DOI 10.24411/2076-1503-2020-10544

ШИНКАРЕЦКАЯ Галина Георгиевна,
доктор юридических наук,
главный научный сотрудник
Института государства и права
Российской академии наук
e-mail: gshink@yandex.ru

БЕРМАН Алиса Михайловна,
младший научный сотрудник
Института государства и права
Российской академии наук
e-mail: alias.berman@mail.ru

ЦИФРОВИЗАЦИЯ И ПРОБЛЕМА ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16012

Аннотация. *Цифровые технологии являются неотъемлемой частью существования современного мирового сообщества и глобальной тенденцией мирового развития. В статье обосновывается, что цифровизация и национальная безопасность государства являются взаимосвязанными и взаимозависимыми явлениями. Для этого даются ответы на следующие вопросы: Какова роль цифровизации как инструмента обеспечения национальной безопасности? Может ли цифровизация стать угрозой национальной безопасности? Каковы факторы, тормозящие развитие цифровых технологий, которые требуют государственного вмешательства?*

Ключевые слова: *цифровизация, цифровые технологии, национальная безопасность, национальная политика, кибербезопасность, криптовалюта, рынок труда, суверенитет государства.*

SHINKARETSKAIA Galina Georgievna,
Doctor of Law,
Chief Researcher of
the Institute of State and Law
of the Russian Academy of Sciences

BERMAN Alisa Mikhailovna,
Junior Researcher of
the Institute of State and Law
of the Russian Academy of Sciences

DIGITALIZATION AND THE NATIONAL SECURITY ISSUE

The reported study was funded by RFBR, project number 18-29-16012

Annotation. *Digital technologies are an integral part of the existence of the modern world community and a global trend in world development. The article substantiates that digitalization and national security of the state are interconnected and interdependent phenomena. For this, answers to the following questions are given: What is the role of digitalization as a tool for national security? Can digitalization be a threat to national security? What are the factors hindering the development of digital technologies that require government intervention?*

Key words: *digitalisation, digital technology, national security, national policy, cybersecurity, cryptocurrency, labor market, state sovereignty.*

В XXI в. цифровые технологии стали одним из главных двигателей прогресса и ресурсов экономической борьбы. Информационно-коммуникационные технологии определяют динамику развития мировой экономики и многие содержательные аспекты отношений между государствами [7]. Однако цифровизация – не только источник долгосрочного экономического роста страны и инструмент экономической гонки на мировой арене (например, посредством повышения конкурентоспособности страны на рынке товаров и услуг, уровня жизни населения и т.д.), но и фактор суверенности и стабильности государства, его национальной безопасности.

Вместе с тем, не только цифровизация влияет на национальную безопасность государства, но и национальная политика, преследующая в т.ч. и цели по обеспечению национальной безопасности, непосредственно влияет на темпы и сферы развития цифровизации. Таким образом, можно говорить о взаимодействии и взаимном влиянии цифровизации и национальной безопасности [22].

I. Цифровизация как инструмент обеспечения национальной безопасности

Одним из катализаторов модификации общественных отношений и государственной политики служит внедрение цифровых технологий в хозяйственную практику и систему общественных взаимодействий. Цифровые технологии являются «двигателем» государственных инновационных процессов, ориентированных на формирование цифровой экономики и обеспечение национальной безопасности и суверенности государства. «Информация, информационные технологии, информатизация всех сторон социума привносит такие изменения в жизнь индустриального и постиндустриального общества, которые требуют изменений, порой коренных, в институтах организации управления и права», – пишет И.Л. Бачило [2].

Зачастую цифровые технологии не влияют на национальную безопасность непосредственно, а воздействие происходит через влияние на динамику и вектор социально-экономического прогресса, поэтому страны, «отстающие» по темпам и масштабам цифровизации, сталкиваются с рядом угроз национальной безопасности. Среди таких угроз можно выделить, например, следующие: догоняющая роль в мировой экономике, ограничение перспектив инновационного развития, снижение конкурентоспособности их компаний (особенно в сравнении с транснациональными корпорациями, ориентированными на самые экономически развитые страны), ограниченность инструментария для обеспечения национальной безопасности и т.д.

Особое значение цифровые технологии приобретают в период, когда то или иное государство сталкивается с большими вызовами, как, например, ухудшение санитарно-эпидемиологической обстановки в мире в начале 2020 г., вызванное распространением пандемии коронавирусной инфекции нового типа – COVID-19. Правдивая, получаемая незамедлительно информация, в основном через Интернет, становится жизненно необходимой.

Подобные обстоятельства требуют также быстрого и эффективного реагирования со стороны мирового сообщества (на уровне государств, интеграционных объединений, отдельных международных организаций и т.д.), ускоряют реализацию и развитие накопленного потенциала использования информационных и цифровых технологий. Так, новые методы в здравоохранении, как, например, интернет-медицина, обсуждались в литературе давно [16], но внедряются в практику медленно.

Тем не менее, в ответ на такие глобальные угрозы, как потепление климата, загрязнение окружающей среды, несоблюдение прав человека происходит повсеместное распространение информационно-коммуникационных и цифровых технологий, особенно в сферах образования, государственного управления, правосудия, онлайн-коммуникаций, электронной торговли, финансов и т.д.

Это, в свою очередь, вызывает необходимость совершенствования действующего законодательства с целью приведения его в соответствие существующим реалиям, увеличения финансирования в сферу информационных и цифровых технологий, повышения степени защиты персональных данных и т.д. [6]. Этот процесс ярко проявился в разных государствах, в т.ч. в России, во время пандемии. С введением государством ограничительных мер, национальные суды приостановили рассмотрение большинства дел, а для обеспечения доступа к правосудию начали проводить онлайн-заседания. Представляется, что данный процесс не будет прекращен со снятием ограничительных мер, а онлайн-правосудие получит дальнейшее развитие [21].

Кроме того, на период карантина все образовательные учреждения были переведены в режим электронно-дистанционного обучения, для чего государственными органами были разработаны интернет-платформы, которые способствуют подобному обучению [15].

Важным планируемым законодательным изменением в нашей стране, вызванным одной из

мер, препятствующих распространению вируса, а именно – долгим отсутствием работников на производстве, является снижение налогообложения в сфере информационных технологий, которая традиционно отличается высокой мобильностью. Это позволит создать в Российской Федерации благоприятные налоговые, финансовые и правовые условия для повышения конкурентоспособности страны и предотвращения «налоговой миграции» IT – специалистов в другие юрисдикции [3].

Вышеизложенное свидетельствует о заинтересованности государства в развитии цифровизации для обеспечения национальной безопасности и интересов общества. Однако может ли цифровизация стать угрозой национальной безопасности?

II. Цифровизация как угроза национальной безопасности

Как и у любого социально-экономического явления, у цифровизации есть не только положительные стороны, но и скрытые угрозы, которые потенциально могут нанести вред национальной безопасности в случае, если вовремя не будут взяты под контроль. В качестве наиболее очевидных следует назвать угрозу экономической стабильности ввиду распространения неконтролируемых денежных средств и угрозу социальной стабильности в силу изменения рынка труда.

а) криптовалюта

Криптовалюта – это условное название зашифрованного нерегулируемого цифрового актива, использующегося в качестве аналога валюты в обменных операциях. Криптовалюта не имеет физической формы, она существует только в электронной сети в виде данных [21]. Банки, а значит, и государства практически не могут регулировать ее эмиссию, а потому подобные финансовые инновации, в т.ч. т.н. криптотехнологии, расцениваются как угроза национальной безопасности.

В данной проблеме следует выделить четыре аспекта. Первый из них заключается в том, что именно криптовалюта зачастую используется для легализации незаконных доходов, финансирования террористических организаций и прочих незаконных операций. Преступников привлекает анонимность расчетов криптовалютой, а также трудность, почти невозможность, отслеживания операций, производимых в криптовалюте [4].

Второй проблемный аспект связан с децентрализованной природой криптовалюты (отсутствие единого эмитента такой валюты и, как следствие, ее экстерриториальность и невозможность подчинения какой-либо юрисдикции), которая при ее капитализации сможет существенно влиять на экономику стран и даже может потенциально подорвать суверенитет и экономическую независимость государства как единственного субъекта, наделенного правом денежной эмиссии и организации денежного обращения. Это, в свою очередь, может повлиять на инфляцию, т.к. финансовые инновации ускоряют темпы прохождения операций, что повышает скорость обращения денег и, как следствие, ускоряет процесс инфляции.

Третий проблемный аспект связан с т.н. «скам-проектами», которые выражаются в создании мошеннических инвестиционных схем при помощи криптовалюты. Криптовалюта, являясь высоко рисковым активом с высокой волатильностью, может потенциально привести к потере средств простыми гражданами при ее использовании в виде средства платежа и накопления, что, в свою очередь, негативно скажется и на самом государстве. В связи с этим, государство должно брать на себя роль регулятора, защищающего права рядовых инвесторов от покупки «спам-токенов» [12].

Заключительный, четвертый, проблемный аспект связан с фискальной функцией государства, т.к. криптовалюта является инструментом, благоприятным для обхода налогообложения. Криптовалюта, будучи быстроразвивающимся механизмом, создает ситуацию, в которой правовое регулирование (в т.ч. и налоговое) существенно отстает от технологий, что приводит к значительным налоговым недопоступлениям в бюджет государства от операций с криптовалютой.

Однако в нынешних реалиях невозможно игнорировать популярность и востребованность криптовалюты, поэтому государствам еще предстоит разработать грамотное регулирование данной отрасли, где должен быть соблюден баланс между национальными интересами и безопасностью государства и изначальной природой криптовалюты, в отношении которой невозможен тотальный контроль, т.к. это разрушит всю идею и смысл ее существования.

б) рынок труда

Одним из дискуссионных вопросов являются социальные последствия цифровизации, а именно – как внедрение новых технологий отразится на рынке труда? Зачастую высказываются опасения о том, что роботизация и автоматизация труда могут повлечь сокращение рабочих мест и, как следствие – рост безработицы, падение уровня жизни значительной части населения, снижение показателей рождаемости, увеличение масштабов преступности и дальнейшее обострение социально-экономических противоречий в обществе. Данный вывод прослеживается на примере технологических революций, которые происходили ранее в истории, что неминуемо приво-

дило к сокращению рабочих мест (вплоть до исчезновения отдельных профессий) и изменению стоимости рабочей силы. Так, например, исчезли такие профессии (о существовании которых уже мало кто помнит), как ледоруб, писарь, плотогон, человек-будильник, оператор коммуникатор, путеукладчик и многие др. [9].

Исторически роботизация, в первую очередь, влияла на те профессии, которые не требуют высокой квалификации наемного работника или связаны с выполнением производственных задач. Обусловливается это тем, что роботизация повышает производительность, снижает издержки и удешевляет производство. Однако в XXI в. начинают озвучивать прогнозы о том, что работу из-за роботов могут потерять и работники умственного труда – юристы, офисные служащие, системные администраторы и др.

Представляется, что подобные «апокалиптические» прогнозы не в полной мере соответствуют действительности и значительно преувеличены. Первая причина видится в том, что для повышения производительности требуется длительный период после внедрения технологий. Примером может служить внедрение касс самообслуживания, которые на начальных этапах работы не только не повышают производительность, но и требуют привлечения нового персонала, помогающего клиентам «осваивать» технологические новинки. Кроме того, внедрение технологий требует прохождения длительного испытательного периода для обеспечения должного уровня безопасности для их полноценного функционирования без помощи человека (примером может служить беспилотный транспорт), а зачастую и разработки соответствующей нормативно-правовой базы, что также требует значительного времени.

Во-вторых, в связи с тем, что роботизация и автоматизация повышает производительность компаний, тем самым увеличивая их прибыль, компании начинают стремиться к расширению бизнеса, что требует привлечения новых сотрудников путем создания дополнительных рабочих мест. Таким образом, в данном случае следует говорить не о потенциальном росте безработицы населения, а о его переквалификации. Кроме того, зачастую автоматизация затрагивает не всю профессию целиком, а только отдельные функции, выполняемые работниками в рамках профессии.

Самое заметное и парадоксальное явление в проблеме занятости в связи с цифровизацией – это т.н. поляризация. Так называют вымывание среднего слоя работников при одновременном росте занятости в крайних стратах. Такой процесс поляризации был сначала отмечен в странах ОЭСР [17], специалисты указывают, что главной причиной поляризации являются цифровизация и автоматизация [14]. Можно предположить, что в основе этого явления лежат социальные причины: к среднему слою относятся те, кто чувствует себя способным делать не самую простую работу, но у них нет доступа к хорошему образованию и нет возможности освоить цифровые операции.

в) киберугрозы

Термин «киберугрозы» используется для обозначения потенциально преступных действий против информационной системы государства [5], поэтому они могут проявляться и в экономике, и в положении трудящихся.

При этом и субъекты, и объекты преступных действий весьма разнообразны. Субъектами могут быть индивиды, стремящиеся получить незаконный доступ к банковским авуарам, а могут быть и государства, намеренно наносящие вред другому государству; объектами всегда выступают информационные системы, но они, в одних случаях, могут принадлежать гражданам и обслуживать их интересы, а в других – выполнять функции государственного управления или поддержания нормальной жизнедеятельности государства.

Киберпреступность началась с элементарного грабежа, т.е. завладения чужой собственностью путем обмана или мошенничества. Уже в XXI в. хакерские атаки начали применяться в качестве средства враждебного воздействия на государства. Есть данные о том, что возможностями такого воздействия располагают более тридцати государств. Однако события с разрушением «башен-близнецов» на Манхэттене показали, что сложные технологические структуры могут оказаться в руках частных лиц и использоваться ими для враждебных действий против целых государств [18].

Все это приводит к необходимости привлечения дополнительного инвестирования (как бюджетного, так и частного) для обеспечения информационной безопасности. В условиях, когда отдельные предприятия неспособны самостоятельно найти источники для финансирования, киберугрозы могут стать не только фактором сдерживания цифровизации отдельных отраслей, но и потенциальной угрозой национальной безопасности всего государства (в зависимости от выбранного для кибератаки объекта или сведений разной степени значимости и секретности) [20].

Необходимость обеспечения кибербезопасности является глобальной проблемой, а не проблемой какого-либо отдельно взятого государства, т.к. сегодня с киберугрозами сталкивается каждое государство, даже такое, которое располагает незначительными информационными и цифровыми технологиями.

Приведенные данные показывают, что борьба с киберпреступностью – сложная проблема, которая не может быть решена простыми средствами. Необходимо достижение организационно-правового режима информационной безопасности [8, с. 11].

Примером может служить Китайская Народная Республика как один из лидеров на рынке информационных и цифровых технологий. Специфика обеспечения информационной безопасности (в КНР используется именно термин «информационная безопасность», а не «кибербезопасность») существенно отличается от западной. В целях недопущения утечки значимой для государства и национальной безопасности информации или, наоборот, проникновения нежелательных данных КНР придерживается политики, что Интернет есть важная инфраструктура государства и поэтому его следует держать под контролем (вплоть до блокировки ряда социальных сетей и поисковых систем). Кроме того, подлежит обязательному лицензированию деятельность компаний, которые предоставляют услуги в киберпространстве. В КНР создана и эффективно функционирует разветвленная система государственных органов, главной задачей которых является обеспечение информационной безопасности страны. Любое посягательство на этот внутренний сегмент воспринимается как угроза национальной безопасности.

Подводя итоги, хотелось бы отметить, что, несмотря на все обозначенные угрозы повсеместной цифровизации, представляется, что глобальный процесс трансформации социально-экономических отношений будет иметь неизбежное дальнейшее всестороннее развитие. В связи с этим, следует более детально рассмотреть факторы, которые могут затормозить процесс развития цифровых технологий, в т.ч. факторы, обусловленные интересами национальной безопасности [10].

III. Факторы, тормозящие развитие цифровых технологий, которые требуют государственного вмешательства

Сегодня проводится объемная работа как на государственном, так и на негосударственном уровне для развития цифровых технологий и их повсеместного проникновения во все сферы жизни общества – инвестирование в развитие национального IT-сектора, финансовое стимулирование создания новейших информационных технологий, кооперация для их создания на международном уровне, стимулирование инвестиций и предпринимательской активности в данной области и т.д. Однако, несмотря на все это, еще существует множество факторов, которые тормозят развитие цифровых технологий, основными из которых представляются следующие три.

Во-первых, степень доверия общества (особенно общества развивающихся стран) к цифровым технологическим новинкам, готовность (а зачастую и базовая возможность) их воспринять и повсеместно использовать находятся на низком уровне, что, соответственно, формирует низкий спрос и, в свою очередь, согласно законам экономики, напрямую влияет на предложение в данной области. Устранение данного барьера возможно, например, посредством проведения политики государства по повышению цифровой и информационной грамотности населения (в т.ч. политики по популяризации технологий в повседневной жизни), созданию доступной технологической среды во всех регионах государства (вне зависимости от степени благосостояния населения) и обеспечению безопасности информационных и инновационных технологий (например, гарантирование неприкосновенности частной жизни при работе в сети Интернет, защита пользовательских данных и прав потребителей, платежных приложений, персональных данных и т.д.).

Во-вторых, даже сегодня еще не все компании осознают пользу внедрения и использования цифровых и информационных технологий для бизнеса (начиная с осуществления сделок в электронной форме, облачного хранения данных и роботизации и заканчивая блокчейном, машинлернингом и искусственным интеллектом), и соответственно не используют свои потенциальные производственные возможности с технологическими мощностями по максимуму. Происходит это, например, из-за нежелания изменять сложившийся уклад, перестраивать корпоративную культуру и отлаженные бизнес-процессы.

В-третьих, самым труднопреодолимым и требующим комплексного решения барьером является незащищенность самой цифровизации от кибератак. Вызвано это тем, что в связи с динамичностью развития данной сферы, угрозы, которым она подвергается, также не стоят на месте, поэтому меры по борьбе с ними должны быть универсальными и должны работать на опережение, а не на устранение последствий уже состоявшихся кибератак.

Во всем мире повсеместно государственная политика в области цифровизации выстраивается по пути формирования комплексных стратегий борьбы с киберпреступностью. Вопросы цифровизации ложатся в основу национальных программ и стратегий государств. Так, последняя подобная стратегия США [13], например, предусматривает ужесточение наказаний за хакерские атаки. ЕС стремится к усилению полномочий агентства по кибербезопасности, а также созда-

нию общеевропейской системы сертификации в сети [11]. В России создаются государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, различные центры кибербезопасности при стратегически значимых объектах, а также единая система противодействия кибератакам [1].

Для развития и повсеместного распространения цифровых технологий необходима гарантия определенного уровня национальной стабильности, а также соблюдение прав граждан и бизнеса, как, например: обеспечение прав пользователей в цифровом мире и сохранности их цифровых данных (в т.ч. посредством защиты от внешнего информационно-технического воздействия на информационную инфраструктуру), повышение уровня доверия к цифровой среде, минимизация количества киберугроз, обеспечение доступа к достижениям цифровизации на территории всей страны, наращивание кадрового и научного потенциала в цифровой области для повышения конкурентоспособности страны, внедрение отечественных разработок в целях уменьшения зависимости социально-экономического развития от экспорта и т.д.

До тех пор, пока государством не будет выстроена и обеспечена эффективная политика в сфере цифровых технологий, технологии не смогут в должной степени выполнять свои функции и служить национальным интересам, т.к. процессы цифровизации и национальная безопасность имеют непосредственное взаимовлияние и находятся в постоянной взаимосвязи.

Список литературы:

[1] Указ Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15 января 2013 г. № 31с // СЗ РФ. - 2013. - № 3. - Ст. 178.

[2] Бачило И.Л. Предпосылки укрепления правового регулирования инновационных процессов в публичном управлении на основе информационных технологий // Труды ИГП РАН. - 2009. - № 5/2009. – С. 10.

[3] «Ведомости» узнали суть налогового маневра в ИТ-сфере // РБК. URL: https://www.rbc.ru/business/22/06/2020/5ef0476c9a79477 4ef894791 (дата обращения: 20.04.2020).

[4] Жарова А.К. Проблема анонимности субъектов в сети Интернет // Труды ИГП РАН. - 2009. - № 5/2009. – С. 135–158.

[5] Палаева Л.В., Хафизов А.М., Гилязетдинова А.М. и др. Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них // Фундаментальные исследования. - 2017. - № 10 (3). – С. 507–511.

[6] Полякова Т.А. Базовые принципы правового обеспечения информационной безопасности // Труды ИГП РАН. - 2016. - № 3 (55). – С. 17–40.

[7] Понятийный аппарат в информационном праве: коллективная монография / под ред. И.Л. Бачило, Т.А. Поляковой, В.Б. Наумова. – М.: ИГП РАН, 2017. – С. 8, 9.

[8] Рыжов В .Б. Информационная безопасность в государствах Европейского союза: к постановке проблемы // Представительная власть – XXI век. - 2018. - № 4 (163). – С. 8 - 12.

[9] Талапина Э.В. Эволюция прав человека в цифровую эпоху // Труды ИГП РАН. - 2019. - Т. 14. - № 3. – С. 122–146.

[10] Шинкарецкая Г.Г. Цифровизация – глобальный тренд мировой экономики // Образование и право. - 2019. - № 8. – С. 119–123.

[11] Regulation (EC) № 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act) // Official Journal of the European Union L 151 of 7 June 2019.

[12] Criminal Compliant // The United States Department of Justice. URL: https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/30/criminal_complaint_force.pdf (дата обращения: 20.04.2020).

[13] National Cyber Strategy of the United States of America // The White House, September 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 20.04.2020).

[14] Akerman A., Gaarder I., Mogstad M. The Skill Complementarity of Broadband Internet // The Quarterly Journal of Economics. - 2015. - Vol. 130. - № 4. – P. 1781–1824.

[15] Black D., Bissessar Ch., Boolaky M. Online Education as an Opportunity Equalizer: The Changing Canvas of Online Education // Interchange. - 2019. - Vol. 50. - № 3. – P. 423 - 443.

[16] Cortez N. Patients Without Borders: The Emerging Global Market for Patients and the Evolution of Modern Health Care // Indian Law Journal. - 2008. - Vol. 83. – P. 71–113.

[17] Goos M., Manning A., Salomons A. Explaining Job Polarization: Routine Biased Technological Change and Offshoring // American Economic Review. - 2014. - Vol. 104. - № 8. – P. 2509–2526.

[18] Hollis D.B. Why States need an International Law for Information Operations // Lewis and Clark Law Review. - 2007. - Vol. 11. - № 4. – P. 1023–1061.

[19] Lee J., Long A., McRae M., Handler S. Bitcoin Basics: a Primer on Virtual Currencies // Business Law International. - 2015. - Vol. 16. - № 1. – P. 21.

[20] O'Connell M.E. Cyber Security without Cyber War // Journal of Conflict Security Law. - 2012. - Vol. 17. - № 2. – P. 187–209.

[21] Ronca M., Ross B., Dodd E. Digital justice: online learning beyond COVID-19 // UTS Centre for Social Justice & Inclusion Newsroom. URL: https://www.uts.edu.au/partners-and-community/initiatives/social-justice-uts/news/digital-justice-online-learning-beyond-covid-19 (дата обращения: 20.04.2020).

[22] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edition / ed. by M.N. Schmitt. CUP. - 2017. – P. 11–16.

Spisok literatury:

[1] Ukaz Prezidenta RF «O sozdanii gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii» ot 15 yanvarya 2013 g. № 31s // SZ RF. - 2013. - № 3. - St. 178.

[2] Bachilo I.L. Predposylki ukrepleniya pravovogo regulirovaniya innovacionnyh processov v publichnom upravlenii na osnove informacionnyh tekhnologij // Trudy IGP RAN. - 2009. - № 5/2009. – S. 10.

[3] «Vedomosti» uznali sut' nalogovogo manevra v IT-sfere // RBK. URL: https://www.rbc.ru/business/22/06/2020/5ef0476c9a794774ef894791 (data obrashcheniya: 20.04.2020).

[4] ZHarova A.K. Problema anonimnosti sub»ektov v seti Internet // Trudy IGP RAN. - 2009. - № 5/2009. – S. 135–158.

[5] Palaeva L.V., Hafizov A.M., Gilyazetdinova A.M. i dr. Osnovnye vidy kiberatak na avtomatizirovannye sistemy upravleniya tekhnologicheskim processom i sredstva zashchity ot nih // Fundamental'nye issledovaniya. - 2017. - № 10 (3). – S. 507–511.

[6] Polyakova T.A. Bazovye principy pravovogo obespecheniya informacionnoj bezopasnosti // Trudy IGP RAN. - 2016. - № 3 (55). – S. 17–40.

[7] Ponyatijnyj apparat v informacionnom prave: kollektivnaya monografiya / pod red. I.L. Bachilo, T.A. Polyakovoj, V.B. Naumova. – M.: IGP RAN, 2017. – S. 8, 9.

[8] Ryzhov V.B. Informacionnaya bezopasnost' v gosudarstvah Evropejskogo soyuza: k postanovke problemy // Predstavitel'naya vlast' – XXI vek. - 2018. - № 4 (163). – S. 8 - 12.

[9] Talapina E.V. Evolyuciya prav cheloveka v cifrovuyu epohu // Trudy IGP RAN. - 2019. - T. 14. - № 3. – S. 122–146.

[10] SHinkareckaya G.G. Cifrovizaciya – global'nyj trend mirovoj ekonomiki // Obrazovanie i pravo. - 2019. - № 8. – S. 119–123.

[11] Regulation (EC) № 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act) // Official Journal of the European Union L 151 of 7 June 2019.

[12] Criminal Compliant // The United States Department of Justice. URL: https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/30/criminal_complaint_force.pdf (data obrashcheniya: 20.04.2020).

[13] National Cyber Strategy of the United States of America // The White House, September 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (data obrashcheniya: 20.04.2020).

[14] Akerman A., Gaarder I., Mogstad M. The Skill Complementarity of Broadband Internet // The Quarterly Journal of Economics. - 2015. - Vol. 130. - № 4. – P. 1781–1824.

[15] Black D., Bissessar Ch., Boolaky M. Online Education as an Opportunity Equalizer: The Changing Canvas of Online Education // Interchange. - 2019. - Vol. 50. - № 3. – P. 423 - 443.

[16] Cortez N. Patients Without Borders: The Emerging Global Market for Patients and the Evolution of Modern Health Care // Indian Law Journal. - 2008. - Vol. 83. – P. 71–113.

[17] Goos M., Manning A., Salomons A. Explaining Job Polarization: Routine Biased Technological Change and Offshoring // American Economic Review. - 2014. - Vol. 104. - № 8. – P. 2509–2526.

[18] Hollis D.B. Why States need an International Law for Information Operations // Lewis and Clark Law Review. - 2007. - Vol. 11. - № 4. – P. 1023–1061.

[19] Lee J., Long A., McRae M., Handler S. Bitcoin Basics: a Primer on Virtual Currencies // Business Law International. - 2015. - Vol. 16. - № 1. – P. 21.

[20] O'Connell M.E. Cyber Security without Cyber War // Journal of Conflict Security Law. - 2012. - Vol. 17. - № 2. – P. 187–209.

[21] Ronca M., Ross B., Dodd E. Digital justice: online learning beyond COVID-19 // UTS Centre for Social Justice & Inclusion Newsroom. URL: https://www.uts.edu.au/partners-and-community/initiatives/social-justice-uts/news/digital-justice-online-learning-beyond-covid-19 (data obrashcheniya: 20.04.2020).

[22] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd edition / ed. by M.N. Schmitt. CUP. - 2017. – P. 11–16.