Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2022. – Т. 8 (74). № 4. – С. 158-165.

УДК 343.9

ЦИФРОВАЯ ИНФОРМАЦИЯ КАК ПРЕДМЕТ ПОСЯГАТЕЛЬСТВА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Семёнова И. В.

Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации

В современном обществе наращиваются обороты по цифровизации данных. Банковская сфера по многим направлениям перешла на информацию, имеющую цифровую форму, бизнес, деятельность в социальной сфере так же осваивает цифровой формат взаимодействия. Складываются цифровые правоотношения, соответственно не могло не привлечь внимание преступного сообщества. Однако в данной сфере необходимы особые знания в IT- сфере, программировании, в связи с этим не любая информация может стать предметом такого рода преступления. Информация должна обладать особыми свойствами и находиться не просто в какой-то квартире или помещении, а в особом специализированном месте, в которое невозможно попасть, применяя толь лишь силовые методы, при этом необходимо обладать специализированной техникой, навыками и умениями.

В статье предпринята попытка обосновать необходимость группу преступлений, именуемых «компьютерные преступления» перевести в разряд преступлений совершенных в сфере «цифровой информации», поскольку такое понимание считаем довольно узким, требующим изменения по групповому признаку и заменить термин.

Ключевые слова: цифровизация, переступления, национальные интересы, информационная сфера, предмет преступления, компьютерная информация, потребитель информации, источник информации, передача цифровой информации.

Рост геополитической нестабильности и конфликтности, усиление межгосударственных противоречий, ухудшение эпидемиологической ситуации в мире способствуют повышенному вниманию вопросам безопасности со стороны руководства государств. Рассматриваются вопросы, посвященные формированию безопасного информационного пространства, защиты российского общества от деструктивного информационно-психологического воздействия. При этом одним из приоритетных направлений формирования национальных интересов должна стоять информационная и экономическая безопасность [1]. В Стратегии национальной безопасности РФ отмечается, что для поддержания национальных интересов необходимо обеспечить защиту от противоправных посягательств на самих граждан, так и на их собственность. На проведенной 12 ноября 2021 г. конференции «Путешествие в мир искусственного интеллекта», посвященной информационным технологиям Президент РФ В.В. Путин упомянул, что развитие цифровых технологий, должны работать на достижение национальных целей. Им был сделан акцент на то, чтобы развитие цифровизации основывалось на принципах деперсонификации и массивного доступа разработчикам искусственного интеллекта из России, научным организациям и бизнесу к обезличенным данным. Необходимо отметить, что Президент РФ, говоря о персональных данных граждан отметил, что особое решение следует принять в отношении информации, имеющей критическое значение для безопасности граждан. При этом, уточняя выше сказанное, акцентировал внимание слушателей на том, что «такая предельно личная информация должна храниться в единой государственной системе биометрической идентификации, то есть государство должно взять на себя

ответственность за ее хранение и при этом обеспечить свободный доступ к ней банкам, другим организациям, но в полностью зашифрованном виде, исключающем любое внешнее вмешательство, открытый доступ к персональным данным». При этом важно обеспечить не только кибербезопасность человека, но и его виртуального двойника – аватара, который будет внутри формирующихся метавселенных. Их разработчики обещают, что человек с помощью таких виртуальных миров сможет преодолевать пространства, не выходя из дома, - отметил Путин В.В. [2].

В век информационных технологий, компьютеризации и цифровизиции вопросы безопасности в этой сфере являются актуальными. Так по итогам первого полугодия 2021 года, был зафиксирован рост числа тяжких и особо тяжких преступлений. По официальным данным МВД РФ, совершение преступлений было сопряжено с применением информационно-теликомуникативных технологий. Отмечен также рост преступлений в IT-сфере, что составило 20,3%, от общего числа преступлений. При этом следует отметить, что в предыдущем 2020 г., число таких преступлений составляло 22,3% от общего числа совершенных преступлений за первое полугодие, при этом в 2021 г. за аналогичный период времени увеличился до 26,5% (от общего числа преступлений). Согласно той же статистике численность преступлений, которые совершены при помощи сети интернет, увеличилась до 42 %, при этом преступления с использованием компьютерной техники составляет из этого числа – 35,7 %, по итогам семи месяцев 2021 г. этот показатель составил 15,7%.

Защита интересов, прав и свобод человека от внешних и внутренних угроз, совершаемых в информационной сфере, является одно из приоритетных направлений деятельности государства. Для этого в Стратегии национальной безопасности определено, что органы государственной власти должны заботиться о развитии информационного пространства, которое будет безопасным для граждан, путем реализации мер, которые направлены на укрепление влияния государства, являющегося гарантом безопасности. Продолжают оставаться активными террористические организации, чья деятельность связана с работой по пропаганде вербовки граждан России для создания своих организаций для осуществления противоправных действий против суверенитета России, в том числе с помощью применения интернет-корпораций [3].

В связи с этим повышается интерес в научных кругах к методам предотвращения, не допущения и раскрытию такого рода преступлений.

Законом закреплено, что под «информационной сферой» понимается «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений» [4]. Представляется, что данное понимание является наиболее полным, поскольку является бланкетным, более точным и лаконичным, сформулированным и признанным на законодательном уровне. Отталкиваясь от такой трактовки, представляется возможным рассмотреть преступления в данной сфере более детально и уделить внимание объединенных в группу преступлений, совершенные в сфере компьютерной информации.

В юридической науке отмечается несколько походов в определении группового признака, по которому происходит объединение преступлений. Так одни авторы в качестве такового выделяют предмет преступления – информацию, указывая на то, что все преступления, которые можно объединить по этому признаку следует называть преступления в «информационной сфере» [5]. Другая же группа ученых придерживается классического понимания, исходя из средства совершения называя данную группу преступлений «в сфере компьютерных преступлений» [6]. Третья группа исследователей называет «преступления в сфере компьютерной информации» [7], такую интерпретацию поддерживает и законодатель, закрепив ее в названии гл. 28 УК РФ. Однако, однозначно утверждать какая трактовка верна достаточно сложно. От полноны и качественного анализа теоретической составляющей, научной обоснованности, в конечном счете, зависит точность выстроенной методики расследования преступления.

Рассматривая такого вида преступления, информация выступает отличительным элементом, по отношению с другими видами преступлений.

При этом следует отметить, что преступления могут быть совершены как с помощью информационной сферы, а также сама информация может выступать объектом и предметом посягательства. Кроме того, понятие «информационная сфера», является более значимой в юридическом понимании категорией, в отличие от отдельно взятых направлений IT сферы, сферы применения системы «Интернет», «компьютерная преступность» [8]. Каждая из категорий входящая в институт «информационной сферы» обладает своей правовой информацией, состоящей из правовых актов и связанных с ними комментариями, справочного, научного материала, охватывающего все направления. Наряду с этим, каждый элемент облает индивидуально – правовым характером, способствующим формированию, трансформации и окончанию действия правоотношений, возникших в результате реализации указанных элементов. Незаконное применение, использование данных объектов преследуется уголовным законодательством.

Говоря о понятийном аппарате и формировании единой терминологии, следует отметить, что в данной сфере еще оно не сформировано окончательно. В связи с этим в научных трудах дается разностороннее толкование преступлений, совершаемых в информационной сфере. Каждый автор, рассматривая институт информационной безопасности, предлагает свое видение данной сферы, пытаясь дать объяснение путем определения его смысла [9]. Через толкования выделяется определение, которое раскрывает и разъясняет содержание и смысл каждого составляющего элемента, входящего в состав рассматриваемой категории.

В контексте нашего исследования интересует понимание «компьютерной информации». Насколько актуальна терминология, исходя из характеристики группового объекта – информации.

При толковании и формулировании определения каждой из составляющей единицы следует помнить о согласованности практической реализации данного элемента научного и теоретического познания. Создание единого понимания, единой концепции в понимании преступлений совершенных в информационной сфере, создание единой теоретической базы будет способствовать совершенствованию методологических особенностей при расследовании данной категории преступлений. «Информационная сфера» данная формулировка считаем наиболее приемлемая,

позволяющая применять ее в различных ситуациях, поскольку она обладает многофункциональным характером, однако она не учитывает специфику информации, не указывает на ее определяющие признаки, которая состоит в том, что вся информация является цифровой. Уголовный кодекс РФ в отдельную группу преступлений выделяет «преступления в сфере компьютерной информации» – гл 28. Данная глава объединяет в себе преступления, связанные с неправомерным доступом, а наравне с этим любые действия направленные на его реализацию и оказание различного рода воздействия. Представляется, что если бы информация, которая не является цифровой, то интерес преступного сообщества был бы иной, тем самым отнести такого рода преступления невозможно к данной группе, поскольку специфика проведения расследования по таким преступлениям в корне меняется. В связи с вышесказанным представляется необходимым рассмотреть теоретическую составляющую элементов, входящих в состав «цифровой информационной сферы». Одним из звеньев данной сферы является информация, которая относится к цифровой.

Основной понятийный аппарат сформулирован и закреплен на законодательном уровне в ст. 1 ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и является отправной точкой для понимания данной сферы деятельности и тех процессов и правоотношений, которые проистекают из нее.

Как ранее уже отмечалось, информация представляет собой определенные сведения, которые могут быть объектом публичных, гражданских правоотношений. Информация может свободно передаваться от одного субъекта к другому, при отсутствии ограничений, устанавливаемых федеральным законодательством. Информация является обобщенным понятием для любых данных, не зависимо от того относится ли она к субъекту (обладатель информации, оператор информационной системы) или объекту (доменное имя, сетевой адрес) или же к коммуникативным способам взаимодействия (информационно-телекоммуникационная сеть, информационные технологии). Буквенный текст, звуки, числа, графическое изображение, видео является формой сведений и данных, которые являются производными информации [10].

Законодателем закреплено толкование и понятие элементов, входящих в состав «информационной сферы». Не смотря на это, следует обратиться к тематическим исследованиям информационной среды, способам ее применения.

Следует отметить, что закрепленные в федеральном законодательстве понятия и их толкования являются постулатами. Однако они имеют свойство трансформироваться, корректироваться со временем в зависимости создания чего-то нового, продвинутого на информационном поле. В связи с этим, необходимо рассмотреть толкования отдельных терминов, закрепленных в федеральном законодательстве.

Для понимания природы преступлений в данной сфере, необходимо уяснить, что эта за категория. Говоря об «информации» как предмете изучения, с точки зрения философии, следует рассматривать ее через три составляющие. Это источник информации, ее потребителя и передающей среды [11]. В контексте криминалистического исследования нас интересует прагматический аспект изучения. При изучении специализированных источников: нормативных - правовых, научных отметим, что под «информацией» в ст. 2 ФЗ № 149-ФЗ [12] понимается любые сведения, которые могут быть предоставлены в различных формах. Информация, приобретая матери-

альную форму, наделяется признаками вещей. Согласно ГК РФ вещи могут свободно отчуждаться от одного субъекта к другому любым дозволенным законом способом [13].

При рассмотрении источника цифровой информации хотелось бы отметить, что данную составляющую невозможно рассмотреть в одной плоскости. Если говорить о том, от куда информация поступает или где хранится (сохраняется пользователем), то для этого существуют три места. В научных кругах эти объекты относят к «электронным носителям информации» [14]. К первому месту хранения отнесем объекты, на которых установлено программное обеспечение. С развитием технологий, средств коммуникаций, цифровизации общества к местам хранения относятся не только персональные компьютеры, но и ноутбуки, планшеты, гаджеты, телевизоры (типа сматрт-ТВ), мобильные устройства (смартфоны), «а также «умные» холодильники, бортовые компьютеры автомашин» [15] и думается, что со временем данный список будет только расширяться. Второй гигантской группой сбора цифровой информации из разных источников является хранилища данных, так называемые банки-данных, которые представлены несколькими типами: - корпоративный; - оперативный; -Data Mart.

Такие типы банков данных могут существовать как самостоятельно, так и образовывать гибридные хранилища, в зависимости от значимости и востребованности информации, а также по различным другим комбинациям.

При рассмотрении института «информации», отталкиваясь ее потребителя (подразумевая, что он может сам создавать информацию в цифровом виде, а так и осуществлять поиск или иметь доступ к ней), можно отметить, что согласно действующему законодательству к «информации» относятся: сведения о личности (персональные данные), о частной жизни субъекта (факты, события, места пребывания, виде деятельности), сведения о юридическом лице, его деятельности, финансовой отчетности, стратегически важных объектах, численности личного состава и т.д. Такого рода информацию можно поделить на две крупные группы: общедоступная и ограниченного доступа [16]. В нынешних нестабильных экономических и политических условиях ключевое место среди лиц, в отношении которых могут совершаться противозаконные действия, будут занимать те потребители информации, которые задействованы или имеют какое-либо отношение к государственному и экономическому сектору. Это могут быть сферы предоставления услуг на уровне государства или муниципального образования; деятельность, связанная с заключением и реализацией государственных контрактов; электронного документа оборота, биометрические персональные данные, а также к системе идентификации и аутентификации личности.

Связующим звеном между потребителем информации и ее источником является передающая среда. Наиболее востребованной передачей цифровой информации в современном мире являются волоконно-оптическая линия связи. Чтобы сигнал был отправлен из места его создания, необходим оптический передатчик, который предназначен для преобразования цифрового (электрического) сигнала в световой сигнал. Для получения сигнала необходим оптический приемник, который будет преобразовывать поступивший световой сигнал обратно и электрические импульсы. При этом в эту систему входят компоненты, которые являются оптическими пассивными – соединители, шнуры, розетки, которые объединяют между собой кон-

векторы (панели распределения, кроссовые шкафы) [17], создавая единую систему обмена информации. Информация может передаваться как в сети Интернет, так и в сетях связи согласно Доктрине, утвержденной Указом Президента РФ от 05.12.2016 № 646, об информационной безопасности Российской Федерации. В отдельных нормативных правовых источниках для информации, которая состоит из сигналов, трансформированных импульсов, закодированных в единицах и ноликах, передающихся по единой системе обмена в сети Интернет, закреплено название «компьютерная информация».

Однако, такое понимание считаем довольно узким, требующим изменения по групповому признаку и заменить термин «компьютерная информация» на «цифровая информация». Также лишним подвидом цифровой информации считает И.Р. Багишев и И.И. Бикеев – компьютерную информацию. В своем исследовании, при рассмотрении ее как предмета преступления, приходят к выводу, что сведения, крутящиеся в устройствах (относящихся к информационно-коммуникационным, входящим в единую систему является) являются цифровыми. В связи с этим такое название будет отражать наиболее точно сущность данной информации [18].

Таким образом, хотелось бы отметить, что термин «компьютерная информация» становится архаичным. Требуется расширить границы понимания информации в связи с компьютеризацией и цифровизацией общества. В связи с этим, необходимо закрепить новое более расширенное понимание такого рода информации, тем самым расширяются количество объектов, входящих в перечень носителей информации. Необходимо привести к согласованности между собой нормативные – правовые акты и закрепить единое понимание и толкование термина. В таком случае, совершенные преступления, можно квалифицировать как преступления, совершенные в «сфере цифровой информации», а не компьютерной.

Список литературы:

1. Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации" // pravo.gov.ru, 03.07.2021

2.Выступление Президента РФ на конференции // https://yandex.ru/video/preview/?text=конференция%20по%20информационной%20безопасности%2012%20ноября%202021%20выступление%20путина&path=yandex_search&parent-reqid=1650960687784472-1119663258361221459 0-vla1-2882-vla-l7-balancer-8080-BAL-4183&from_type=vast&filmId=7693856425870508655

3.Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации" // "Собрание законодательства РФ", 05.07.2021, № 27 (часть II), ст. 5351

4.Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // www.pravo.gov.ru, 06.12.2016, "Собрание законодательства РФ", 12.12.2016, № 50, ст. 7074.

5.Триба, К. А. Уголовная ответственность за совершение преступлений в информационной сфере / К. А. Триба // Colloquium-journal. – 2020. – № 3-10(55). – С. 59-62. – EDN LRBKFN.; Марков, Е. И. Некоторые способы совершения преступлений в информационной сфере и пути их предупреждения / Е. И. Марков // Актуальные проблемы кибербезопасности в сети Интернет : Сборник научных трудов Всероссийской конференции, Москва, 23 апреля 2020 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2020. – С. 99-101. – EDN CMLPXO; Лебедев, А. С. Уголовно-правовая ответственность за преступления в информационной сфере / А. С. Лебедев, И. М. Сошина // Мировая наука. – 2020. – № 12(45). – С. 203-205.

6.Горбачева, О. С. Компьютерные преступления и роль компьютерной экспертизы в расследовании этих преступлений / О. С. Горбачева // Право и образование. – 2001. – № 5. – С. 125-133. – EDN HTYVBH.; Смирнов, И. М. Компьютерные преступления - компьютерные преступления мирового масштаба / И. М. Смирнов // Верховенство права: международный и национальный аспект : сборник

статей Международной научно-практической конференции, Воронеж, 01 мая 2020 года. – Уфа: Общество с ограниченной ответственностью "Аэтерна", 2020. – С. 44-45. – EDN NWVLIU.
7.Попов, А. М. Особенности производства осмотра по преступлениям в сфере компьютерной информации КАК ЭЛЕМЕНТ ДОКАЗЫВАНИЯ / А. М. Попов, А. И. Дубовицкий // Право: история и современность. – 2020. – № 1. – С. 109-115. – DOI 10.17277/pravo.2020.01.pp.109-115. – EDN QXLQSW; Коробеев, А. И. "Цифровизация" преступности и проблемы квалификации преступлений в сфере компьютерной информации / А. И. Коробеев // Роль права в развитии интеграционных процессов в Азиатско-Тихоокеанском регионе: современные тенденции и вызовы : V Тихоокеанский юридический форум, посвященный празднованию 120-летия Дальневосточного федерального университета и 100-летия юридического образования на Дальнем Востоке России, Владивосток, 03–05 октября 2019 года. – Владивосток: Дальневосточный федеральный университет, 2020. – С. 127-129. – EDN ONVFHT.
8.Лопатина Т.М. Криминологические и уголовно- правовые основы противодействия компьютерной преступности: дис. … док. юрид. Наук:12.00.08/ Т.м. Лопатина. М., - 2007. -418с. Добровольцев Д.В.. Актуальные проблемы борьбы с компьютерной преступностью: дис канд. юрид. наук: 12.00.08/ Д.В. Добровольский. - М., 2005. – 218 с.
9.Ожегов С. И. Словарь русского языка. М., 1999. С. 756.
10. Смирнов Виталий Михайлович, Филиппова Полина Игоревна. Обеспечение информационной безопасности для защиты компьютерных и сетевых данных // StudNet. 2021. №5. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-dlya-zaschity-kompyuternyh-i-setevyh-dannyh (дата обращения: 10.02.2022.
11. Философский словарь / под ред. И.Т. Фролова. 6-е изд., перераб. и доп. М.: Политиздат, 1991. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.10.2021) // "Собрание законодательства РФ", 31.07.2006, № 31 (1 ч.), ст. 3448.
12. Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 № 51-ФЗ (ред. от 28.06.2021, с изм. от 26.10.2021).
13. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. канд. юрид.наук: 12.00.09 / Балашова Анна Александровна, Москва, 2020, С. 20-41.
14. Федотов И.С., Смагин П.Г. электронные носители информации: «вещественные доказательства» или «иные документы»// Вестник ВГУ. Серия: Право. 2014. № 3. С. 195.
15. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.10.2021) // "Собрание законодательства РФ", 31.07.2006, № 31 (1 ч.), ст. 3448. Ст 5.
16. Куан И.А., Азимбаев Д.Ж., Щербаченя А.Н., Гербер А.С. ВОЛОКОННО-ОПТИЧЕСКИЕ ЛИНИИ СВЯЗИ // Вестник науки. 2018. №5 (5). URL: https://cyberleninka.ru/article/n/volokonno-opticheskie-linii-svyazi (дата обращения: 05.04.2022). ГОСТ
17. Багишев И.Р Преступления в сфере обращения цифровой информации // И.Р. Багишев, И.И. Бикеев — Казань: Изд-во «Познание» Казанского инновационного университета, 2020. С. 34.

Semenova I.V. Digital information as a subject of encroachments of crimes in the field of computer information // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2022. – T. 8 (74). № 4. – P. 158-165.

In modern society, the pace of digitalization of data is increasing. Banking, social sphere, business in many areas have switched to digital information. Economic and political activity is also mastering the digital format of interaction. The emerging digital legal relations, respectively, could not fail to attract the attention of the criminal community. However, special knowledge is needed in the IT field, programming, in this regard, not any information can become the subject of this kind of crime. Information must have special properties and be located not just in some apartment or room, but in a special specialized place that cannot be accessed using only force methods, while it is necessary to have specialized equipment, skills and abilities.

The article attempts to justify the need for a group of crimes called "computer crimes" to be transferred to the category of crimes committed in the field of "digital information", since such we consider the understanding to be rather narrow, requiring a change on a group basis and replacing the term.

Keywords: digitalization, transgressions, national interests, information sphere, subject of crime, computer information, consumer of information, source of information, transmission of digital information.

Spisok literatury:

1. Ukaz Prezidenta RF ot 02.07.2021 № 400 "O Strategii nacional'noj bezopasnosti Rossijskoj Federacii" //

pravo.gov.ru, 03.07.2021
2. Vystuplenie Prezidenta RF na konferencii // https://yandex.ru/video/preview/?text=konferenciya%20po%20informacionnoj%20bezopasnosti%2012%20noyabrya%202021%20vystuplenie%20putina&path=yandex_search&parent-reqid=1650960687784472-1119663258361221459 0-vla1-2882-vla-l7-balancer-8080-BAL-4183&from_type=vast&filmId=7693856425870508655
3. Ukaz Prezidenta RF ot 02.07.2021 № 400 "O Strategii nacional'noj bezopasnosti Rossijskoj Federacii" // "Sobranie zakonodatel'stva RF", 05.07.2021, № 27 (chast' II), st. 5351
4. Ukaz Prezidenta RF ot 05.12.2016 № 646 "Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii" // www.pravo.gov.ru, 06.12.2016, "Sobranie zakonodatel'stva RF", 12.12.2016, № 50, st. 7074
5. Triba, K. A. Ugolovnaya otvetstvennost' za sovershenie prestuplenij v informacionnoj sfere / K. A. Triba // Colloquium-journal. – 2020. – № 3-10(55). – S. 59-62. – EDN LRBKFN.; Markov, E. I. Nekotorye sposoby sovershen iya prestuplenij v informacionnoj sfere i puti ih preduprezhdeniya / E. I. Markov // Aktual'nye problemy kiberbezopasnosti v seti Internet : Sbornik nauchnyh trudov Vserossijskoj konferencii, Moskva, 23 aprelya 2020 goda. – Moskva: Moskovskij universitet Ministerstva vnutrennih del Rossijskoj Federacii im. V.YA. Kikotya, 2020. – S. 99-101. – EDN CMLPXO; Lebedev, A. S. Ugolovno-pravovaya otvetstvennost' za prestupleniya v informacionnoj sfere / A. S. Lebedev, I. M. Soshina // Mirovaya nauka. – 2020. – № 12(45). – S. 203-205. – EDN KRRRJX.
6. Gorbacheva, O. S. Komp'yuternye prestupleniya i rol' komp'yuternoj ekspertizy v rassledovanii etih prestuplenij / O. S. Gorbacheva // Pravo i obrazovanie. – 2001. – № 5. – S. 125-133. – EDN HTYVBH.; Smirnov, I. M. Komp'yuternye prestupleniya - komp'yuternye prestupleniya mirovogo masshtaba / I. M. Smirnov // Verhovenstvo prava: mezhdunarodnyj i nacional'nyj aspekt : sbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii, Voronezh, 01 maya 2020 goda. – Ufa: Obshchestvo s ogranichennoj otvetstvennost'yu "Aeterna", 2020. – S. 44-45. – EDN NWVLIU.
7. Popov, A. M. Osobennosti proizvodstva osmotra po prestupleniyam v sfere komp'yuternoj informacii KAK ELEMENT DOKAZYVANIYA / A. M. Popov, A. I. Dubovickij // Pravo: istoriya i sovremennost'. – 2020. – № 1. – S. 109-115. – DOI 10.17277/pravo.2020.01.pp.109-115; Korobeev, A. I. "Cifrovizaciya" prestupnosti i problemy kvalifikacii prestuplenij v sfere komp'yuternoj informacii / A. I. Korobeev // Rol' prava v razvitii integracionnyh processov v Aziatsko-Tihookeanskom regione: sovremennye tendencii i vyzovy : V Tihookeanskij yuridicheskij forum, posvyashchennyj prazdnovaniyu 120-letiya Dal'nevostochnogo federal'nogo universiteta i 100-letiya yuridicheskogo obrazovaniya na Dal'nem Vostoke Rossii, Vladivostok, 03–05 oktyabrya 2019 goda. – Vladivostok: Dal'nevostochnyj federal'nyj universitet, 2020. – S. 127-129.
8. Lopatina T.M. Kriminologicheskie i ugolovno- pravovye osnovy protivodejstviya komp'yuternoj prestupnosti: dis. … dok. yurid. Nauk:12.00.08/ T.m. Lopatina. M., - 2007. -418s. Dobrovol'cev D.V.. Aktual'nye problemy bor'by s komp'yuternoj prestupnost'yu: dis kand. yurid. nauk: 12.00.08/ D.V. Dobrovol'skij. - M., 2005. – 218 s.
9. Ozhegov S. I. Slovar' russkogo yazyka. M., 1999. S. 756.
10. Smirnov Vitalij Mihajlovich, Filippova Polina Igorevna OBESPECHENIE INFORMACIONNOJ BEZOPASNOSTI DLYA ZASHCHITY KOMP'YUTERNYH I SETEVYH DANNYH // StudNet. 2021. №5. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-dlya-zaschity-kompyuternyh-i-setevyh-dannyh (data obrashcheniya: 10.02.2022
11. Filosofskij slovar' / pod red. I.T. Frolova. 6-e izd., pererab. i dop. M.: Politizdat, 1991. str. 166
12. Federal'nyj zakon ot 27.07.2006 № 149-FZ (red. ot 02.07.2021) "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" (s izm. i dop., vstup. v silu s 01.10.2021) // "Sobranie zakonodatel'stva RF", 31.07.2006, № 31 (1 ch.), st. 3448.
13. Grazhdanskij kodeks Rossijskoj Federacii (chast' pervaya)" ot 30.11.1994 № 51-FZ (red. ot 28.06.2021, s izm. ot 26.10.2021).
14. Balashova A.A. Elektronnye nositeli informacii i ih ispol'zovanie v ugolovno-processual'nom dokazyvanii: dis. kand. yurid.nauk: 12.00.09 / Balashova Anna Aleksandrovna, Moskva, 2020, S. 20-41.
15. Fedotov I.S., Smagin P.G. elektronnye nositeli informacii: «veshchestvennye dokazatel'stva» ili «inye dokumenty»// Vestnik VGU. Seriya: Pravo. 2014. № 3. S. 195.
16. Federal'nyj zakon ot 27.07.2006 № 149-FZ (red. ot 02.07.2021) "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" (s izm. i dop., vstup. v silu s 01.10.2021) // "Sobranie zakonodatel'stva RF", 31.07.2006, № 31 (1 ch.), st. 3448. St 5.
17. Kuan I.A., Azimbaev D.ZH., SHCHerbachenya A.N., Gerber A.S. VOLOKONNO-OPTICHESKIE LINII SVYAZI // Vestnik nauki. 2018. №5 (5). URL: https://cyberleninka.ru/article/n/volokonno-opticheskie-linii-svyazi (data obrashcheniya: 05.04.2022). GOST
18. Bagishev I.R Prestupleniya v sfere obrashcheniya cifrovoj informacii // I.R. Bagishev, I.I. Bikeev — Kazan': Izd-vo «Poznanie» Kazanskogo innovacionnogo universiteta, 2020. S. 34.

.