ЛОГИКО-ЯЗЫКОВЫЕ ФЕНОМЕНЫ ПРЕДМЕТА НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИИ (ст. 274[1] УК РФ)

ПЫХТИН
Иван Геннадьевич
аспирант кафедры уголовного права Юго-Западного государственного университета (г. Курск)
abcqip@gmail.com

https://doi.org/10.33874/2072-9936-2021-0-1-118-124

Настоящая статья посвящена проблеме правопонимания основных логико-языковых феноменов, входящих в предмет неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации и закрепленных в ст. 274[1] Уголовного кодекса РФ. Показана сложность юридико-технической конструкции ч. 1–3 уголовно-правовой нормы, предусматривающей ответственность и наказание за неправомерное посягательство на важнейшие объекты информационной инфраструктуры страны. Отмечается, что комбинационность в рассматриваемой статье УК РФ характерна для конструкции ее первых трех частей, диспозиции которых имеют такие отличительные черты, которые позволяют сделать вывод о том, что ст. 274[1] УК РФ содержит три совершенно автономных друг от друга состава преступления, которые могут квалифицироваться отдельно как единичные преступления или по совокупности. Проведенный в рамках настоящей статьи анализ показал, что ч. 1–3 ст. 274[1] УК РФ практически полностью повторяют логико-языковые конструкции диспозиций ст. 272–274 УК РФ лишь с той разницей, что в ст. 274[1] УК РФ объективные и субъективные признаки «увязаны» с критической информационной инфраструктурой России. В статье отмечается, что логико-языковые феномены, сами выступая в качестве различных видов информации, не дают достаточного теоретического понимания определению «компьютерная информация» в критической информационной инфраструктуре. В частности, «компьютерная информация» как предмет преступления, предусмотренный ст. 274[1] УК РФ, нуждается в теоретическом обосновании своей материальной природы как вещи, материальной субстанции, которая является признаком предмета любого общественно опасного деяния. Предметом настоящего исследования являются законодательное определение и доктринальное обоснование «компьютерной информации» (и связанных с ним логико-языковых феноменов) как специфического предмета материального мира и, следовательно, предмета преступления, определяющего незаконное воздействие на общественные отношения в сфере критической информационной инфраструктуры Российской Федерации. Цель статьи состоит в выявлении проблемных аспектов технико-юридической архитектуры ст. 274[1] УК РФ и содержания понятия «компьютерная информация», аккумулирующей в своих значениях предмет состава неправомерного воздействия на критическую информационную инфраструктуру страны. В процессе работы над темой были использованы технико-юридический и логические методы, позволяющие объяснить и доказать правильность выбора законодателем специфической конструкции состава преступления, закрепленного в ст. 274[1] УК РФ. Применение диалектического, грамматического и технического методов позволили определить «материальную» суть «компьютерной информации» как вещи, которая в настоящее время обладает ценой, а также может покупаться и продаваться. Проведенное автором исследование позволило определить основные проблемы, связанные с конструкцией ст. 274[1] УК РФ и ее триединым содержанием, в целом отражающим неправомерность воздействия на критическую информационную инфраструктуру России в ч. 1–3 указанной уголовно-правовой нормы; изучить основные позиции теоретиков уголовного права о возможности рассматривать компьютерную информацию как предмет компьютерного преступления и сделать собственный вывод о специфической материальности компьютерной информации как вещи внешнего мира, аккумулирующей в своих значениях предмет состава неправомерного воздействия на критическую информационную инфраструктуру страны.

Компьютерная информация; критическая информационная инфраструктура; законодательная архитектура; неправомерное воздействие; защита информации; обеспечение безопасности; информационные технологии; состав преступления; предмет преступления

Ivan G. PYKHTIN
Postgraduate Student, Department of Criminal Law, South-West State University (Kursk)
abcqip@gmail.com

LOGIC-LANGUAGE PHENOMENA OF THE SUBJECT OF INCORRECT IMPACT ON THE CRITICAL INFRASTRUCTURE OF RUSSIA (ARTICLE 274[1] OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)

Computer information; critical information infrastructure; legislative architecture; unlawful influence; information protection; security; information technology; *corpus delicti*; subject of crime

This article is devoted to the problem of legal understanding of the main logical-linguistic phenomena included in the architecture of the composition of the unlawful impact on the critical information infrastructure of the Russian Federation and enshrined in Art. 274[1] of the Criminal Code of the Russian Federation. The complexity of the legal and technical design of parts 1–3 of the criminal law norm stipulating responsibility and punishment for unlawful encroachment on the most important objects of the country's information infrastructure, as well as those concepts of disposition that relate to the subject of the crime, is shown. It is noted that the combination in the article under review is also characteristic of the design of its first three parts, the dispositions of which have such distinctive features that allow us to conclude that Art. 274[1] of the Criminal Code of the Russian Federation contains three completely autonomous from each other corpus delicti, which can be qualified separately as single crimes or in aggregate. The analysis carried out within the framework of this article also showed that parts 1–3 of the Art. 274[1] of the Criminal Code of the Russian Federation almost completely repeat the logical-language constructions of the dispositions of Arts. 272–274 of the Criminal Code of the Russian Federation only with the difference that in Art. 274[1] of the Criminal Code of the Russian Federation, objective and subjective attributes are "linked" to the critical information infrastructure of Russia. The article notes that logical-language phenomena, acting as various types of information themselves, do not provide a sufficient theoretical understanding of the definition of "computer information" in a critical information infrastructure. In particular, "computer information" as a subject of a crime under Art. 274[1] of the Criminal Code of the Russian Federation needs a theoretical justification of its material nature as a thing, material substance, which is a sign of the subject of any socially dangerous act. The subject of this study is the legislative definition and doctrinal justification of "computer information" as a specific subject of the material world and, consequently, the subject of a crime that determines the illegal impact on public relations in the field of critical information infrastructure of the Russian Federation. The purpose of the article is to identify the problematic aspects of the technical and legal architecture of Art. 274[1] of the Criminal Code of the Russian Federation and the content of the concept of "computer information" accumulating in its meanings the subject of the composition of the unlawful impact on the critical information infrastructure of the country. In the process of working on the topic, technical, legal and logical methods were used to explain and prove the correctness of the legislator's choice of the specific design of the "cuticle" of the corpus delicti, as enshrined in Art. 274[1] of the Criminal Code of the Russian Federation. The use of dialectical, grammatical and technical methods of interpretation made it possible to define the "materialistic" essence of "computer information" as things that currently have a price and can also be bought and sold. A study conducted by the author, allowed to identify the main problems associated with the construction of Art. 274[1] of the Criminal Code of the Russian Federation and its triune content, which generally reflects the unlawfulness of the impact on the critical information infrastructure of Russia in parts 1–3 of the desired criminal law norm, to study the main positions of theorists of criminal law on the possibility of considering computer information as a subject of computer crime and drawing its own conclusion about the specific materiality of computer information as a thing of the outside world accumulating in its meanings the subject of a composition of unlawful influence on the country's critical information infrastructure.

Уголовно-правовая защита наиболее значимых объектов информационной инфраструктуры России от общественно опасных посягательств осуществляется с помощью ст. 274[1] Уголовного кодекса РФ (далее – УК РФ), предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру страны [1]. Данная норма состоит из пяти частей. Анализ диспозиций ч. 1–3 показывают, что они представлены различными, не похожими друг на друга составами преступлений бланкетного характера, предусматривающими меры уголовной репрессии за: создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ч. 1 ст. 274[1] УК РФ); неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре России (ч. 2 ст. 274[1] УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 3 ст. 274[1] УК РФ). Иными словами, мы имеем дело с триединым составом преступления; каждый из образующих его составов может выступать и квалифицироваться отдельно либо они могут рассматриваться совокупно.

Квалифицированные составы анализируемой уголовно-правовой нормы представлены традиционными для российского уголовного законодательства квалифицирующими обстоятельствами: совершение преступных деяний группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения (ч. 4) и если они повлекли тяжкие последствия (ч. 5). Квалифицирующие признаки ст. 274[1] УК РФ, в свою очередь, являются средством дифференциации уголовной ответственности в системе преступлений в сфере компьютерной информации (гл. 28 УК РФ).

В целом же ст. 274[1] УК РФ определяется уголовно-правовая охрана критической информационной инфраструктуры в широком смысле, которая выражается в привлечении виновных лиц к уголовной ответственности и назначении им наказания за неправомерное воздействие на охраняемую компьютерную информацию, объекты информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов критической информационной инфраструктуры, а также на сети электросвязи, используемые для организации взаимодействия таких особо значимых объектов.

Кроме того, установлено, что признаки состава неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК РФ) по своим характеристикам практически соответствует тем признакам, которые мы обнаруживаем в трех различных составах преступлений, предполагающих уголовную ответственность за преступления в сфере компьютерной информации, – ст. 272–274 УК РФ. Особенностью ч. 1–3 ст. 274[1] УК РФ, отграничивающей их от вышеуказанных норм уголовного закона, является существенное различие в предмете преступления. В первом случае им будет являться компьютерная информация, содержащаяся в критической информационной инфраструктуре России, а во втором – компьютерная информация безотносительно к субъекту владения ею и места ее расположения. Таким образом, ст. 274[1] УК РФ по отношению к ст. 272–274 УК РФ рассматривается как специальная норма.

Большинство языковых объектов, содержащихся в описании той или иной формы неправомерного воздействия на критическую информационную инфраструктуру, являются оценочными, достаточно сложными для понимания и не отражают завершенности в определении всех признаков преступного деяния.

На бланкетный характер ч. 1–3 ст. 274[1] УК РФ указывает описание элементов составов преступления обобщающими признаками-понятиями, в первую очередь такими как «компьютерная информация», «критическая информационная инфраструктура», и понятиями, которые содержатся в нормативно-правовых актах, непосредственно регулирующих отношения в области защиты информации, информационных технологий и обеспечения безопасности критической информационной инфраструктуры [2; 3]. Иными словами, законодательное формулирование в ст. 274[1] УК РФ объектов критической информационной инфраструктуры достаточно объемное, и, кроме самой критической информационной инфраструктуры (которая состоит из значимых объектов инфраструктуры страны), уголовно-правовая норма перечисляет некий инженерно-технологический комплекс, включающий в себя средства защиты, хранилища информации, электрические сети и др., используемые для организации взаимодействия (и управления) значимых объектов [3]. Значимыми объекты информационной инфраструктуры становятся после их категорирования в зависимости от социальной, политической, экономической, оборонной, правоохранительной и иной важности для Российской Федерации.

Действующая редакция ст. 274[1] УК РФ не учитывает подобной категоризации значимых объектов, что представляется существенным упущением с точки зрения дифференциации уголовной ответственности.

Все вышеперечисленные логико-языковые феномены технической группы материальны и претендуют на роль предмета преступления в архитектуре

состава преступления, предусмотренного ст. 274[1] УК РФ. Поэтому вполне логично, что большинство ученых констатируют, что единообразного нормативно-правового и теоретического понимания предмета рассматриваемого преступного деяния и логико-языковых феноменов, составляющих правовую конструкцию ст. 274[1] УК РФ, на сегодняшний день не существует [4, с. 26; 5, с. 154; 6, с. 206]. По мнению исследователей проблем неправомерного воздействия на критическую информационную инфраструктуру, подобное обстоятельство не способствует пониманию законодательной мысли и правильной квалификации преступлений, связанных с общественно опасным воздействием на информационную инфраструктуру [7, с. 42–46].

На наш взгляд, использование бланкетных признаков в диспозиции ст. 274[1] УК РФ, в том числе подпадающих по формальным характеристикам под определение предмета преступления, создает коллизию и затрудняет возможности отграничения от смежных составов преступлений. Разрешение такой коллизии на начальном этапе применения анализируемой статьи УК РФ в части всего того, что связано с предметом преступления, нуждается в теоретических разъяснениях и толковании с последующим устранением выявленных недостатков законодательной техники при построении уголовно-правовой нормы.

«Компьютерная информация» как предмет преступления не совпадает с классическим понятием «предмета преступления» как материальной субстанции внешнего мира. Никакая иная его причастность и принадлежность к теории уголовного права не рассматривалась до тех пор, пока «информация» и ее виды не стали объектами общественных отношений и «предметом» преступных посягательств. Между тем в современном мире компьютерная информация, разноаспектная по своей сути, в известной мере является составной частью общества, государства и различных субъектов управления информационной инфраструктурой.

В дискуссиях по вопросам содержания и овеществления компьютерной информации (как предмета преступления) ученые принципиально соглашаются с тем, что у различных видов информации наличествует существенное сходство, например, между лексическими символами, фиксируемыми в текстах, и комбинациями двоичных цифр (0 и 1) в программах для ЭВМ, а также между последовательной работой над лексемами формального языка с его формальной грамматикой и разработкой компьютерных программ, основанных на комбинациях двоичных цифр (0 и 1), впоследствии выступающих в качестве «компьютерного языка» [8, с. 48; 9, с. 30]. В том и другом случае в итоге возникают структуры данных или сведений, удобных для последующей обработки (например, в виде синтаксического дерева или компьютерной информации).

Уголовно-правовое содержание компьютерной информации раскрывается в прим. 1 к ст. 272 УК РФ и касается всех норм главы о преступлениях в сфере компьютерной информации. В примечании определено, что указанный вид информации есть сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Такое определение согласовывается с общим легальным понятием «информация», не противоречит ему, одновременно уточняет формы ее представления, однако не перечисляет средства ее хранения, обработки и передачи, по сути оставляя перечень таких средств открытым [2]. Последнее, на наш взгляд, связано с тем, что средства хранения, обработки и передачи компьютерной информации формируются, совершенствуются и постоянно развиваются. Например, такому прогрессу могут быть подвержены средства блокирования, переформатирования, поиска или извлечения информации. Кроме того, их эволюция не исключает поступательные движения по отдельным векторным процессам и направлениям как научно-прикладного знания, так и унифицированного совершенствования.

Развернувшаяся в науке уголовного права дискуссия касательно материальности/нематериальности компьютерной информации, а также возможности либо невозможности считать ее предметом в составах преступлений в сфере компьютерной информации сводится к двум аспектам и, соответственно, к двум основным позициям специалистов. Первая позиция отражает мнение тех ученых, которые приводят свои аргументы в пользу того, что компьютерная информация, имея нематериальный характер, тем не менее может считаться предметом всех тех преступлений, которые закреплены в гл. 28 УК РФ (ст. 272–274[1]) [10, с. 28]. Другой точки зрения придерживаются те ученые, которые полагают, что компьютерная информация и информация в любом ее проявлении не может быть предметом преступления в силу того, что она не материализована в качестве вещи, что считается безусловным условием общественно опасного деяния [11, с. 114].

Объективный анализ уголовного закона показывает, что виртуальный характер той или иной информации давно наличествует в нормах российского уголовного закона. В ряде составов преступления для квалификации имеет значение именно информация, содержание которой определяется какими-либо сведениями, определяющими конкретный состав преступления (например, клевета, нарушение неприкосновенности частной жизни, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну). Однако и при том, и при другом подходе ученые столкнулись с про-

блемой признаков, которые в полной мере отражали бы определение (понятие) предмета преступления в сфере компьютерной информации. Исследователи, усматривающие материальную природу в предмете преступления в сфере компьютерной информации, исходят из того, что материальность компьютерной информации выражена в вариативной «двоичной цифре», в связи с чем, во-первых, правильнее было бы именовать предмет рассматриваемого преступления как «цифровая информация», а во-вторых, поскольку вариативный двоичный код компьютерной программы (0 и 1) в совокупности является не чем иным, как сосредоточением лексических данных, то материальный носитель программного обеспечения ЭВМ (на котором фиксируются информационные данные) будет считаться вещественной оболочкой информации, формой компьютерной информации, и таким образом последняя приобретает материальное, вещественное выражение [12, с. 40].

Соглашаясь в целом с материальной сущностью «компьютерной информации», мы хотели бы уточнить и обосновать некоторые аспекты указанных свойств-признаков компьютерной информации.

Первое. Мы исходим из того, что конструирование того или иного научного понятия должно основываться на определенной философской концепции (материалистическая, идеалистическая или дуалистическая либо иные нетрадиционные, но научно обоснованные взгляды). При рассмотрении сущности компьютерной информации полагаем, что речь идет о «виртуализированных сведениях», понимание которых одновременно «наполнено объективным и субъективным содержанием, зависящим от современных и последующих временных философских подходов, а также научно-технических преобразований» [13, с. 46]. Из сказанного следует, что понятие «компьютерная информация» должно наполняться не только материалистическим содержанием, но и идеалистическим (субъективным смыслом), подобным архитектуре понятия «состав преступления» (совокупность объективных и субъективных признаков).

Второе. Известно, что в термодинамическом смысле информация формально образуется в результате атомно-молекулярных, химико-физических процессов, происходящих в головном мозге человека (энтропией). Для того чтобы привести оба понятия к одной форме, информацию измеряют так же, как и энтропию, но только со знаком «минус». Следовательно, формально мы можем идентифицировать информацию как специфическую физическую субстанцию (гипотетические частицы – «психоны» [14, с. 146]), которая применительно к нашим рассуждениям может быть предметом преступления.

Третье. Юридический анализ понятия «компьютерная информация» обнаруживает наличие тех признаков, которые относятся к основным признакам «вещи» (предмета), например: а) *ее полезности* (*a priori* или по умолчанию) и *принадлежности* компьютерной информации конкретному физическому либо юридическому лицу (субъекту); б) *востребованности, оборотоспособности*; в) *материальности* (компьютерная информация, как и любая вещь, имеет финансовую и материальную ценность). Иными словами, компьютерную информацию можно продать, купить, обменять, использовать для изменения материальных свойств того или иного предмета материального мира, извлекать из нее ценностные свойства и т.п.

Обозначенные проблемы логико-языковых феноменов, составляющих содержание гипотезы ст. 274[1] УК РФ, конечно, не могут претендовать на доскональный юридический анализ и всестороннее освещение проблемы правотворческих ошибок, допущенных законодателем в ходе юридико-технической работы над уголовно-правовой нормой, предусматривающей уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру России. Мы обращаем внимание лишь на некоторые из проблем, касающихся логико-языковых феноменов и предмета преступления в ст. 274[1] УК РФ. Вместе с тем должно быть очевидно, что практическая реализация защиты критической информационной инфраструктуры способна объективно снизить безопасность как компьютерной информации, так и охраняемого значимого объекта инфраструктуры, где информация служит целям эффективного управления функционированием объекта. Одновременно проблемы логико-языковых феноменов способны породить серьезные проблемы, например, с квалификацией преступлений.

Один из способов решения указанной проблемы видится в раскрытии содержания логико-языковых феноменов и связанных с ними оценочных понятий Верховным Судом РФ, который давал бы разъяснения и толкование технических терминов, перечня значимых объектов инфраструктуры и др. – всего того, что поможет правоприменителю правильно понимать смысл правового установления, закрепленного в ст. 274[1] УК РФ.

Пристатейный библиографический список

1. Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»» // СЗ РФ. 2017. № 31 (ч. 1). Ст. 4743.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 3 апреля 2020 г.) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3448.

3. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (ч. 1). Ст. 4736.

4. *Кучина Я. О.* Квалификация преступлений, предусмотренных статьей 272 Уголовного кодекса Российской Федерации // Академический юридический журнал. 2019. № 2 (76).

5. *Стяжкина С. А.* Информация как объект уголовно-правовой охраны: понятие, признаки, виды // Вестник Удмуртского университета. 2015. № 25. Вып. 2.

6. *Нажимов М. Ш.* Понятие и виды компьютерной информации как доказательства в криминальном процессе // Образование и наука в России и за рубежом. 2020. Т. 66. № 2.

7. *Евдокимов К. Н.* Вопросы уголовно-правовой квалификации неправомерного доступа к компьютерной информации и его отграничения от смежных составов преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. 2009. № 2 (10).

8. *Кагиров И. А., Леонтьева А. Б.* Автоматический синтаксический анализ русских текстов на основе грамматики составляющих // Известия высших учебных заведений. Приборостроение. 2008. Т. 51. № 11.

9. *Ромашов Р. А., Панченко В. Ю.* О соотношении материального и виртуального в современной правовой реальности // Юридическая наука. 2017. № 1.

10. *Ястребов Д. А.* Международно-правовое сотрудничество государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Юридический мир. 2008. № 12.

11. *Хилюта В. В.* Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014 № 3.

12. *Бегишев И. Р., Бикеев И. И.* Преступления в сфере обращения цифровой информации. Казань : Изд-во «Познание» Казанского инновационного университета, 2020.

13. *Новичков В. Е.* Прогнозирование социально-правовых аспектов борьбы с преступностью (проблемы теории и практики) : монография. Курск : Курск. гос. техн. ун-т, 2004.

14. *Кобозев Н. И.* Исследования в области термодинамики процессов информации и мышления. М. : Изд-во МГУ, 1971.

References

1. Federal Law of 26 July 2017 No. 194-FZ "On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Criminal Procedure Code of the Russian Federation in Connection with the Adoption of the Federal Law 'On the Security of Critical Information Infrastructure of the Russian Federation'". *Collection of the Legislation of the Russian Federation*. 2017. No. 31 (part 1). Art. 4743.

2. Federal Law of 27 July 2006 No. 149-FZ (as amended on 3 April 2020) "On Information, Information Technologies and the Protection of Information". *Collection of the Legislation of the Russian Federation*. 2006. No. 31 (part 1). Art. 3448.

3. Federal Law of 26 July 2017 No. 187-FZ "On the Security of Critical Information Infrastructure of the Russian Federation". *Collection of the Legislation of the Russian Federation*. 2017. No. 31 (part 1). Art. 4736.

4. *Kuchina Ia. O.* Qualification of Crimes Provided for in Article 272 of the Criminal Code of the Russian Federation. *Academic Law Journal*. 2019. No. 2 (76).

5. *Stiazhkina S. A.* Information as an Object of Criminal Law Protection: Concept, Features, Types. *Bulletin of Udmurt University*. 2015. No. 25. Iss. 2.

6. *Nazhimov M. Sh.* The Concept and Types of Computer Information as Evidence in the Criminal Process. *Education and Science in Russia and Abroad*. 2020. Vol. 66. No. 2.

7. *Evdokimov K. N.* Issues of Criminal Legal Qualification of Unlawful Access to Computer Information and its Delimitation from Related Offenses. *Bulletin of the Academy of the General Prosecutor of the Russian Federation*. 2009. No. 2 (10).

8. *Kagirov I. A., Leontiev A. B.* Automatic Syntactic Analysis of Russian Texts Based on the Grammar of the Components. *Proceedings of Higher Educational Institutions. Instrument Making*. 2008. Vol. 51. No. 11.

9. *Romashov R. A., Panchenko V. Iu.* On the Relationship of Material and Virtual in Modern Legal Reality. *Legal Science*. 2017. No. 1.

10. *Iastrebov D. A.* International Legal Cooperation of the Member States of the Commonwealth of Independent States in the Fight Against Crimes in the Field of Computer Information. *Legal World*. 2008. No. 12.

11. *Khiliuta V. V.* Criminal Liability for Theft with the Use of Computer Technology. *Journal of Russian Law*. 2014. No. 3.

12. *Begishev I. R., Bikeev I. I.* Crimes in the Field of the Circulation of Digital Information. Kazan: Publishing House "Knowledge" of Kazan Innovation University, 2020.

13. *Novichkov V. E.* Prediction of Socio-Legal Aspects of the Fight Against Crime (Problems of Theory and Practice): Monograph. Kursk: Kursk State Technical University, 2004.

14. *Kobozev N. I.* Research in the Field of Thermodynamics of Information and Thinking Processes. Moscow: MSU Publishing House, 1971.