www.volsu.ru

DOI: https://doi.org/10.15688/lc.jvolsu.2019.3.3

UDC 343
LBC 67.408

Submitted: 20.05.2019
Accepted: 18.06.2019

THE DIGITAL ECONOMY DEVELOPMENT OF THE RUSSIAN FEDERATION AND CRIMINAL LAW: TENDENCIES OF INTERACTION

Anna V. Denisova

University of the Prosecutor's Office of the Russian Federation, Moscow, Russian Federation

Introduction: all branches of law are constantly under the influence of the social environment, especially of the national policy and economy. In this regard, the author of the paper set the **aim** to research the influence of the processes of the digital economy development of the Russian Federation on the industry of Russian criminal law and to identify the relevant trends and relationships. **Methods:** the methodological framework for this study is a set of methods of scientific knowledge, among which the main ones are the methods of consistency, analysis and the comparative law method **Results:** grounded in the paper the author's point of view is based on the domestic and foreign legislation, international legal acts and opinions of the academic community on the problems of interaction of the economic and legal systems, processes and results of their mutual influence. Based on the analysis, a list of problems currently impeding the development of the digital economy of Russia, which can be resolved using the criminal law means, is revealed. The questions of the gap in the Russian criminal legislation concerning a number of socially dangerous acts committed with the use of modern information technologies are raised. **Conclusions:** the study revealed the importance of the intersystem links between the national economy and its digital sector with Russian criminal law, the need to take them into account in the law-making work and their impact on the effectiveness of the industry, the implementation of its sectoral goals and objectives. It is proposed to criminalize a number of socially dangerous acts committed with the use of modern information technologies, taking into account the traditions of the national law-making and the successful experience of the international community and a number of foreign countries in preventing attacks on the information security.

Key words: digital economy, intersystem links, economic criminal law, cybercrime, information economic crimes, criminal law provision of information security, criminalization of new types of socially dangerous acts.

Citation. Denisova A.V. The Digital Economy Development of the Russian Federation and Criminal Law: Tendencies of Interaction. *Legal Concept*, 2019, vol. 18, no. 3, pp. 18-25. (in Russian). DOI: https://doi.org/10.15688/lc.jvolsu.2019.3.3

УДК 343
ББК 67.408

Дата поступления статьи: 20.05.2019
Дата принятия статьи: 18.06.2019

РАЗВИТИЕ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ И УГОЛОВНОЕ ПРАВО: ТЕНДЕНЦИИ ВЗАИМОВЛИЯНИЯ

Анна Васильевна Денисова

Университет прокуратуры Российской Федерации, г. Москва, Российская Федерация

Введение: все отрасли права постоянно находятся под воздействием окружающей социальной среды, в особенности национальной политики и экономики, в связи с чем автором в работе поставлена цель исследования влияния процессов развития цифровой экономики Российской Федерации на отрасль российского уголовного права, выявления соответствующих тенденций и взаимосвязей. **Методы:** методологическую основу данного исследования составляет совокупность методов научного познания, среди которых основное место занимают методы системности, анализа и сравнительно-правовой. **Результаты:** обоснованная в работе авторская позиция опирается на отечественное и зарубежное законодательство, международно-правовые акты и мнения компетентной научной среды по проблемам взаимодействия экономической и правовой систем, процессов и результатов их взаимовлияния. На основании проведенного анализа выявляется пере-

© Денисова А.В., 2019

чень проблем, препятствующих в настоящее время развитию цифровой экономики России, которые могут быть разрешены с использованием уголовно-правовых средств. Поднимаются вопросы пробельности российского уголовного законодательства относительно ряда общественно опасных деяний, совершаемых с использованием современных информационных технологий. **Выводы:** в результате исследования выявлены важность межсистемных связей национальной экономики и ее цифрового сектора с российским уголовным правом, необходимость их учета в правотворческой работе и их влияние на эффективность действия отрасли, выполнение ею отраслевых целей и задач. Предложено криминализировать ряд общественно опасных деяний, совершаемых с использованием современных информационных технологий, с учетом традиций национального правотворчества и успешного опыта международного сообщества и ряда зарубежных стран в противодействии посягательствам на информационную безопасность.

Ключевые слова: цифровая экономика, межсистемные связи, экономическое уголовное право, киберпреступления,информационные экономические преступления, уголовно-правовое обеспечение информационной безопасности.

Цитирование. Денисова А. В. Развитие цифровой экономики Российской Федерации и уголовное право: тенденции взаимовлияния // Legal Concept = Правовая парадигма. – 2019. – Т. 18, № 3. – С. 18–25. – DOI: https://doi.org/10.15688/lc.jvolsu.2019.3.3

Введение

Общеизвестно, что право, являясь социальной подсистемой, постоянно испытывает на себе направляющее воздействие окружающей социальной среды, в особенности национальных политической и экономической систем. Если вспомнить основные постулаты теории К. Маркса, то право как часть политической надстройки имеет своим базисом экономику, и поэтому не может не ощущать на себе первоочередного влияния экономических процессов, происходящих в обществе. Все те же самые правила актуальны и для российского уголовного права: в литературе отмечается, что экономика, преступность, этнокультура, язык, юридическая практика, наука, политика, международные стандарты и пр. образуют так называемую внешнюю системную среду уголовного права, под которую последнее вынуждено подстраиваться в целях развития и решения социальных задач [1, с. 5]. Следовательно, содержание российского уголовного права напрямую или опосредованно зависит от состояния национальной экономики, направлений внешней и внутренней политики государства, от уровня правосознания населения, количественных и качественных характеристик преступности, правоохранительной деятельности, уровня развития юридической науки, нравственности и религии и т. д. То есть изучение межсистемных связей между уголовным правом и вышеназванными социальными явлениями позволит объяснить содержательно-структурные отраслевые модификации и даже в определенной степени управлять ими с учетом их зависимого поведения в социальной среде.

Впервые зависимости права от иных социальных явлений были замечены теоретиками права, которые отмечают, что право и его регулятивный потенциал зависят от состояния более широких сфер регулирования, частью которых они являются; в процессе регуляции внешняя среда подтягивает систему до своего уровня, не позволяет ей отставать в развитии, а тем более деградировать и распадаться [4, с. 8]. Более того, границы права, экономики и политики весьма условно проведены в современном социальном пространстве. Политика с давних времен пытается вмешиваться во все (подтверждение тому можно найти в виде многочисленных политически мотивированных, конъюнктурных изменений в законодательстве, в том числе уголовном), экономика тоже в последнее время стала присоединять к себе целые ареалы новых, ранее не относящихся к ней социальных отношений (в результате стали актуальны такие понятия как цена преступности, экономическое уголовное право, экономический анализ уголовного правотворчества, проблемы спроса на уголовное право, взаимодействие бизнеса и правоохранительных органов и т. д.). Соответственно, право тоже вынуждено вторгаться в общественные сферы, которые до последнего времени регулировались поверхностно или не регулировались вовсе. Все это свидетельствует о тесных связях и зависимостях между вышеуказанными социальными явлениями.

Влияние цифрового сектора национальной экономики на российское уголовное право

Безусловно, национальная политика является доминирующим, определяющим явлением в процессе уголовного правотворчества и правоприменения, опутывает отрасль права своими сильными и жесткими связями. Поэтому так важно на сегодняшний день учитывать ее приоритетные направления, связанные со все более активным внедрением информационных и коммуникационных технологий, развитием информационного общества в Российской Федерации и формированием национальной цифровой экономики [9].

Учитывая то обстоятельство, что уголовно-правовое регулирование является частью государственного управления, а отраслевые средства выступают инструментами управленческой деятельности государства, с которых возможно решение сложных оперативно-тактических и стратегических задач руководства обществом, не вызывает сомнений тот факт, что возможности отрасли уголовного права будут востребованы и при решении ряда злободневных проблем, препятствующих в настоящее время развитию цифровой экономики России. К таковым следует отнести проблемы обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом), сохранности цифровых данных пользователя, а также проблемы обеспечения доверия граждан к цифровой среде; рост масштабов компьютерной преступности, в том числе международной; новые угрозы личности, бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, широко использующих виртуализацию, удаленные (облачные) хранилища данных, а также разнородные технологии связи и оконечные устройства; наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру, в том числе на критическую информационную инфраструктуру. Часть этих проблем с очевидностью относятся к юрисдикции российского уголовного права и подлежат разрешению с использованием арсенала соответствующих отраслевых средств.

Но право (и уголовное право в частности) никогда не бывает всего лишь инструментом в руках государства, оно по сути должно нести некий «высший план» общественного развития, предначертанный правопорядок, по отношению к которому государство и его управление, в свою очередь, выступают в инструментальной роли. Управляющее воздействие на отрасль уголовного права развивает ее систему, поддерживает и оптимизирует системные характеристики отрасли, производит упорядочивающий в отношении нее эффект. Так, модернизация отечественной экономической системы остро поставила вопрос о совершенствовании мер по обеспечению информационной безопасности во всех секторах экономики. В 2017 г. при разработке проекта Программы «Цифровая экономика Российской Федерации» было опрошено существенное количество представителей российских компаний; по мнению двух третей опрошенных, количество преступлений в цифровой среде за 3 последних года возросло на 75 процентов, и оно будет только увеличиваться в связи с проводящейся цифровизацией экономики страны [6].

В связи с этим в Национальной программе «Цифровая экономика Российской Федерации» 2019 г. [5] акцентируются вопросы уголовно-правового обеспечения защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности в условиях цифровой экономики. В п. 1.17 указывается на необходимость криминализации новых типов общественно опасных деяний, совершенных с использованием современных информационных технологий; в п. 4.1 – необходимость определения на законодательном уровне состава сведений, составляющих банковскую тайну, тайну связи, врачебную тайну, коммерческую тайну и иные виды тайн, и порядка их передачи третьим лицам, что крайне важно для реализации на практике ряда статей Уголовного кодекса РФ (ст. 137, 138, 183 и пр.) и их предупредительного потенциала.

Исследование

Вышеуказанная обязанность по разработке проектов новых составов преступлений, совершаемых с использованием информаци-

онных технологий, возложена на Министерство внутренних дел РФ и подлежит исполнению в срок до 30 июня 2020 года. Представляется, что для успешного выполнения данного поручения было бы целесообразно обратиться к опыту зарубежных стран, в законодательстве которых так называемые информационные экономические преступления появились еще несколько десятилетий назад (например, в США Computer Fraud and Abuse Act был принят в 1984 г., в Великобритании Computer Misuse Act – в 1990 г.). Отметим, что в большинстве зарубежных стран, имеющих серьезный опыт противодействия «информационным экономическим преступлениям», криминализированы следующие виды общественно опасных деяний: незаконный доступ к компьютерной системе; незаконные действия, связанные с входом в части компьютерной системы или в компьютерную систему целиком без разрешения или правомерного основания; хакерство; незаконное вмешательство в компьютерную систему; незаконные действия, создающие препятствия для работы компьютерной системы; атака типа «отказ в обслуживании», повреждение компьютерной системы; незаконное вмешательство в компьютерные данные (действия, связанные с повреждением, удалением, ухудшением, изменением или блокировкой компьютерных данных без разрешения или основания; удаление файлов компьютерных систем без разрешения); незаконный перехват компьютерных данных или доступ к ним (незаконные действия, связанные с получением доступа к компьютерным данным без разрешения или основания, включая получение данных во время процесса передачи, которая не рассчитана на то, чтобы быть публичной, а также получение компьютерных данных (такое, как копирование данных) без разрешения); запись передачи данных без права на это в беспроводной сети; копирование компьютерных файлов без разрешения и др. [10].

Так, согласно статье 202 Уголовного кодекса Германии незаконное получение лицом компьютерных данных, которые предназначались не для него, находящихся под специальной защитой от неправомочного доступа, с целью извлечения выгоды для себя или для третьего лица влечет лишение свободы сроком до трех лет. Наказанию в виде штрафа или заключения сроком до двух лет подлежат стирание, уничтожение, приведение в негодность, изменение компьютерных данных или попытки произвести такие действия.

Пункт «b» статьи 303 этого же кодекса предусматривает ответственность за так называемые DNS-атаки (компьютерный саботаж) и создание вредоносных программ. Под компьютерным саботажем понимается вмешательство в обработку данных, которое может причинить существенный вред предприятию, государственному органу или ведению бизнеса. Соответствующее деяние может быть осуществлено путем уничтожения, повреждения, приведения в негодность, изменения компьютерной системы или вмешательства в передачу данных.

В Нидерландах криминализовано умышленное, с целью извлечения выгоды для себя или для третьего лица использование лицом технических устройств для перехвата или записи данных из телекоммуникационных систем или присоединенного оборудования, если данные не предназначаются только для соответствующего лица (статья 139c УК). Отдельный состав предусмотрен и для пособников данному преступлению – подлежат уголовной ответственности лица, снабжающие средствами для незаконного перехвата и записи данных, идущих по телекоммуникационным или автоматизированным системам (статья 139d). А также для лиц, прикосновенных к вышеуказанным преступлениям – а именно обладающих данными, о которых эти лица знают или должны знать, что они были получены в результате незаконного прослушивания, записи или перехвата данных автоматизированных систем или телекоммуникационных систем (статья 139e). Также к компьютерным преступлениям по голландскому законодательству относятся: несанкционированный доступ в компьютерные сети; несанкционированное копирование данных; компьютерный саботаж; распространение вирусов; компьютерный шпионаж. В ряд статей УК Голландии, предусматривающих ответственность за совершение «общеуголовных» преступлений (вымогательство, мошенничество, подлог и др.), были внесены дополнения и разъяснения, позволяющие использовать данные соста-

вы и для борьбы с компьютерными преступлениями.

При разработке новых составов преступлений, совершаемых с использованием современных информационных технологий, для нужд отечественного законодательства и правоприменения в первую очередь следует ориентироваться на нашу национальную правовую систему, особенности отечественной юридической техники, имеющиеся уголовно-правовые нормы и практику их применения. Однако игнорировать в сложившейся ситуации успешный опыт международного сообщества и ряда зарубежных стран в противодействии посягательствам на информационную безопасность представляется безрассудством и существенным упущением в борьбе с транснациональной киберпреступностью.

Результаты

Отметим, что в абсолютном большинстве случаев как в России, так и за рубежом «кибероружие» используется в сфере экономической деятельности хозяйствующих субъектов для извлечения материальной выгоды для злоумышленников или других лиц, либо для причинения имущественного вреда потерпевшим – добросовестным пользователям информационных и коммуникационных технологий. Учитывая также, что данные преступления не только опасны для граждан, общества, бизнеса и государства, но и подрывают инфраструктуру безопасности цифровой экономики России, представляется целесообразным отнести их к информационным экономическим преступлениям [7, с. 7]. Данная группа преступлений, находясь на стыке институтов экономических и компьютерных преступлений, безусловно, имеет непосредственное отношение к зарождающейся в системе российского уголовного права «молодой» подотрасли «экономического/хозяйственного уголовного права», призванной защитить инвестиции, кредитные отношения, потребительский рынок и снизить экономические издержки, делая рынок более эффективным [2, с. 961–969; 3, с. 48–58].

В идеалистической философии становление обычно рассматривается телеологически – как направленная реализация некоторой внутренней цели [11, с. 636]. Представляется, что становление подотрасли «экономического уголовного права» в российском уголовном праве обусловлено необходимостью реализации следующих целей – благотворное воздействие отрасли уголовного права на экономическое развитие страны, в том числе на развитие национальной цифровой экономики, создание благоприятных условий для честных участников рынка и минимизация рисков и угроз их информационной безопасности.

В настоящее время современная экономика находится под достаточно серьезным социальным контролем, представленным государством и осуществляемым с помощью правовых средств. Следовательно, право также имеет определенные возможности по влиянию на экономическую деятельность, воздействию на нее. Более того, не может быть эффективно функционирующей национальной экономики без эффективной уголовно-правовой охраны ее ключевых систем.

Любой социальный институт (в том числе и институты рыночной экономики) имеет в своем составе элемент из нормативного блока (нормы, правила, законодательство, ответственность и пр.). Эта составляющая, будучи ядром института, определяет его профиль, указывает на характер и пределы его действия [1, с. 22]. Представляется, что в каркас экономических институтов заложены не только гражданско-правовые нормы о них, но и уголовно-правовые нормы об их охране. Доказательством этому служит то обстоятельство, что одним из правомочий субъектов общественных отношений имущественной сферы является юридическая возможность защиты своих субъективных прав. Отрасль уголовного права предоставляет субъектам хозяйственной деятельности свои собственные отраслевые средства защиты и охраны. Более того, в специальной литературе отмечено, что многие болезни и перерождение экономических институтов начинаются с неполадок в их нормативном регулировании, из-за несовершенств законодательной основы [4, с. 449]. Наличие последних чревато для соответствующего института кризисом или даже развитием процессов его деградации, сопровождающихся утратой границ его возможных структурных и функциональных изменений, а в це-

лом – снижением значимости форм, которые делают институт определенным по предмету и действию.

Поэтому столь важно, чтобы изменения, вносимые в текст уголовного законодательства, имели бы, помимо всего прочего, и серьезное экономическое обоснование, которое не сводилось бы к констатации того, что реализация соответствующего законопроекта не повлечет за собой изменений финансовых обязательств государства и не потребует расходов, покрываемых за счет средств федерального бюджета. Представляется, что в финансово-экономическом обосновании к законопроекту об изменении УК РФ экспертам по экономическим вопросам необходимо указывать финансовую выгодность или невыгодность принятия данного акта, анализировать показатели возможных затрат и прибыли от него, устанавливать соотношение объемов финансового обеспечения и размеров экономических последствий от реализации закона (в том числе недопущенные потери в связи со своевременным пресечением насанкционированных вмешательств в управление межмашинным взаимодействием в области новейших технологий). Согласно разъяснениям Минфина России от 19 марта 2015 г., также необходимо указывать о влиянии предлагаемых решений на достижение целей государственных программ РФ, на вероятные поступления и уменьшение расходов (увеличение расходов) бюджетов бюджетной системы РФ, на вероятные доходы и расходы граждан и юридических лиц, сведения об иных социально-экономических последствиях, которыми, по нашему мнению, могут быть и обеспечение устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации на всех уровнях информационного пространства; обеспечение организационной и правовой защиты личности, бизнеса и государственных интересов при взаимодействиях в условиях цифровой экономики.

В Доктрине информационной безопасности Российской Федерации [8] указывается, что в настоящее время на территории России возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее. Кроме того, наблюдается увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры Российской Федерации, нарастают угрозы применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации. Поэтому в качестве одной из стратегических целей обеспечения информационной безопасности Российской Федерации указано повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям. Однако конкретные средства реализации данной цели нигде не указаны, и как их будет разрабатывать и внедрять ответственное ведомство (в данном случае – Министерство внутренних дел РФ), как это скажется на отрасли уголовного права в целом, – остается загадкой.

Государство, воплощая авторитет и власть, поддерживает стабильность различных динамичных систем ради общественных интересов, принимает ответственные решения по поводу управляемых им объектов через проводимую государственную политику. Правовое регулирование является частью государственного управления, но в то же время испытывает на себе управляющее воздействие со стороны государства. В идеале соответствующее воздействие на отрасль уголовного права должно ее развивать, поддерживать и оптимизировать системные характеристики отрасли, производить упорядочивающие в отношении нее эффекты. Однако на практике все не столь радужно, и управляющее воздействие со стороны государства иногда может, наоборот, «расшатывать» отраслевые системные характеристики, снижать их «коэффициент полезного действия». Когда по-

стоянно осуществляется внешнее воздействие на систему, на ее элементы, в систему привносится «внешняя» информация, подталкивающая ее к определенным изменениям, – в таких случаях обязательно в наличии должен быть некий план воздействия, чтобы реорганизовать систему таким образом, что в ней будут вызваны внутренние изменения, в наибольшей степени отвечающие ее связям с внешней средой. Поэтому столь важно не только описать в различных документах общими словами направления уголовной политики в области обеспечения информационной безопасности, а также указать на необходимость выработки каких-то абстрактных мер по совершенствованию системы уголовно-правового обеспечения информационной безопасности, но и предоставить конкретные ориентиры для соответствующей деятельности.

Выводы

Подытоживая все вышеизложенное, отметим, что российское уголовное право связано межсистемными взаимодействиями с иными социальными явлениями и процессами (политикой, экономикой, моралью, нравственностью и пр.). Данные связи имеют даже более важный характер, чем связи уголовного права с другими правовыми явлениями, ибо именно под их воздействием происходит существенное обновление отрасли, постоянно находящейся под внешним воздействием. Во-вторых, особое значение имеют связи российского уголовного права с экономикой, ибо они формируют синергетичность отрасли права, обеспечивают ее адаптивность и в то же время – гомеостатичность, поддерживают ее открытое состояние, способность обмениваться с внешней средой информацией, «взаимными сигналами». В-третьих, качество связей российского уголовного права с национальной экономикой, особенностями ее развития на современном этапе и их учет в процессе реформирования законодательства – это не только важное условие обеспечения эффективности отрасли уголовного права, но и в то же самое время необходимое условие для достижения состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, суверенитет и устойчивое социально-экономическое развитие Российской Федерации в условиях цифровой экономики.

СПИСОК ЛИТЕРАТУРЫ

1. Бойко, А. И. Системная среда уголовного права : автореф. дис. ... д-ра юрид. наук / Бойко Александр Иванович. – М., 2008. – 49 с.

2. Есаков, Г. А. Экономическое уголовное право: понятие, содержание и перспективы / Г. А. Есаков // Lex Russica. – 2013. – № 9. – С. 961–969.

3. Клепицкий, И. А. Экономика и уголовное право / И. А. Клепицкий // Закон. – 2013. – № 8. – С. 48–58.

4. Мальцев, Г. В. Социальные основания права / Г. В. Мальцев. – М. : Норма, 2014. – 800 с.

5. Паспорт национального проекта Национальная программа «Цифровая экономика Российской Федерации» : (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). – Электрон. дан. – Режим доступа: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (дата обращения: 07.07.2019).

6. Распоряжение Правительства РФ от 28 июля 2017 года № 1632-р «Об утверждении Программы “Цифровая экономика Российской Федерации”» (утратило силу) // Собрание законодательства РФ. – 2017. – № 32. – Ст. 5138.

7. Турышев, А. А. Информация как признак преступлений в сфере экономической деятельности : автореф. дис. ... канд. юрид. наук / Турышев Александр Александрович. – Омск, 2006. – 23 с.

8. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016. – № 50. – Ст. 7074.

9. Указ Президента РФ от 09 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства РФ. – 2017. – № 20. – Ст. 2901.

10. УНП ООН. Международная классификация преступлений для статистических целей: Вариант 1.0. – Вена : United Nations Office on Drugs and Crime, 2015. – 157 с.

11. Философский энциклопедический словарь. – М. : Сов. энцикл., 1983. – 840 с.

REFERENCES

1. Boyko A.I. *Sistemnaya sreda ugolovnogo prava: avtoref. dis. ... d-ra yurid. nauk* [The System Environment of Criminal Law. Cand. jurid. sci. abs. diss.]. Moscow, 2008. 49 p.

2. Esakov G.A. Ekonomicheskoe ugolovnoe pravo: ponyatie, soderzhanie i perspektivy [Economic Criminal Law: Concept, Content and Prospects]. *Lex Russica*, 2013, no. 9, pp. 961-969.

3. Klepitskiy I.A. Ekonomika i ugolovnoe pravo [Economics and Criminal Law]. *Zakon* [Law], 2013, no. 8, pp. 48-58.

4. Maltsev G.V. *Sotsialnye osnovaniya prava* [Social Foundations of Law]. Moscow, Norma Publ., 2014. 800 p.

5. *Pasport natsionalnogo proekta Natsionalnaya programma «Tsyfrovaya ekonomika Rossiyskoy Federatsii»: (utv. prezidiumom Soveta pri Prezidente RF po strategicheskomu razvitiyu i natsionalnym proektam, protokol ot 04.06.2019 № 7)* [Passport of the National Project The National Program "Digital Economy of the Russian Federation" (approved by the Presidium of the Presidential Council for Strategic Development and National Projects under the President of the Russian Federation, Minutes No. 7 of June 4, 2019)]. URL: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii__NcN2nOO.pdf (accessed 7 July 2019).

6. Rasporyazhenie Pravitelstva RF ot 28 iyulya 2017 goda № 1632-r «Ob utverzhdenii Programmy "Tsifrovaya ekonomika Rossiyskoy Federatsii"» (utratilo silu) [Order of the Government of the Russian Federation dated July 28, 2017 No. 1632-p "On Approval of the Program" Digital Economy of the Russian Federation "(invalid))]. *Sobranie zakonodatelstva RF* [Collected Legislation of the Russian Federation], 2017, no. 32, art. 5138.

7. Turyshev A.A. *Informatsiya kak priznak prestupleniy v sfere ekonomicheskoy deyatelnosti: avtoref. dis. ... kand. yurid. nauk* [Information as a Sign of Crimes in the Sphere of Economic Activity. Cand. jurid. sci. diss.]. Omsk, 2006. 23 p.

8. Ukaz Prezidenta Rossiyskoy Federatsii ot 5 dekabrya 2016 g. № 646 «Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii» [Decree of the President of the Russian Federation dated December 5, 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation"]. *Sobranie zakonodatelstva RF* [Collected Legislation of the Russian Federation], 2016, no. 50, art. 7074.

9. Ukaz Prezidenta RF ot 09 maya 2017 g. № 203 «O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody» [Presidential Decree of May 9, 2017 No. 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030"]. *Sobranie zakonodatelstva RF* [Collected Legislation of the Russian Federation], 2017, no. 20, art. 2901.

10. *UNP OON. Mezhdunarodnaya klassifikatsiya prestupleniy dlya statisticheskikh tseley: Variant 1.0* [UNODC. International Classification of Crimes for Statistical Purposes: Option 1.0]. Vienna, United Nations Office on Drugs and Crime, 2015. 157 p.

11. *Filosofskiy entsyklopedicheskiy slovar* [Philosophical Encyclopedic Dictionary]. Moscow, Sov. Entsyklopediya Publ., 1983. 840 p.

Information about the Author

Anna V. Denisova, Doctor of Sciences (Jurisprudence), Associate Professor, Chief Researcher, Department of Prosecutorial Supervision Problems and Consolidation of Legality in Criminal Law Regulation, Execution of Criminal Penalties and Other Criminal Law Measures, University of the Prosecutor's Office of the Russian Federation, 2-ya Zvenigorodskaya St., 15, 123002 Moscow, Russian Federation, anden2012@yandex.ru, nii@agprf.org, https://orcid.org/0000-0003-1193-272X

Информация об авторе

Анна Васильевна Денисова, доктор юридических наук, доцент, главный научный сотрудник отдела проблем прокурорского надзора и укрепления законности в сфере уголовно-правового регулирования, исполнения уголовных наказаний и иных мер уголовно-правового характера, Университет прокуратуры Российской Федерации, ул. 2-я Звенигородская, 15, 123002 г. Москва, Российская Федерация, anden2012@yandex.ru, nii@agprf.org, https://orcid.org/0000-0003-1193-272X