2020 г. было запланировано проведение четырех учений[2], однако в связи с эпидемией коронавируса мартовские учения были отложены[3].

Помимо Минкомсвязи и других «соответствующих ведомств», отвечающих за целостность и работоспособность информационно-коммуникационного пространства, в РФ создана система по противодействию кибератакам на информационные системы объектов, наиболее важных для функционирования государства. Ключевым объектом этой структуры является Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который отслеживает инциденты, направленные против значимых объектов критической информационной инфраструктуры[4]. НКЦКИ является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Реестр значимых объектов критической информационной инфраструктуры ведет Федеральная служба по техническому и экспортному контролю[5].

На уровне отдельных компаний и организаций вопросами киберзащиты в централизованном порядке занимается только Департамент информационной безопасности Банка России (ФинЦЕРТ), осуществляющий мониторинг и реагирование на компьютерные атаки в кредитно-финансовой сфере[6]. Компании, профессионально занимающиеся информационной безопасностью (например, *Group-IB, Positive Technologies* и *Solar JSOC*), работают с инцидентами в корпоративном сегменте на коммерческой основе. Остальные крупные российские компании самостоятельно решают возникающие перед ними проблемы информационной безопасности. Однако 70% респондентов считают, что программно-аппаратные решения, которые их компании применяют для защиты систем, устарели, и только 1/4 (26,6%) респондентов полностью уверены в их надежности[7]. При этом малые и средние предприятия чаще всего выбирают максимально простые и дешевые защитные средства, которые далеко не всегда адекватны возникающим угрозам. Но даже при наличии современных инстру-

---

[1] Интернет. – *Компания TAdviser*. 06.09.2019. Доступ: http://www.tadviser.ru/index.php/Статья:Интернет (проверено 04.04.2020).

[2] Приказ Минкомсвязи России № 839 «Об утверждении графика проведения плановых учений по обеспечению устойчивого, безопасного и целостного функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования в 2020 году». – *Министерство цифрового развития, связи и массовых коммуникаций РФ. Официальный сайт*. Доступ: https://digital.gov.ru/ru/documents/7002/ (проверено 04.04.2020).

3 Минкомсвязь отложила из-за коронавируса учения по обеспечению устойчивой работы Рунета. – *ТАСС*. 20.03.2020. Доступ: https://tass.ru/ekonomika/8032625 (проверено 04.04.2020).

[4] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Доступ: http://www.consultant.ru/document/cons_doc_LAW_220885/ (проверено 04.04.2020); приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам». Доступ: http://www.consultant.ru/document/cons_doc_LAW_306334/ (проверено 04.04.2020).

[5] Приказ Федеральной службы по техническому и экспортному контролю от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации». – *Федеральная служба по техническому и экспортному контролю*. Доступ: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1587-prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227 (проверено 30.03.2020).

[6] ФинЦЕРТ. – *Официальный сайт Банка России*. Доступ: https://cbr.ru/information_security/fincert/ (проверено 25.05.2020).

[7] Жукова К. Киберзащита не успевает обновляться. Компании опасаются устаревания решений. – *Коммерсантъ*. № 123. 16.07.2019. С. 10. Доступ: https://www.kommersant.ru/doc/4032484?utm_source=newspaper&utm_medium=email&utm_campaign=newsletter (проверено 04.04.2020).

ментов защиты в компаниях имеет место острая нехватка квалифицированного персонала[1].

Что касается населения РФ, то, к сожалению, в государстве нет инфраструктуры, которая занималась бы оперативной работой по предотвращению киберинцидентов и защите населения от них. Для исправления сложившейся ситуации Генпрокуратура России подготовила концепцию создания программно-аппаратного ресурса для сбора информации о кибермошенничестве в финансовой среде, совершенном против гражданского населения[2]. А пока граждане вынуждены сами заботиться о своей безопасности в виртуальном пространстве, используя для этого различные системы антивирусной защиты, наиболее известными из которых являются программные продукты российской компании «Лаборатория Касперского».

Справедливости ради следует отметить, что немногие страны выделяют ресурсы на защиту собственных граждан от массированного кибермошенничества. Так, согласно статистике британской полиции, жертвы киберпреступности теряют в Великобритании более 190 000 фунтов в день. Причем более 1/3 жертв в этот период стали жертвами взлома социальных сетей и почтовых ящиков[3]. Так как киберпреступления носят трансграничный характер, то должна вестись совместная работа по их пресечению. Но даже внутри Европейского союза этого не происходит. Только для того чтобы осознать, что большая часть преступлений совершается в виртуальном пространстве, британскому правительству потребовалось 10 лет[4]. Можно только предполагать, сколько времени потребуется для достижения практических результатов.

Упомянутые выше государственные структуры решают различные вопросы по защите российского киберпространства. Однако есть еще группа проблем, которые требуют системного решения. Наиболее важной из них является недостаточно широкое использование отечественного программного обеспечения и отсутствие элементной базы, произведенной в России, что влечет за собой риск программно-аппаратных закладок в информационно-коммуникационных системах. Пока эта проблема не будет решена, нельзя говорить о том, что безопасность российского виртуального пространства будет обеспечена на должном уровне. Руководство государства осознает риск того, что при обострении ситуации нам могут либо не продать, либо отключить уже приобретенное нами ранее электронно-коммуникационное оборудование. Однако практические действия по изменению сложившейся ситуации в течение длительного времени не предпринимались. Серьезной заявкой на изменение сложившегося положения стало утверждение премьер-министром РФ М.В. Мишустиным Стратегии развития электронной промышленности Российской Федерации в период до 2030 года[5], которая наметила меры по разработке и производству российской электроники. Согласно этому документу, уже на 1-м этапе (2020–2021 гг.) пла-

---

[1] Шалыто А.А. К вопросу о «цифровом ополчении. – *D-russia.ru:* онлайн-издание. 05.07.2019. Доступ: http://d-russia.ru/k-voprosu-o-tsifrovom-opolchenii.html (проверено 02.04.2020)

[2] Дементьева К. Мошенники одного окна. Информацию о киберпреступлениях соберут через портал госуслуг. – *Коммерсантъ.* № 18. 03.02.2020. С. 1. Доступ: https://www.kommersant.ru/daily/2020-02-03 (проверено 04.04.2020).

[3] Lee J. «We lost nearly £10k to TV licence scammers». – *BBC News.* 07.01.2019. URL: https://www.bbc.com/news/uk-47016671 (accessed 25.05.2020).

[4] The Guardian view on cybercrime: the law must be enforced. – *The Guardian.* 03.06.2019. URL: https://www.theguardian.com/commentisfree/2019/jun/03/the-guardian-view-on-cybercrime-the-law-must-be-enforced (accessed 09.04.2020).

[5] Стратегия развития электронной промышленности Российской Федерации на период до 2030 года. Утв. распоряжением Правительства РФ от 17.01.2020 № 20-р. Доступ: http://government.ru/docs/38795/ (проверено 29.03.2020).

нируется производить часть необходимой элементной базы для внутреннего рынка и национальных проектов, а в дальнейшем все основные компоненты будут производиться в нашей стране.

Следует отметить, что программное и аппаратное обеспечение неразрывно связаны, поэтому развитие отечественного аппаратного обеспечения должно происходить согласованно с развитием программного обеспечения. Для поддержки отечественных разработчиков программного обеспечения Минкомсвязи издало приказ, согласно которому госкомпании и госкорпорации должны использовать преимущественно отечественное программное обеспечение (ПО)[1]. В развитие этой тенденции Минпромторг России предложил при госзакупках присваивать статус отечественной только той промышленной продукции, в производстве которой применялось российское ПО[2].

Есть и другие факты, подтверждающие изменение отношения к использованию программного обеспечения, созданного российскими разработчиками. Так, на портале общественных обсуждений опубликован проект приказа Федеральной службы по техническому и экспортному контролю о внесении изменений в требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (КИИ) Российской Федерации[3]. Изменения направлены на использование в КИИ РФ преимущественно отечественного программного обеспечения и оборудования в целях гарантии ее технологической независимости и безопасности. Казначейство России объявило конкурс на закупку российской СУБД, планируя отказаться от СУБД *Oracle*[4]. Компании, входящие в группу «Ростех», начинают выпуск защищенных российских мобильных устройств для корпоративного сегмента, на которых планируется установить российские средства криптографической и антивирусной защиты, обмена сообщениями и пр.[5] В ноябре 2019 г. был принят закон, согласно которому при продаже отдельных видов технически сложных товаров (смартфоны, компьютеры и телевизоры с функцией «смарт-ТВ» и т.п.) на них должно быть установлено российское программное обеспечение[6]. Перечень подобных фактов можно продолжить.

Отметим, что сформулированная выше проблема стоит практически перед всеми странами, которые зависят от элементной базы, подавляющий объем

---

1 Приказ Минкомсвязи России от 20.09.2018 № 486 (ред. от 18.04.2019) «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения». Доступ: http://www.consultant.ru/document/cons_doc_LAW_314283/ (проверено 02.04.2020).

2 Степанова Ю., Никитина О. Российский софт запустят в производство. – *Коммерсантъ*. № 30. 19.02.2020. С. 7. Доступ: https://www.kommersant.ru/doc/4260012?utm_source=newspaper&utm_medium=email&utm_campaign=newsletter (проверено 04.04.2020).

3 Проект приказа ФСТЭК России «О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239». Доступ: https://regulation.gov.ru/projects#npa=99311 (проверено 29.03.2020).

4 Заявка № 0895100000120000026. Оказание услуг по передаче неисключительных прав на программное обеспечение для нужд Федерального казначейства. – *Единая информационная система в сфере закупок*. Доступ: https://zakupki.gov.ru/epz/order/notice/ea44/view/documents.html?regNumber=0895100000120000026 (проверено 04.04.2020).

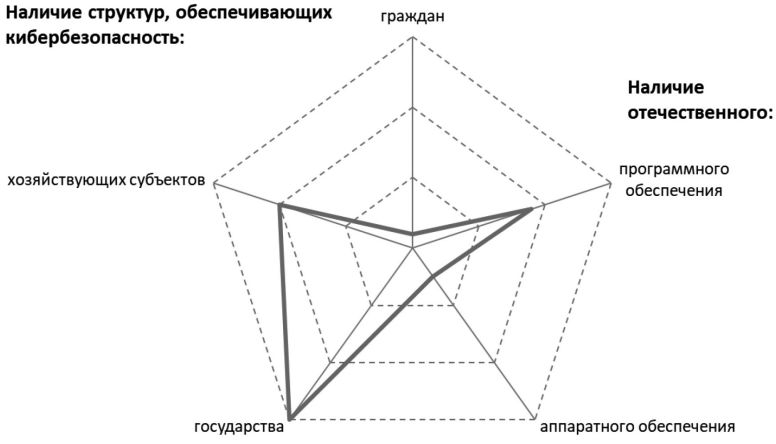
5 Тишина Ю. Смартфоны пересоберут в России. Mobile Inform Group и «Ростех» локализуют производство мобильных устройств. – *Коммерсантъ*. № 19. 04.02.2020. С. 7. Доступ: https://www.kommersant.ru/doc/4242123?utm_source=newspaper&utm_medium=email&utm_campaign=newsletter (проверено 04.04.2020).

6 Закон о предустановке российского софта на смартфоны принят в третьем чтении. – *Государственная Дума ФС РФ. Официальный сайт*. 21.11.2019 Доступ: http://duma.gov.ru/news/47043/ (проверено 29.03.2020).

которой произведен в Китае[1], и внешних библиотек программных кодов, используемых при отображении веб-страниц, бóльшая часть которых связана с узлами *Google, Cloudflare и Facebook*, расположенными на территории США[2].

Таким образом, приведенная выше информация говорит о том, что риски, порождаемые развитием цифровых технологий, угрожают основам экономики, общества и самого государственного строя России. При этом вопросами защиты государственных интересов занимаются все государственные структуры, начиная с Министерства обороны, ФСБ и Минкомсвязи и заканчивая специально созданными для этого институтами (НКЦКИ). В кредитно-финансовой сфере вопросами кибербезопасности занимается департамент Банка России (ФинЦЕРТ). Остальной корпоративный сегмент обеспечивает свою кибербезопасность самостоятельно, так же как и население РФ. Концепция Генпрокуратуры России о создании системы сбора информации о кибермошенничестве, совершенном против гражданского населения, еще не реализована и ограничена финансовой сферой. Переход программно-аппаратного обеспечения на отечественные разработки происходит неравномерно, с серьезным отставанием аппаратного сегмента.

Выводы. Результаты рассмотрения вопроса о признаках освоения Россией (как государством) виртуального пространства для обеспечения безопасности, охраны общественного порядка, обеспечения суверенитета и территориальной целостности, а также защиты существующего политического строя и правовой системы представлены на рис. 1 в виде лепестковой диаграммы.



Источник: Составлено авторами.

Рисунок 1. Степень освоения Россией виртуального пространства в сфере безопасности

На основании проведенного анализа функций, выполняемых Российской Федерацией в виртуальном пространстве по обеспечению безопасности, можно сделать следующие выводы.

1. В киберпространстве основной ценностью является информация, под которой следует понимать не только данные, но и управленческие решения,

[1] Почему вся электроника производится в Китае? – *EXPRO*. Доступ: https://chinaexpro.ru/blog/pochemu-vsya-elektronika-proizvoditsya-v-kitae/ (проверено 09.04.2020).

[2] Венедюхин А. Централизованный Интернет. – *D-russia.ru:* онлайн-издание. 13.03.2019. Доступ: http://d-russia.ru/tsentralizovannyj-internet.html (проверено 09.04.2020).

информационные потоки, медиаконтент и т.п., которую необходимо защитить как от хищений, так и от искажения и компрометации.

2. Риски, порождаемые развитием цифровых технологий, угрожают основам экономики, общества и самого государственного строя России. Поэтому защитой государственных интересов в виртуальном пространстве занимаются как государственные структуры, так и специально созданные для этого институты.

3. В кредитно-финансовой сфере вопросами кибербезопасности занимается департамент Банка России (ФинЦЕРТ). Корпоративный сегмент обеспечивает свою кибербезопасность самостоятельно, так же как и население РФ.

4. Переход программно-аппаратного обеспечения на отечественные разработки происходит неравномерно, с серьезным отставанием аппаратного сегмента.

Список литературы

Грунтов А. 2019. Информационная безопасность бизнеса: самые эффективные решения. – *Выступление на XIV ежегодной конференции «Комплексная безопасность бизнеса и противодействие хищениям»*. 9–10 октября 2019 г. М.: Ассоциация «Объединение сертифицированных специалистов по расследованию хищений». Доступно по запросу: info@acfe-rus.org (проверено 03.04.2020).

Чалдаева Л.А., Килячков А.А., Якорев А.А. 2020. К вопросу о становлении экономико-организационных функций государственного управления в виртуальном пространстве России. – *Власть*. Т. 28. № 2. С. 63-73.

CHALDAEVA Larisa Alekseevna, Dr.Sci. (Ec.), Professor; Professor of the Chair of Economics, Financial University under the Government of the Russian Federation (49 Leningradsky Ave, Moscow, Russia, 125993; Chaldaeva45@mail.ru)

KILYACHKOV Anatoliy Anatol'evich, Cand.Sci. (Techn.Sci.), Senior Scientific Researcher; Scholar of Security Problems Studies Centre of the Russian Academy of Sciences (21b Garibaldi St, Moscow, Russia, 119334; AAKil@mail.ru)

YAKOREV Anatoliy Aleksandrovich, Director of the Institute for International Cooperation, Compliance and Business Protection (bld. 1, 9 Khoroshevsky Pas, Moscow, Russia, 123007; cybericle@mail.ru); Vice-Chairman for International Cooperation of INGO «National Public Control Committee»

ON THE FORMATION OF STATE FUNCTIONS TO ENSURE SECURITY IN THE VIRTUAL SPACE OF RUSSIA

Abstract. *The paper considers the signs of the formation of the Russian Federation state functions to ensure security in cyberspace. The internal function of the state to ensure security and public order presupposes the protection of the rights and legitimate interests of citizens, legal entities and the state. When considering the signs of the formation of state functions in the virtual space, it is necessary to answer the following questions: (1) what is the object of protection in the digital space, (2) which state institution performs these functions, and (3) how these functions are implemented. In the digital space, the main value is information, which is necessary not only to accumulate, store and process, but to ensure its security. Information security is not only its protection against theft, but also the prevention of distortion and compromise. The risks posed by the development of digital technologies threaten the foundations of the economy, society and the very state system of Russia. At the same time, all state structures are involved in protecting state interests. In the credit and financial sector, the Department of the Bank of Russia (FinCERT) deals with cyber security issues. The rest of the corporate segment provides its cyber security on its own, as well as the population of the Russian Federation. The transition of hardware and software to domestic developments is uneven with a serious lag in the hardware segment.*

Keywords: *virtual space, formation of virtual state, ensuring safety of population and state, formation of state functions in virtual space*