

Научная статья
УДК 343.3/.7
DOI: 10.47475/2311-696X-2024-43-4-122-128

С. 122–128

ПОНЯТИЕ, СИСТЕМА И ПРИЗНАКИ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ

Альбина Александровна Шутова

Казанский инновационный университет им. В. Г. Тимирязова, Казань, Россия
shutova1993@inbox.ru

 <https://orcid.org/0000-0003-3015-3684>

Аннотация. В последнее время авторы достаточно мало уделяют внимание междисциплинарным подходам, в особенности таким разным направлениям, как технологии и право. Однако выявление закономерностей без всестороннего подхода видится малоперспективным, поскольку не позволит увидеть природу происходящих процессов, а в частности — понять природу преступности. Изучение цифровых преступлений, их специфики, признаков и системы является важным направлением в области уголовно-правовой доктрины в свете форсированной цифровизации и процессов, порождаемых ею. На данный момент в теории не выработано единообразное понимание сущности цифровых уголовно наказуемых деяний, выявлено то, что подходы авторов весьма разнообразны, что не вносит ясности в их уголовно-правовую оценку и в целом оказывает негативное влияние на правоприменение. В статье предпринята попытка критического анализа большинства имеющихся точек зрения авторов отечественной и зарубежной доктрины относительно понимания цифровых преступлений и их признаков. В результате проведенного исследования и с учетом изучения сущности цифровых технологий, их специфики и влияния на преступность, а также непосредственно такого явления, как цифровизация, сформулирован авторский подход к их дефинированию и формированию их системы. Введение в уголовно-правовую доктрину термина «цифровое преступление» является безусловно нужным и советующим современным реалиям.

Ключевые слова: цифровые преступления, преступления против цифровой безопасности, цифровые технологии, цифровая информация, уголовно-правовая охрана, высокотехнологичные преступления


Для цитирования: Шутова А. А. Понятие, структура и признаки цифровых преступлений // Правопорядок: история, теория, практика. 2024. № 4 (43). С. 122–128. DOI: 10.47475/2311-696X-2024-43-4-122-128

Research article

CONCEPT, SYSTEM AND SIGNS OF DIGITAL CRIMES

Albina A. Shutova

Kazan Innovation University named after V. G. Timiryasova, Kazan, Russia
shutova1993@inbox.ru

 <https://orcid.org/0000-0003-3015-3684>

Abstract. Recently, authors have paid little attention to interdisciplinary approaches, especially to such different areas as technology and law. However, identifying patterns without a comprehensive approach seems unpromising, since it will not allow us to see the nature of the processes taking place, and in particular, to understand the nature of crime. The study of digital crimes, their specifics, features and system is an important area in the field of criminal law doctrine in light of accelerated digitalization and the processes generated by it. At the moment, the theory has not developed a uniform understanding of the essence of digital criminal offenses, it has been revealed that the approaches of the authors are very diverse, which does not clarify their criminal law assessment and generally has a negative impact on law enforcement. The article attempts to critically analyze most of the existing points of view of the authors of domestic and foreign doctrine regarding the understanding of digital crimes and their features. As a result of the conducted research and taking into account the study of the essence of digital technologies, their specificity and impact on crime, as well as such a phenomenon as digitalization itself, the author's approach to their definition and formation of their system has been formulated. The introduction of the term "digital crime" into the criminal law doctrine is certainly necessary and appropriate to modern realities.

Keywords: digital crimes, crimes against digital security, digital technologies, digital information, criminal law protection, high-tech crimes

For citation: Shutova AA. Concept, system and signs of digital crimes. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(4):122-128. (In Russ.) DOI: 10.47475/2311-696X-2024-43-2-122-128

Введение

Обеспечение цифровой безопасности системы здравоохранения требует многостороннего и междисциплинарного подходов, синхронно сочетающих медицину, цифровые технологии и право, в том числе уголовное. Исследуемые общественные отношения складываются в новых областях медицины, основанных на фундаментальных достижениях науки и практики, применение которых, с одной стороны, позволяет оказывать качественно и достаточно оперативно медицинскую помощь населению, но, с другой стороны, содержит в себе значительное количество рисков в связи с еще недостаточно исследованным характером новых сквозных технологий.

В свете перехода от информационного к цифровому обществу значительное внимание уделяется цифровым технологиям и процессам, происходящими с ними (в частности обработка цифровой информации).

Кроме того, на данный момент обмен информацией осуществляется посредством цифровых технологий. Преступления, совершаемые с использованием возможностей цифровых технологий, совершаются достаточно часто. Стоит констатировать их рост в дальнейшем в условиях тотальной цифровизации всех сторон общественной жизни. Данные обстоятельства приводят к необходимости формирования комплекса мер противодействию подобным уголовно наказуемым деяниям, признания устойчивым в уголовно-правовой доктрине термина «цифровые преступления», его подробного исследования, формулирования критериев отнесения деяний к «цифровым», выявления особенностей их квалификации, отграничения от таких категорий, как киберпреступления, преступления в сфере компьютерной информации, которые часто рассматриваются как равнозначные. В результате это позволит исследовать общие признаки противоправных деяний в русле современных цифровых технологий и порождаемых цифровизацией процессов.

Материалы и методы

В качестве научного материала были использованы отечественные и зарубежные публикации, отражающие исследования по рассматриваемой проблеме. В статье предпринята попытка систематизировать имеющиеся теоретические воззрения как отечественных, так и зарубежных авторов, обобщить полученный материал в контексте развития цифровизации, цифровых технологий и влияния этого процесса преступность. Полученные материалы были критически оценены автором, что позволило с учетом сущности цифровых технологий сформулировать собственную концепцию цифровых преступлений, их структуру и признаки.

Описание исследования

Цифровые преступления:

существующие уголовно-правовые концепции

Стоит уточнить то, что в действующем законодательстве определение понятия «цифровых преступлений» не разработано.

Отметим, что понятие «цифровые преступления» является достаточно устойчивым среди специалистов в области уголовно-правовой доктрины. Так, представленный термин употребляют Е. А. Русскевич, И. Р. Бегишев, М. М. Долгиева, Т. В. Пинкевич, Е. Н. Рахмонова и другие авторы. Некоторые специалисты используют достаточно схожий, но иной термин «преступления в цифровой среде» [Ю. А. Воронин, И. М. Беляева, Т. В. Кухтина [1]], «преступления в цифровом пространстве» [2], «преступления в сфере цифровой трансформации» [3]. Категория «digitalcrimes» употребляется и зарубежными специалистами, что также свидетельствует о его универсальности и научной обоснованности [4].

Исследуемая нами категория активно употребляется и в разговорной речи должностных лиц органов государственной власти и иных субъектов на политической арене. Так, председатель совета Фонда развития цифровой экономики Герман Клименко рассказал, что цифровые преступления совершаются мгновенно, поэтому реагировать на них нужно очень быстро¹.

Кроме того, представленный термин употребляется в отечественной и зарубежной криминологии [5; 6], входящей в группу наук криминального цикла, что подчеркивает определенную преемственность в изучении подобных уголовно наказуемых деяний. В законодательстве и в доктрине единое (универсальное) определение понятия «цифровые преступления» или его синонимы («преступления, совершаемые в цифровой сфере», «преступления, совершаемые в цифровом пространстве / в цифровой среде») не выработано.

Так, М. М. Долгиева к «цифровым преступлениям» относит любые посягательства, совершаемые в сети Интернет с использованием соответствующих компьютерных технологий [7, с. 254]. Полагаем, что представленное определение является достаточно дискуссионным по той причине, что специалист выделяет такую разновидность технологий как «компьютерные», при этом, по нашему мнению, ограничивая иные виды цифровых технологий, что нам представляется недостаточным и верным.

Пожою позицию относительно определения понятия «цифровые преступления» придерживается Б. М. Ибраева, которая к цифровым преступлениям относит «деяния, совершаемые в Интернете, а также все виды уголовно наказуемых деяний, совершаемых в сфере информационных и телекоммуникационных систем. При этом предметом правонарушения являются все информационные ресурсы и технологии, а целью — преступные посягательства». При этом, по мнению автора, в киберпреступлениях объектом является информационная безопасность, а компьютер выступает предметом [8, с. 60]. Полагаем, что, исходя из легального определения, сеть Интернет представляет собой разновидность

¹ Совина М. В России рассказали о мгновенно совершаемых цифровых преступлениях // Lenta.ru. URL: <https://lenta.ru/news/2023/10/31/v-rossii-rasskazali-o-mgnovenno-sovershaemyh-tsifrovyyh-prestupleniyah/> (дата обращения: 21.07.2024).

информационно-телекоммуникационной сети, поэтому выделять их в разные разновидности не стоит. Кроме того, исходя из конструкции уголовно-правового запрета, предусмотренного ст. 272 УК РФ, компьютерная информация является предметом преступления, при этом компьютер как вещь материального мира не выступает предметом как обязательным признаком состава преступления.

В уголовно-правовой доктрине предусмотрен и иной подход, согласно которому авторы выделяют конкретные составы преступлений, входящие в группу «цифровых». По мнению И. В. Ботвина, действующее уголовное законодательство условно можно разделить на две группы норм, содержащих запрет на цифровые посягательства, совершаемые с использованием современных технологий, в том числе сети Интернет: главу 28 («Преступления в сфере компьютерной информации»), состоящую всего из 5 статей, и группу статей, которые рассредоточены по Особенной части УК РФ (ст. 110.1, 110.2, 128.1, 245 УК РФ и другие) [9, с. 161].

Схожей позиции придерживается И. В. Поляков, считающий, что уголовное законодательство содержит ряд уголовно-правовых норм, призванных охранять цифровые отношения от преступных посягательств [10, с. 23].

В свою очередь А. С. Перины к цифровым преступлениям относит «деяния, совершаемые посредством компьютерных, цифровых, информационно-телекоммуникационных и иных современных технологий либо в киберпространстве» [11, с. 109]. При этом специалист выделяет значительный массив технологий, указывая при этом неопределённый термин «иные современные технологии», что нам представляется не совсем верным.

И. Р. Бегишев исследует цифровые преступления, совершаемые в отношении роботов (неправомерное использование, неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в роботе), и за захват управления роботом посредством создания, распространения компьютерных программ [12, с. 109].

Профессор Т. В. Пинкевич в определение понятия «цифровые преступления» относит широкий круг деяний: в отношении цифровых технологий или с их использованием; с использованием компьютерных устройств и программ как средство, орудие, предмет преступления [13, с. 24–25].

Ю. А. Воронин отмечает два подхода: когда объединенным предметом посягательств непосредственно является цифровая информация, и способ совершения преступных деяний — использование цифровой информации (цифровых технологий) [14, с. 75].

Зарубежные авторы указывают на то, что до сих пор не существует единообразного понимания цифровой преступности, и относят к последним правонарушения в отношении компьютерных данных или систем, несанкционированный доступ, модификация или повреждение компьютера или цифровой системы [4, с. 13–14].

Другие правоведы в толкование категории «цифровые преступления» закладывают иной подход. Так,

И. В. Поляков и иные авторы предлагают выделять две группы цифровых преступлений:

— преступления с использованием цифровых технологий;

— преступления в отношении цифровых технологий (например, в сфере компьютерной информации [10, с. 23]).

На данный момент наметилась тенденция исследованиями авторами цифровых преступлений в определенной сфере:

Г. Р. Григорян исследует цифровые имущественные преступления и обосновывает необходимость модернизации главы 21 УК РФ [15, с. 88];

В. Иванюк изучает вопросы прогнозирования такого вида цифровых финансовых преступлений, как мошенничество, на основе методов машинного обучения [16];

Желько Белаяц, А. Филиппович рассматривают такую разновидность цифровых преступлений, как цифровое насилие [17];

Ву-Чун Джун изучает феномен цифровых сексуальных преступлений в Корее, способы их совершения, а также характеристику потерпевших от подобных уголовно наказуемых деяний и иные закономерности, меры по их предупреждению [18];

А. С. Перины выделяет цифровые преступления против личности [19, с. 90], она относит распространение «цифрового» способа совершения преступлений на уже имеющиеся составы, направленные против личности;

Е. З. Сидорова считает то, что предметом совершения цифровых преступлений выступают персональные данные, а также электронные средства платежа. Еще одной чертой данных составов является совершение преступления с использованием компьютерных сетей или же ИТТ [20, с. 71].

Полагаем, что сложность в выработке и обосновании понятия цифровых преступлений связана с тем, что этот термин в разных странах понимается и определяется по-разному. Более того, нет соответствующей конкретной статистики по совершенным преступлениям такого рода [21, с. 194].

Отличие цифровых преступлений

от иных видов противоправных деяний

Достаточно часто в обыденной речи, а также в уголовно-правовой доктрине можно заметить то, что в содержание цифровых преступлений вкладывают такие понятия, как компьютерная преступность, преступления в сфере компьютерной информации, интернет-преступления либо электронные уголовно наказуемые деяния. В правовой доктрине сложились разные точки зрения относительно соотношения собственно цифровых и иных уголовно наказуемых деяний, что позволило сформировать доктринальные подходы.

Первый подход связан с абстрактным и широким определением понятия «цифровые преступления», так как последние не имеют конкретных признаков. Так, Е. А. Русскевич к таковым относит как «компьютерные преступления», посягающие на объекты информационно-коммуникационной инфраструктуры (в том числе

компьютерную информацию), так и «компьютеризированные преступления» по признакам объекта [22, с. 29].

Второй подход строится на рассмотрении компьютерной и киберпреступности уже цифровой преступности. По их мнению, «цифровая преступность — это социальное противоправное явление, включающее в себя совокупность преступлений, совершаемых в сфере цифровых технологий или с их использованием, включая незаконное завладение и предложение или распространение информации в информационно-телекоммуникационных сетях и в виртуальной среде, дополняющей реальность» [23, с. 196].

Третий подход. Отождествление цифровых и компьютерных преступлений, цифровых и электронных уголовно наказуемых деяний.

Однако мы полагаем, что:

1) использовать подобный термин является некорректным. Во-первых, используемое в УК РФ словосочетание «компьютерная информация» является устаревшим. Следует уточнить, что в современных условиях следует говорить о цифровой, а не о компьютерной информации. С появлением цифровых устройств, позволяющих обрабатывать, в том числе получать, передавать и хранить данные в цифровой форме, понятие «компьютер», должно быть исключено из текстов нормативных правовых актов. В современном мире рынок перенасыщен цифровыми устройствами, поэтому если информация будет создана на каком-либо устройстве, к примеру, телефоне, планшете, цифровом фотоаппарате, то она уже не будет являться компьютерной, а будет — цифровой;

2) отождествлять цифровые преступления с электронными неверно. В статье 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹ дается определение понятия «электронный документ»². Определение представленного термина в законе позволяет утверждать о понимании электронного документа как обрабатываемого именно с использованием электронных вычислительных машин. Несомненно, прилагательное «электронный» связывается с движением электронов или устройств, в основе которых лежит их движение. Напомним то, что в физике электрон является элементарной неделимой частицей³. Электрон может проявлять свойства волны (электромагнитного излучения). Электроны и частицы света — фотоны — в волоконно-оптических линиях связи являются носителями информации электронных документов, которые

могут передаваться по информационно-телекоммуникационным сетям. Однако стоит задуматься, если информация будет обрабатываться с помощью других технологий, к примеру, оптических, тогда документ будет называться оптическим, а не электронным? Кроме того, для обработки информации могут быть использованы и другие технологии, в том числе цифровые, квантовые. В связи с этим применение слова «электронный» в контексте действующего законодательства применительно к понятию «электронный документ» и электронные преступления не имеет логического смысла.

Признаки цифровых преступлений

В процессе исследования установлено то, что *цифровые преступления характеризуются специфическими признаками:*

во-первых, уголовно наказуемым деяниям свойственен транснациональный характер. Цифровое преступление может быть совершено в одной стране или регионе против интересов другого государства, общества или личности [4, с. 13–14]. Особенностью этих уголовно наказуемых деяний является то, что сегодня они не ограничены государственными границами, они могут быть совершены откуда угодно и против любого пользователя, находящегося в любом месте. При этом все больше противоправных деяний в цифровом пространстве затрагивает одновременно множество стран;

во-вторых, в первую очередь в процессе выполнения общественно опасного деяния важен сам функционал и возможности цифровой технологии, ее наполнение и те возможности, которые они в себе содержат, а не ее материальная форма воплощения, это и отличает, к примеру, от преступлений против собственности. Например, с целью лишения жизни человека злоумышленник получает доступ к медицинскому изделию, основанному на работе технологий искусственного интеллекта, в результате чего перепрограммирует его и отключает пациента от систем жизнеобеспечения, что приводит его к смерти. В данном случае смерть наступила от доступа к цифровой технологии, а не использовались какие-либо предметы материального мира, то же медицинское изделие [11, с. 111];

в-третьих, функционал цифровых технологий, те возможности, которые они в себе содержат, значительным образом облегчают совершение преступлений;

в-четвертых, цифровые технологии оказывают непосредственное влияние на процесс совершения преступлений. При этом они могут быть использованы как средство и способ совершения противоправного посягательства, а также уголовно наказуемые деяния могут быть совершены и против них и их возможностей;

в-пятых, при совершении преступлений с использованием цифровых технологий злоумышленник стремится причинить вред многим потерпевшим и вызвать цепи многоуровневых общественно опасных последствий [22, с. 9]. Так, в результате атаки на цифровую безопасность больницы в г. Дюссельдорф компьютерные системы больницы выходили из строя одна за одной, из-за чего тяжелых пациентов направляли в другие госпитали,

¹ Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (ч. I). Ст. 3448.

² Электронный документ — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

³ Слепцов И. А., Слепцов А. А. Физика атома и ядра (курс лекций). URL: <https://yagu.s-vfu.ru/mod/book/view.php?id=3151&chapterid=217> (дата обращения: 21.07.2024).

а все плановые операции были отменены, многие пациенты находились в опасности, а одна скончалась¹;

в-шестых, для совершения противоправного деяния используются цифровые данные, цифровые системы или социальные сети. Так, И. Р. Бегишев и другие авторы основным признаком цифровой преступности выделяют предмет посягательства, который должен выражаться в форме информации, циркулирующей в информационном и телекоммуникационных устройствах, их системах и сетях [23];

в-седьмых, если преступление совершается с использованием цифровых технологий или в отношении нее, но когда воздействие происходит на ее «интеллектуальное» наполнение, то местом совершения цифрового уголовно наказуемого деяния будет виртуальная среда. Напомним, что противоправные деяния совершаются с использованием цифровых данных, систем или информационно-телекоммуникационные сети сетей [24].

Кроме указанных нами признаков Э. Л. Сидоренко и другие эксперты Белого Интернета указывают, что российская цифровая преступность в последние годы приобрела устойчивые негативные качества: *высокую латентность, профессионализм, организованный и корпоративный характер*², которые также раскрывают специфические признаки подобных уголовно наказуемых деяний.

Е. А. Русскевич указывает на такой атрибутивный признак цифровой преступности, как *мультипликативность, как способности к самовоспроизводству* [22, с. 9]. Так, атака на программное обеспечение любой даже частной организации может причинить вред как непосредственно этой организации, так и поставит вопрос о национальной безопасности страны в связи с тем, что страдает сфера здравоохранения как одна из важнейших в обеспечении государства. Распространяясь, компьютерный вирус будет поражать все доступные цели, включая объекты государственного управления.

Несомненно, стоит указать на то, что уголовное законодательство не всегда своевременно реагирует на проявления цифровой преступности, так как действующая редакция УК РФ не содержит в себе составы преступлений, связанные с использованием цифровых технологий, что вынуждает сотрудников практических органов квалифицировать деяния по действующим уголовно-правовыми запретами [25, с. 61], которые разрабатывались без учета современных реалий и возможностей, которые несут в себе цифровые технологии.

Заключение и вывод

Употребление в разговорной речи, в доктрине и в законодательстве термина «цифровое преступление» и его

однозначное толкование является необходимым и соответствующим цифровым реалиям в связи с тем, что:

1) находится в русле тенденций цифровизации и процессов, происходящих с нею, не ограничиваясь при этом традиционными понятиями «компьютер», «компьютерная информация», «сеть Интернет»;

2) находится в соответствии с действующим нормативным регулированием, современными тенденциями порождаемых цифровизацией понятий на уровне законодательного регулирования (использование таких категорий, как «цифровая экономика», «цифровая медицина», «цифровой двойник», «цифровые технологии» и т. д.);

3) демонстрирует «правовую природу» и степень влияния цифровых технологий на уголовно наказуемые деяния;

4) позволяет ограничивать цифровые от других преступлений;

5) позволяет под влиянием цифровизации выделить признаки, характеризующие цифровые преступления [26, с. 156].

Итак, *цифровые преступления* — виновно совершенные общественно опасные деяния, совершенные с использованием цифровых технологий и (или) в отношении них.

Основные признаки цифровых преступлений:

— цифровые технологии являются конструктивным признаком составов преступлений (средством, способом, предметом преступного посягательства);

— использование цифровых технологий (их возможностей) в целях совершения преступлений;

— совершение преступлений в отношении цифровых технологий;

— происходит воздействие на цифровые данные, так как цифровые технологии могут обрабатывать цифровую информацию и совершать с ней различные действия;

— могут оказать влияние как на одного потерпевшего, так и на их множество, а также на отдельные государства.

Система цифровых преступлений состоит:

1. Из преступлений против цифровых технологий (цифровые технологии являются предметом преступного посягательства).

В данном случае целесообразно выделять уголовно наказуемые деяния, совершаемые:

— *непосредственно против цифровой технологии;*

— *против результата цифровой технологии.*

Существуют риски противоправных действий в отношении законного оборота биопринтера, в том числе хищение биопринтера, биочернил, незаконная торговля биопринтерами, биочернилами.

2. Преступлений, совершенных с использованием цифровых технологий (цифровые технологии используются в качестве средства и способа).

Приведем следующие примеры.

Злоумышленники под видом медицинских работников могут оказывать консультации с использованием соответствующих телемедицинских цифровых технологий,

¹ Герасюкова М. Не успели спасти: пациентка умерла из-за хакерской атаки. URL: https://www.gazeta.ru/tech/2020/09/18/13255255/ransomware_death.shtml (дата обращения: 17.07.2024).

² Сидоренко Э. Л. Цифровая преступность: угрозы и тренды. Топ-10. URL: https://www.president-sovet.ru/members/blogs/post/tsifrovaya_prestupnost_ugrozy_i_trendy_top_10/ (дата обращения: 21.07.2024).

ставить пациентам диагнозы и назначать методы лечения, не имея соответствующего образования и права заниматься медицинской практикой¹.

Воздействуя на цифровой код компьютерной программы медицинского робота, лицо осуществило неправомерный доступ и захватило управление им в целях уничтожения имущества больницы (в крупном размере). В данном случае лицо использует медицинского робота в качестве средства совершения преступления, предусмотренного ст. 167 УК РФ.

Злоумышленники уже используют технологию дипфейков для совершения мошеннических действий. Зимой 2024 года в одной компании были украдены несколько аккаунтов пользователей Telegram, затем были получены аудиофайлы (голосовые сообщения). После этого аудиофайлы были использованы для генерации поддельных записей, в которых мошенники от имени владельца аккаунта вымогали денежные средства у пользователей, которые состояли вместе с ним в различных чатах².

¹ Фролова М. В левых халатах: в Москве задержали группировку лжеврачей // Известия. URL: <https://iz.ru/1732351/mariia-frolova/v-levykh-khalatakh-v-moskve-zaderzhali-gruppirovku-lzhevrachei> (дата обращения: 05.08.2024).

² Новикова М. Фейковые боссы атакуют в Telegram // TelecomDaily. URL: <https://telecomdaily.ru/news/2024/01/30/fejkovyie-bossy-atakuyut-v-telegram> (дата обращения: 05.08.2024).

Список источников

1. Воронин Ю. А., Беляева И. М., Кухтина Т. В. Современные тенденции преступности в цифровой среде // Вестник Южно-Уральского государственного университета. Серия «Право». 2021. Т. 21, № 1. С. 7–12. DOI: 10.14529/law210101
2. Базоров Н. П., Сагарев И. Ю. Мотивы совершения преступления в цифровом пространстве // Вестник науки. 2024. № 5 (74). С. 133–139.
3. Тхакумачев Б. Ю. Специфика расследования преступлений в сфере цифровой трансформации // Право и государство: теория и практика. 2023. № 7 (223). С. 428–430. DOI: 10.47643/1815-1337_2023_7_428
4. Mohammed S. An Introduction to Digital Crimes // International Journal in Foundations of Computer Science & Technology. 2015. № 5. P. 13–24. DOI: 10.5121/ijfcsst.2015.5302
5. Сахабутдинова А. С., Корчагин А. Г. Цифровая преступность: причины, виды, тенденции преступности, личность преступника, меры противодействия // Аграрное и земельное право. 2023. № 8 (224). С. 25–28. DOI: 10.47643/1815-1329_2023_8_25
6. Сидорова Е. З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) // Сибирский юридический вестник. 2023. № 3 (102). С. 70–78. DOI: 10.26516/2071-8136.2023.3.70
7. Долгиева М. М. Цифровой объект преступления // Вестник Томского государственного университета. 2022. № 483. С. 253–260. DOI: 10.17223/15617793/483/27
8. Ибраева Б. М. Теория цифровой преступности // Интерактивная наука. 2016. № 9. С. 60–62. DOI: 10.21661/i-114276
9. Ботвин И. В. Основные черты уголовной политики в сфере цифровых преступлений // Вестник Сибирского юридического института МВД России. 2022. № 4 (49). С. 160–164.
10. Поляков И. В. Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. 2020. № 4. С. 21–25.
11. Перина А. С. «Цифровые преступления»: понятие, типология, признаки // Юридический вестник Самарского университета. 2023. Т. 9, № 3. С. 106–115. DOI: 10.18287/2542-047X-2023-9-3-106-115
12. Бегишев И. Р. Цифровые преступления, совершаемые в отношении роботов // Социально-политические науки. 2021. № 3 (11). С. 67–73. DOI: 10.33693/2223-0092-2021-11-3-67-73
13. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология : учебное пособие. Москва: Академия управления МВД России, 2021. 244 с.
14. Воронин Ю. А. Преступления в сфере обращения цифровой информации и их детерминанты // Виктимология. 2020. № 1 (23). С. 74–80.
15. Григорян Г. Р. «Цифровые» имущественные преступления: вопросы криминализации и законодательной регламентации // Юридический аналитический журнал. 2020. Т. 15, № 2. С. 73–90. DOI: 10.18287/1810-4088-2020-15-2-73-90
16. Ivanyuk V. Forecasting of digital financial crimes in Russia based on machine learning methods // J Comput Virol Hack Tech. 2024. Vol. 20. P. 349–362. DOI: 10.1007/s11416-023-00480-3
17. Bjelajac Ž. & Filipović A. (2022). Specific Characteristics of Digital Violence and Digital Crime // Pravo — Teorija i Praksa. 2022. Vol. 38, no. 4. P. 16–32. DOI: 10.5937/ptp2104016B
18. Jun W.-C. A Study on the Analysis of and Educational Solution for Digital Sex Crimes in Korea // International Journal of Environmental Research and Public Health. 2023. Vol. 20, no. 3. Art. 2450. DOI: 10.3390/ijerph20032450
19. Перина А. С. Квалификация цифровых преступлений против личности: проблемные вопросы // Вестник Югорского государственного университета. 2023. № 2 (69). С. 89–104. DOI: 10.18822/byusu20230289-104
20. Сидорова Е. З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) // Сибирский юридический вестник. 2023. № 3 (102). С. 70–78. DOI: 10.26516/2071-8136.2023.3.70

21. Rakhmanova E. N., Pinkevich T. V. Digital Crime Concept // Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth (MTDE 2020) : Proceedings of the 2nd International Scientific and Practical Conference. Published by Atlantis Press SARL, 2020. P. 193–196. DOI: 10.2991/aebmr.k.200502.031
22. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография. 2-е изд., перераб. и доп. Москва : ИНФРА-М, 2022. 350 с.
23. Begishev I., Bersei D., Peryakina M., Zhirov R., Kovyazin V., Gerasimova Yu., Arshinov A., Ryabova L. Signs of digital crime: Legal issues // AIP Conference Proceedings : VII International Conference «Safety Problems of Civil Engineering Critical Infrastructures» (SPCECI2021), Yekaterinburg, May 27–28, 2021. Vol. 2701, no. 1. Yekaterinburg : AIP Publishing, 2023. P. 02003–4. DOI 10.1063/5.0130209
24. Антопольский А. Б. Государственный надзор и охрана прав владельцев цифровых объектов // Проблемы законодательства в сфере информатизации : сборник тезисов докладов участников десятой Всероссийской конференции. Москва : Изд-во ВНИИПВТИ, 2002. С. 2–2.
25. Шишкин Р. В. Потребительский рынок как объект посягательства цифровых преступлений // Академическая мысль. 2021. № 4 (17). С. 60–62.
26. Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. 2022. Т. 9, № 2. С. 148–156. DOI: 10.47475/2411-0590-2022-19202

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 31.07.2024.

Дата рецензирования статьи / Revised: 23.09.2024.

Дата принятия статьи к публикации / Accepted: 15.10.2024.