DOI dx.doi.org/10.24866/VVSU/2073-3984/2019-4/023-032

УДК 34.03:004.056.5

Д.В. Лобач[1]

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

Е.А. Смирнова[2]

Дальневосточный федеральный университет
Владивосток. Россия

Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам*

Предметом рассматриваемой статьи является кибербезопасность как состояние защищенности публичных (государство, общество) и частных (физические и юридические лица) интересов от противоправных кибератак (цифровых атак), совершаемых против компьютеров, компьютерных систем, их сетей, а также объектов критической информационной инфраструктуры. Целью статьи является анализ состояния киберпреступности в России в фокусе интенсивного развития и широкого распространения сквозных (дизруптивных) информационно-коммуникативных технологий, а также исследуется динамика развития нормативно-правовой базы относительно обеспечения кибербезопасности в России в современных условиях. В свою очередь, проведенный анализ количественных показателей совершенных в России киберпреступлений (преступления, совершенные с использованием информационно-коммуникационных технологий или в сфере компьютерной информации) позволяет составить репрезентативную модель состояния кибербезопасности. Предметно исследуется процесс создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информацион-

[1] Лобач Дмитрий Владимирович – канд. юрид. наук, доцент кафедры теории и истории российского и зарубежного права; e-mail: dimaved85@mail.ru

[2] Смирнова Евгения Александровна – канд. юрид. наук, старший преподаватель кафедры трудового и экологического права; e-mail: smirnova.ea@dvfu.ru

* *Публикация осуществлена в рамках I Дальневосточного международного форума «Роботы заявляют о своих правах: доктринально-правовые основы и нравственно-этические стандарты применения автономных роботизированных технологий и аппаратов». Мероприятие проведено при финансовой поддержке Российского фонда фундаментальных исследований, проект № 19-011-20072.*

ные ресурсы Российской Федерации (ГосСОПКА) и дается правовая оценка федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Отмечается, что правоохранительный потенциал анализируемого закона выражается в нормативном закреплении обязанностей в отношении субъектов критической информационной инфраструктуры, связанных с необходимостью проведения мероприятий по информированию федеральных органов исполнительной власти о компьютерных инцидентах и обеспечением выполнения порядка и технических условий установки и эксплуатации средств инфраструктуры. В заключении статьи резюмируются актуальные проблемы, связанные с нормативным регулированием отношений кибербезопасности. В работе используются статистический метод в части анализа данных о киберпреступлениях за период с 2014 по 2019 гг. и формально-юридический метод, связанный с исследованием ключевых правовых характеристик федерального закона № 187-ФЗ.

Ключевые слова и словосочетания: преступность, безопасность, киберугроза, кибератака, кибербезопасность, дизруптивные информационно-коммуникативные технологии, цифровые атаки, киберпреступления.

D.V. Lobach

Vladivostok State University of Economics and Service
Vladivostok. Russia

E.A. Smirnova

Far Eastern Federal University
Vladivostok. Russia

The status of cyber security in Russia at the modern stage of the digital transformation of the company and the formation of the national system of countering cyber threats

The subject of the article is cybersecurity as a state of protection of public (state, society) and private interests (individuals and legal entities) from illegal cyber attacks (digital attacks) committed against computers, computer systems, their networks, as well as objects of critical information infrastructure. The purpose of the article is to analyze the state of cybercrime in Russia in the focus of intensive development and widespread dissemination of cross-cutting (disruptive) information and communication technologies, and also study the dynamics of the development of the regulatory framework regarding ensuring cyber security in Russia in modern conditions. In turn, the analysis of quantitative indicators of crimes committed in Russia committed using information and communication technologies or in the field of computer information (cybercrime) will allow us to create a representative model of cybersecurity. The article investigates the process of creating a state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation (GosSOPKA) and gives a legal assessment to the federal law of July 26, 2017 № 187 «On the security of critical information infrastructure of the Russian Federa-

tion». It is noted that the law-enforcement potential of the analyzed law is expressed in the normative consolidation of duties in relation to the subjects of critical information infrastructure related to the need to carry out measures to inform computer incidents of federal executive authorities and to ensure compliance with the procedure and technical conditions for installing and operating infrastructure facilities. In conclusion, the article summarizes current issues related to the regulatory regulation of cybersecurity relations in wide coverage. The statistical method is used in the work in terms of analyzing data on cybercrimes for the period since 2014 to 2019 years and the formal legal method associated with the study of key legal characteristics of federal law № 187.

Keywords: crime, security, cyberthreat, cyberattack, cybersecurity, disruptive information and communication technologies, digital attacks, cybercrime.

Интенсивное развитие, распространение и интегративное применение сквозных (дизруптивных) информационно-коммуникативных технологий в условиях так называемой Четвертой промышленной революции предопределяют множество положительных эффектов, связанных с оптимизацией производственных отношений, рационализацией систем публичного управления, снижением транзакционных издержек, ростом уровня жизни, повышением уровня комфортности жизни и гармонизацией социального устройства. Между тем современное состояние цифровизации социальных отношений также обусловливает актуализацию новых (нетипичных) угроз, посягающих на частные и публичные интересы [10]. Особое внимание обращают на себя киберугрозы, представляющие совокупность факторов и условий, создающих опасность нарушения информационной безопасности. С объективной стороны киберугрозы охватывают действия злоумышленников в киберпространстве, направленные на проникновение в информационную систему с целью кражи данных, денежных средств или с иными намерениями, которые потенциально ведут к негативным последствиям для государства, общества, бизнеса или частных лиц.

Анализ специальных отчетов, посвященных изучению современного состояния кибербезопасности в мире, позволяет констатировать, что по состоянию на II квартал 2019 г. противоправное завладение информацией и получение финансовых выгод остаются приоритетной задачей большинства кибератак. Кибератаки с целью завладения закрытой информацией совершаются в отношении физических (55% случаев) и юридических лиц (58% случаев). При этом корыстная мотивация при совершении кибератак прослеживается в 42% случаев в отношении физических лиц и в 30% – юридических лиц.

В контексте отраслевой привязки объектами кибератак в большинстве случаев выступают государственные учреждения (19%), промышленные компании (10%), медицинские учреждения (8%), финансовая отрасль (6%), а также наука и образование (6%). В оставшихся 27% случаев кибератаки обращены на IT-компании, сферу услуг, коммерческие структуры, блокчейн-проекты, транспортную инфраструктуру и другие объекты без отраслевой привязки. Вместе с тем наблюдается некоторая дифференциация атак относительно компонентов информационно-телекоммуникационной инфраструктуры. Так, если рассматривать кибератаки, совершаемые против юридических лиц, то в 65% случаев они

направлены против компьютеров, серверов и сетевого оборудования, в 25% случаев – против веб-ресурсов организации, в остальных случаях кибератаки осуществляются в отношении интернет-вещей, мобильных устройств, банкоматов и POS-терминалов. Что касается физических лиц, то кибератаки против компьютеров, серверов и сетевого оборудования составляют только 27%, в 29% случаев атаки совершаются против мобильных устройств. При этом отмечается, что в 33% случаев атаки направлены непосредственно против охраняемых законом частных интересов (атаки, направленные на противоправное завладение информацией, хищение или вымогательство денежных средств) [1].

В современных условиях распространения информационных технологий также наблюдаются качественная диверсификация и функциональная дифференциация хакерских атак. Качественная диверсификация хакерских атак выражается в появлении новых вредоносных программ, которые ориентированы не только на кражу данных, но в случае необходимости способных уничтожить зараженную систему. Кроме того, современные вредоносные программы моделируются по принципу превентивного обезвреживания антивирусных программ и виртуальных сред для анализа вирусов. В специальной литературе по вопросам кибербезопасности отмечается тенденция к увеличению вредоносных программ вымогателей и программ, ориентированных на противоправный майнинг криптоволюты. Появляются новые способы монетизации взломанных ресурсов, которые заключаются в несанкционированном дистанционном подсоединении к взломанным компьютерам в целях их дальнейшего использования в майнинге криптовалюты. При этом низкий порог входа в противоправную хакерскую деятельность обусловлен ростом предложения и увеличением спроса на вредоносные программы, инструкции и техники, предлагаемые в теневом Интернете (DarkNet).

Что касается функциональной дифференциации хакерских атак, то здесь речь идет о криминальной специализации применительно к осуществлению преступных замыслов по проведению многоэтапных хакерских атак, что проявляется в увеличении количества новых криминальных IT-профессий – дидосеры, дропперы, фишеры, кардеры, вирусописатели, заливщики. Следует также отметить и тот факт, что преступники все чаще прибегают к сложным и многоэтапным техникам, включающим в себя взлом инфраструктуры компаний-партнеров, заражение ресурсов известных производителей программного обеспечения или комбинацию нескольких методов в рамках одной атаки.

Широкое распространение кибератак становится острой проблемой для Российской Федерации в современных условиях цифровой трансформации социальных отношений и публичного управления, что подтверждается следующими статистическими данными.

По данным МВД РФ, за период с января по сентябрь 2019 г. в стране было зарегистрировано 205 116 преступлений, совершенных с использованием информационно-коммуникационных технологий или в сфере компьютерной информации (киберпреступления). В 2018 г. в России было зарегистрировано 174 674 киберпреступления, в 2017 г. 90 587 киберпреступлений, в 2016 г. – 66 322 преступления. Наблюдается рост удельного веса киберпреступлений в общем количестве преступлений за год при снижении общего уровня преступности: в 2016 г. удельный вес составил 3,8% (общее количество преступлений

составляет 2 160 063), в 2017 г. – 4,4% (общее количество преступлений составляет 2 058 476 преступлений), в 2018 г. – 8,7% (всего преступлений было совершено 1 991 532) и за период с января по сентябрь 2019 г. удельный вес киберпреступлений составил 13,4% (всего преступлений было совершено 1 521 683) [9].

Учитывая экспоненциальный рост кибератак, совершаемых в отношении физических и юридических лиц, а также государственных и муниципальных органов власти, руководство Российской Федерации приняло решение о принятии неотложных адаптивных организационно-правовых мер, направленных на обеспечение национальных интересов в области кибербезопасности адекватно актуальным и потенциальным киберугрозам. В сущности, современная политика в части обеспечения кибербезопасности России сводится к созданию Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Первый шаг в этом направлении был сделан Президентом РФ, который 15 января 2013 г. подписал Указ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Данный подзаконный нормативно-правовой акт закрепил за Федеральной службой безопасности РФ полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, представляющие собой информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом. Указанные полномочия конкретизируются в специальных задачах, возложенных на ФСБ РФ. Перечень задач включает в себя организацию и проведение работ по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), разработку методики обнаружения компьютерных атак и порядка обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, организацию мероприятий по оценке степени защищенности критической информационной инфраструктуры РФ от компьютерных атак, а также создание методических рекомендаций по организации защиты критической информационной инфраструктуры РФ [7].

В августе 2013 г. ФСБ РФ опубликовала подготовленные ведомством законопроекты, касающиеся безопасности критической информационной инфраструктуры России. Первый из законопроектов определяет, за счет чего в России обеспечивается безопасность критической ИТ-инфраструктуры[1] и устанавливает принципы обеспечения такой деятельности, а также полномочия органов государственной власти в данной области. Существенная часть критических ИТ-систем не находится в собственности государства, поэтому законопроект предусматривает

[1] Под критической ИТ-инфраструктурой следует понимать совокупность программных сервисов, служб, аппаратных средств и корпоративных документов, обеспечивающих возможности создания, хранения, передачи, обработки, защиты и удаления информации в пределах отдельной организации или системы организаций.

также «дополнительные обременения» для лиц, владеющих такими системами на правах собственности. Второй законопроект был направлен на установление мер ответственности за нарушение законодательства о безопасности критической информационной инфраструктуры [4].

Следующим шагом в развитии национальной стратегии обеспечения кибербезопасности стало утверждение в декабре 2014 г. Президентом РФ концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Интересно отметить, что ФСБ РФ официально опубликовала только выписку из этого документа, раскрывающую планируемую структуру будущей системы, что позволяет говорить о частичной засекреченности документа в целях исключения рисков анализа данной концепции на предмет уязвимостей [3]. В соответствии с этим документом система представляет собой единый централизованный территориально-распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган власти, уполномоченный в области обеспечения безопасности критической инфраструктуры РФ, и орган власти, уполномоченный в области создания и обеспечения функционирования системы. При этом в концепции определяется, что система представляет собой взаимосвязь технологических решений (средства) и специальных субъектов – подразделения и сотрудники со стороны федерального органа власти, ответственного за систему, а также операторов связи и других организаций, осуществляющих лицензируемую деятельность в сфере защиты информации. В сущности, представленная концепция является программной основой дальнейшего развития законодательной базы в сфере обеспечения кибербезопасности, а также определяет порядок обмена информацией о компьютерных атаках, стандарты деятельности субъектов системы в области обнаружения, предупреждения и ликвидации последствий атак. Особое внимание обращает на себя целевая ориентация концепции на организацию взаимодействия с правоохранительными и другими госорганами, владельцами информационных ресурсов РФ, операторами связи и интернет-провайдерами на национальном и международном уровнях.

В 2016 г. начинают совершаться первые практические мероприятия, связанные с реализацией программных положений вышеуказанной концепции. Во-первых, были приняты рекомендации №149/2/7-200 от 24.12.2016, регламентирующие порядок создания ведомственных и корпоративных центров ГосСОПКА. Во-вторых, появляется первый опыт взаимодействия и интеграции в части подключения и развития ГосСОПКА (например, Центр обнаружения, предупреждения и ликвидации последствий компьютерных атак (КЦОПЛ), госкорпорация Ростех, правительство Самарской области, тендер АФК «Система», намерение ФСО привлечь ГосСОПКА для создания и обеспечения работы закрытой государственной сети RSNet) [2].

В ноябре 2017 г. компании Solar Security и Positive Technologies инициировали запуск совместного бизнес-направления по созданию ведомственных и корпоративных центров ГосСОПКА на базе комплекса технологий и экспертизы Positive

Technologies, а также сервисов Solar Security по мониторингу и реагированию на инциденты.

Значимым событием в сфере обеспечения национальной кибербезопасности стало принятие 26 июля 2017 г. Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [8]. Юридическое содержание принятого нормативно-правового акта заключается в определении принципов, объектов и субъектов критической информационной инфраструктуры (КИИ), а также требований по обеспечению и оценке безопасности указанных объектов. В законе регламентируется, что ГосСОПКА включает в себя силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Понятие «сила» как функциональный элемент рассматриваемой системы охватывает три вида субъектов, уполномоченных в области обеспечения функционирования ГосСОПКА: 1) подразделения и должностные лица федерального органа исполнительной власти; 2) национальный координационный центр по компьютерным инцидентам); 3) подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты. В свою очередь, под средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, закон понимает технические, программные, программно-аппаратные и иные средства, а также криптографические средства защиты такой информации. Более подробные характеристики таких средств отражены в приказе ФСБ РФ от 6 мая 2019 г. № 196 [5].

В законе особо подчеркивается целевое назначение государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак. В частности, в ч. 5 ст. 5 данного закона определено, что в системе происходит сбор, накопление, систематизация и анализ информации, которая поступает в данную систему через специальные средства (технические, программные, программно-аппаратные и иные), информации, представленной субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, а иными (не являющимися субъектами критической информационной инфраструктуры) органами и организациями, в том числе иностранными и международными.

Правоохранительный потенциал анализируемого закона также выражается в нормативном закреплении обязанностей в отношении субъектов КИИ, связанных с необходимостью проведения мероприятий по информированию о компьютерных инцидентах федеральных органов исполнительной власти и обеспечению выполнения порядка и технических условий установки и эксплуатации средств инфраструктуры объектов КИИ. Кроме того, субъекты в силу закона

должны реагировать на компьютерные инциденты, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ, и непрерывно взаимодействовать с ГосСОПКА. Закон направлен на предупреждение компьютерных атак, равно как и последствий их совершения, способных подорвать критическую информационную инфраструктуру государства, вызвать социальную, организационную, финансовую и экологическую катастрофу.

Вместе с тем, несмотря на предпринятые государством шаги в сфере обеспечения защиты объектов критической информационной инфраструктуры, имеются актуальные проблемы, связанные с нормативным регулированием отношений кибербезопасности в широком освещении. Прежде всего, хотелось бы отметить, что реализация концепции ГосСОПКА далека от своего логического завершения, поскольку создание отраслевых центров ГосСОПКА, которое осуществляется при субсидировании из госбюджета и на конкурсной основе, только началось [6]. Во-вторых, остается нерешенным вопрос о бремени финансовых затрат, возникающих при создании центров ГосСОПКА. На сегодняшний день такие центры могут создаваться только в федеральных органах власти и крупных корпорациях, в то время как малый и средний бизнес фактически остаются без поддержки ГосСОПКА, поскольку подключение к системе представляется довольно затратным мероприятием. В-третьих, в действующем законодательстве в сфере обеспечения кибербезопасности все еще отсутствует унифицированная определенность операциональных понятий (к вопросу о нормативной дефинитивной определенности), а используемые на практике дефиниции часто трактуются довольно пространно, что обусловливает неопределенность в концептуально-правовом поле. В частности, при всем многообразии киберугроз необходимо определиться с такими понятиями, как информационная атака, dos-атака, фишинг, спам, заражение, хактивизм, кибертерроризм. Нерешенным остается вопрос об концептуально-правовой определенности понятия «кибербезопасность», которое в действующем законодательстве все еще не сформировано. Представляется, что нормативное закрепление рассматриваемых дефиниций позволит сфокусировать и сбалансировать как правоприменительную практику, так и дальнейшую правотворческую работу в сфере противодействия киберугрозам. В-четверых, в фокусе противодействия киберугрозам актуализируется вопрос о пределах государственного вмешательства в те сферы информационно-коммуникационной системы, которые могут стать объектом кибератак. Учитывая принцип свободного обмена информацией и нерегулируемый со стороны государства характер функционирования Интернета, следует признать, что государственное вмешательство может быть допустимым лишь в том случае, если этические основы таких интернет-сообществ будут неэффективными.

В заключение необходимо отметить, что кибербезопасность представляет собой состояние защищенности публичных и частных интересов от противоправных атак, совершаемых в отношении компьютеров, компьютерных систем и их сетей, а также объектов критической информационной инфраструктуры. Увеличение количества хакерских атак в России за последние 6 лет предопределило

правотворческую динамику политико-правового реагирования в отношении современных киберугроз. Вместе с тем правовая политика в области обеспечения кибербезопасности сопровождается рядом проблем, требующих своего разрешения в обозримом будущем.

1. Актуальные киберугрозы: II квартал 2019 г. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q2/
2. Бодрик А. Кибербезопасность России: итоги 2016 года и стратегии для 2017 [Электронный ресурс]. URL: https://www.itweek.ru/security/article/detail.php?ID=191370
3. Выписка из концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274) [Электронный ресурс]. URL: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf
4. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА [Электронный ресурс]. URL: http://www.tadviser.ru
5. Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты: приказ ФСБ России от 6 мая 2019 г. № 196 (не вступил в силу) [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/72157648/
6. Об утверждении Правил предоставления субсидий из федерального бюджета на создание отраслевого центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах: постановление Правительства РФ от 7 октября 2019 г. № 1285 [Электронный ресурс]. URL: http://base.garant.ru/72826274/#ixzz65jK6IQeF
7. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: указ Президента Российской Федерации от 15 января 2013 г. № 31с г. Москва [Электронный ресурс]. URL: https://rg.ru/2013/01/18/komp-ataki-site-dok.html
8. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26.07.2017 № 187-ФЗ [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru
9. Статистика и аналитика Министерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics
10. Шваб К. Четвертая промышленная революция. – М.: Эксмо, 2018. С. 12–45.

Транслитерация

1. Aktual'nye kiberugrozy: II kvartal 2019 g. [Elektronnyj resurs]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q2/
2. Bodrik A. Kiberbezopasnost' Rossii: itogi 2016 goda i strategii dlya 2017 [Elektronnyj resurs]. URL: https://www.itweek.ru/security/article/detail.php?ID=191370
3. Vypiska iz koncepcii gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii (koncepciya utverzhdena Prezidentom Rossijskoj Federacii 12 dekabrya 2014 g. № K 1274) [Elektronnyj resurs]. URL: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf
4. Gosudarstvennaya sistema obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak GosSOPKA [Elektronnyj resurs]. URL: http://www.tadviser.ru

5. Ob utverzhdenii Trebovanij k sredstvam, prednaznachennym dlya obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak i reagirovaniya na komp'yuternye incidenty: prikaz FSB Rossii ot 6 maya 2019 g. № 196 (ne vstupil v silu) [Elektronnyj resurs]. URL: https://www.garant.ru/products/ipo/prime/doc/72157648/
6. Ob utverzhdenii Pravil predostavleniya subsidij iz federal'nogo byudzheta na sozdanie otraslevogo centra Gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak (GosSOPKA) i vklyuchenie ego v sistemu avtomatizirovannogo obmena informaciej ob aktual'nyh kiberugrozah: postanovlenie Pravitel'stva RF ot 7 oktyabrya 2019 g. № 1285 [Elektronnyj resurs]. URL: http://base.garant.ru/72826274/#ixzz65jK6IQeF
7. O sozdanii gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii: ukaz Prezidenta Rossijskoj Federacii ot 15 yanvarya 2013 g. N 31s g. Moskva [Elektronnyj resurs]. URL: https://rg.ru/2013/01/18/komp-ataki-site-dok.html
8. O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii: federal'nyj zakon ot 26.07.2017 № 187-FZ [Elektronnyj resurs]. Oficial'nyj internet-portal pravovoj informacii. URL.: http://www.pravo.gov.ru
9. Statistika i analitika Ministerstva vnutrennih del Rossijskoj Federacii [Elektronnyj resurs]. URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics
10. Shvab K. CHetvertaya promyshlennaya revolyuciya. – M.: Eksmo, 2018. S.12-45.

Для цитирования: Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11, № 4. С. 23–32.

For citation: Lobach D.V., Smirnova E.A. The status of cyber security in Russia at the modern stage of the digital transformation of the company and the formation of the national system of countering cyber threats, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2019, Vol. 11, № 4, pp. 23–32.

DOI dx.doi.org/10.24866/VVSU/2073-3984/2019-4/023-032

Дата поступления: 29.11.2019.