Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт права, социального управления и безопасности

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ ПРОЦЕССЕ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Коллективная монография

Ижевск
2024

ISBN 978-5-4312-1216-1
DOI:**10.35634/978-5-4312-1216-1-2024-1-120**

УДК 343.13:004.9
ББК 67.410.2с51
И741

Рекомендовано к изданию редакционно-издательским советом УдГУ

Рецензенты: профессор каф. судебной деятельности и уголовного процесса УрГЮУ им. В.Ф. Яковлева, д-р юрид. наук, доцент **А.О. Машовец;** судья Устиновского районного суда г. Ижевска УР **Н.В. Злобин.**

Научный редактор: зав. каф. уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет», д-р юрид. наук, профессор **Л.Г. Татьянина.**

Коллектив авторов:
Ф.А. Абашева, А.М. Каминский, Т.В. Решетнева, Г.А. Решетникова,
В.В. Ровнейко, С.В. Соболев, Д.В. Татьянин, Л.Г. Татьянина, Е.Ф. Тенсина,
Э.Г. Хомяков, Р.М. Хуснутдинов, А.М. Шамсеева

И741 Информационные технологии в уголовном процессе: современное состояние и перспективы развития : коллективная монография / науч. ред. Л.Г. Татьянина. – Ижевск : Удмуртский университет, 2024. – Электрон. (символьное) изд. (1,4 Мб). – 120 с. – Текст : электронный

В издание вошли статьи, подготовленные преподавателями Института права, социального управления и безопасности Удмуртского государственного университета и посвященные, главным образом, наиболее актуальным вопросам использования информационных технологий в уголовном процессе, представляющим взаимный интерес коллектива авторов. Авторами с учетом комплексного подхода исследуются вопросы использования технологий искусственного интеллекта при осуществлении правосудия, обеспечения информационной безопасности, «цифровизации» досудебного производства использования «электронного» доказательства, применения современных технологий при криминалистических исследованиях.

Монография может быть полезна студентам, магистрантам, преподавателям, осуществляющим подготовку по правовым основам профессиональной деятельности, а также практикующим юристам.

Минимальные системные требования:
Celeron 1600 Mhz; 128 Мб RAM; WindowsXP/7/8 и выше;разрешение экрана 1024×768 или выше; программа для просмотра pdf

ISBN 978-5-4312-1216-1
DOI:10.35634/978-5-4312-1216-1-2024-1-120

Подписано к использованию 13.12.2024
Объем электронного издания 1,4 Мб
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru

ПРЕДИСЛОВИЕ

Вниманию предлагается коллективный труд, посвященный исследованию наиболее актуальных вопросов развития информационных технологий в уголовном процессе. Современная жизнь уже немыслима без активного использования технологий и их внедрения во все сферы общественной жизни. Не является исключением и уголовно-процессуальная сфера. Несмотря на все те преимущества, которые, безусловно, имеют место быть вследствие «технологизации» уголовно-процессуальных отношений: доступность, быстрота обработки информации, мобильность при осуществлении связей с участниками уголовного процесса в связи с их удаленностью и ряд других; в кругах ученых-юристов, практиков ведутся активные дискуссии о целесообразности расширения «цифровизации», «информатизации» уголовно-процессуальной деятельности. Все чаще с площадок различного уровня звучат призывы к детальному изучению, правовому прогнозированию всех допустимых правовых рисков, которые уже возникают или могут возникнуть при внедрении информационных технологий; к исследованию этических принципов при использовании технологий искусственного интеллекта, особенно, когда речь идет об обеспечении прав участников уголовного процесса, или принятии решений судьей в обозримом будущем на основании проекта судебного решения, подготовленного при помощи «робота-судьи». Кроме того, научного обоснования требуют широко внедряемые и используемые не только в повседневной жизни, но и в среде профессионалов-юристов таких понятий, как «электронное правосудие», «электронное доказательство» и др. Существующее правовое регулирование общественных отношений, в которых используются информационные технологии, далеко от идеала, что обусловлено динамичным развитием «цифры», поэтому актуализируется вопрос об адаптации действующих правовых предписаний к соответствующим отношениям. В настоящей монографии получили свое разрешение не все вопросы, связанные с внедрением информационных технологий в уголовный процесс, а лишь те, которые представляют взаимный интерес коллектива авторов.

Ровнейко Вера Владимировна,
кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии

«Чу́дище о́бло, озо́рно, огро́мно, стозе́вно и ла́яй»
Эпиграф к книге Александра Радищева
«Путешествие из Петербурга в Москву»

ПОНЯТИЕ И ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Существует достаточно большое количество различных понятий, которые используются в нормативных актах, международных договорах, судебной практике и специальной литературе для обозначения одной и той же группы преступлений:

– киберпреступления;

– компьютерные преступления;

– преступления в сфере информационных технологий;

– преступления в сфере компьютерной информации, а также иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»;

– преступления, совершенные с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации;

– а также: «информационные преступления», «преступления в сфере высоких технологий», «IT-преступления» и т.д.

При этом большинство авторов в тексте в качестве синонима вышеприведенных громоздких словосочетаний используют более легкое и понятное для восприятия понятие «киберпреступление».

Необходимость единого подхода к нормативному определению этого понятия отмечается многими авторами[1] и заслуживает поддержки.

[1] *Бутусова Л.И.* К вопросу о киберпреступности в международном праве // Вестник экономической безопасности. 2016. № 2. С. 48–52; Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. Ч. 1 / под ред. А.В. Аносова. М. : Академия управления МВД России, 2019. С. 11.

Определение понятия «киберпреступление» в источниках права отсутствует. Само понятие «киберпреступление» официально используется очень редко. Так, в названии международных договоров и соглашений оно не используется, хотя Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185[2] имеет второе название – Конвенция о киберпреступности. На сайте МИД России в официальных информационных сообщениях для СМИ (например в работе над универсальным договором о противодействии использованию информационно-коммуникационных технологий в преступных целях) понятие «киберпреступность» используется постоянно[3], хотя прослеживается и постоянство в отказе от использования понятия «киберпреступление» («киберпреступность») в официальных названиях договоров и соглашений.

Как синоним понятия «киберпреступление» используются понятия «компьютерное преступление» и «информационное преступление». Если различать понятие «киберпреступления» в широком и узком смысле, то понятие «киберпреступление» в широком смысле позволяет рассматривать их как информационные преступления. «В научных трудах используется понятие «информационные преступления»… Под информационными преступлениями понимаются общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершенные в области широкого круга отношений… »[4]. Эта формулировка представляется некоторым авторам самой неудачной[5], хотя, как ни странно, она наиболее точно отражает особенности общественной опасности киберпреступлений в широком смысле. Понимание киберпреступлений как информационных преступлений основано на том, что кибернетика – «наука об общих закономерностях процессов управления и передачи информации в машинах, живых организмах и обществе»[6].

---

[2] Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185 (23 ноября 2001 г., г. Будапешт).

[3] Об итогах голосования в Генассамблее ООН по российскому проекту резолюции по противодействию киберпреступности (27.12.2019). URL: https://www.mid.ru/main_en/-/asset_publisher/G51iJnfMMNKX/content/id/3988579; О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях (28.07.2021). URL: https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4831832

[4] *Пережогина Г.В.* Проблемы определения понятия «преступления, совершаемые с использованием информационных технологий» в современных условиях // Уголовное право: стратегия развития в XXI веке : материалы XVIII Междунар. науч.-практ. конф. М. : РГ-Пресс, 2021. С. 99.

[5] Там же.

[6] Советский энциклопедический словарь / науч.-ред. совет: А.М. Прохоров (пред.), М.С. Гиляров, Е.М. Жуков, Н.Н. Иноземцев, И.Л. Кнунянц, П.Н. Федосеев, М.Б. Храпченко. М. : Изд-во «Советская Энциклопедия», 1981. С. 944.

Но необходимо учитывать и другие особенности кибернетики, с развитием которой и связано появление киберпреступлений. Кибернетика – это «наука об общих законах получения, хранения, передачи и переработки информации – т.н. кибернетические системы, рассматриваемые абстрактно, вне зависимости от их материальной природы… Основное техническое средство для решения задач кибернетики – ЭВМ. Поэтому возникновение кибернетики как самостоятельной науки связано с созданием в 40-х гг. XX в. этих машин, а развитие кибернетики в теоретическом и практическом аспектах – с процессом электронной вычислительной техники»[7].

«Исторически первым термином, обозначающим рассматриваемый вид преступлений, указывают «Cybercrime» («киберпреступление»)[8]. Данное определение отражается в рекомендациях экспертов ООН, где термин «киберпреступление» отражен как любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети»[9].

Многие авторы отмечают, что среди ученых нет единства в определении киберпреступности и цифровой преступности[10]. При этом отмечается, что слово «кибер» имеет английское происхождение. С учетом современного семантического значения слова «кибер» («cyber» – это прилагательное, означающее **«относящийся к компьютерам, информационным технологиям, интернету»**[11]) и слова «киберпространство» (метафорическая абстракция, используемая в философии и компьютерных технологиях, являющаяся виртуальной реальностью; второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей[12]) можно сказать об использовании этого понятия для обозначения

---

[7] Советский энциклопедический словарь / науч.-ред. совет: А.М. Прохоров (пред.), М.С. Гиляров, Е.М. Жуков, Н.Н. Иноземцев, И.Л. Кнунянц, П.Н. Федосеев, М.Б. Храпченко. М. : Изд-во «Советская Энциклопедия», 1981. С. 578.

[8] *Дубко М.А.* О понятии компьютерного преступления // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/analitics/computercrime06; *Чекунов И.Г.* Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37.

[9] Преступления, связанные с использованием компьютерной сети : справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети // Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями (Вена, 10–17 апреля 2000 года). С. 6. URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf

[10] *Рахманова Е.Н., Пономарева Е.В.* Киберпреступность, цифровая преступность и кибербезопасность: проблемы определения и взаимосвязи // Уголовное право: стратегия развития в XXI веке. 2023. № 3. М. : Издательство «Проспект», 2023. С. 204.

[11] Словарь «Нейро» // Яндекс. URL: https://yandex.ru/

[12] Словарь. URL: https://translate.yandex.ru/dictionary/Английский.Русский/cyber

группы преступлений в узком смысле. Слово «цифровой», применительно к интересующей нас теме, переводится как digital (цифровой, электронный[13]). Можно сказать, что оба понятия имеют схожее содержание, допустимо их использовать как синонимы с учетом определенных особенностей, но при этом оба не являются официальными терминами.

Таким образом, понятие «киберпреступление» в узком смысле возникло как синоним понятия «компьютерное преступление», но на сегодняшний день переросло его. «Понятие киберпреступлений шире компьютерных, так как охватывает большую сферу действий, совершаемых преступниками. Киберпреступления – это те виды преступлений, которые совершаются посредством не только использования компьютеров, но и других технических устройств, виртуального пространства, сети «Интернет». Компьютерные же преступления связаны именно с компьютерами, где компьютер выступает как средство совершения преступления либо как объект посягательства, не обязательно при этом использование глобальных сетей»[14]. Существуют и другие определения киберпреступлений, в которых авторы не связывают совершение киберпреступлений только с компьютерами, компьютерными сетями и компьютерной информацией[15].

На необходимость различать киберпреступления в широком и узком смысле было обращено внимание еще в 2000 году на Десятом конгрессе ООН по предупреждению преступности и обращению с правонарушителями: «Существует две категории киберпреступлений: a) киберпреступление в узком смысле («компьютерные преступления»)…; b) киберпреступление в широком смысле («преступление, связанное с использованием компьютеров)» (п. 14)[16]. Но в вышеприведенном положении имеет место отождествление киберпреступлений с компьютерными преступлениями, и не учитывается их информационный характер в целом.

---

[13] Словарь «Нейро» // Яндекс. URL: https://yandex.ru/

[14] *Бутусова Л.И.* Указ. соч. С. 49.

[15] *Тропина Т.Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дисс. … канд. юрид. наук. Владивосток, 2005. С. 9–16. URL: https://www.dissercat.com/content/kiberprestupnost-ponyatie-sostoyanie-ugolovno-pravovye-mery-borby); *Щетилов А.* Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом // Информатизация и информационная безопасность правоохранительных органов : материалы XI Межд. конф. М., 2002. С. 17, 57; *Чекунов И.Г.* Современные киберугрозы. Уголовно-правовая и криминологическая квалификация киберпреступлений // Право и кибербезопасность. 2012. С. 35.

[16] Преступления, связанные с использованием компьютерной сети: справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети // Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями (Вена, 10–17 апреля 2000 года). С. 6. URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf

Понятие «киберпреступление» (в узком смысле) адекватно воспринимается, но в юридической литературе могут использоваться сложносочиненные термины, такие как «преступления, совершаемые с использованием информационных технологий»[17], или «преступления, совершаемые с использованием электронных информационно-телекоммуникационных и иных цифровых технологий»[18], или «преступления, совершенные с использованием информационных, коммуникационных и высоких технологий»[19]. В судебной практике используется достаточно многословное понятие «преступления в сфере компьютерной информации, а также иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"»[20]. В статистической отчетности используется понятие «преступления, совершенные с использованием (применением) информационно-телекоммуникационных технологий, или в сфере компьютерной информации»[21].

Из всех вышеперечисленных терминов, исходя из содержания понятия «информационные технологии», наиболее корректным для обозначения киберпреступлений в широком смысле является понятие «преступления в сфере информационных технологий», т.к. согласно ст. 2 Федерального закона «Об информации, информационных технологиях и защите информации» «информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»[22].

---

[17] *Пережогина Г.В.* Указ. соч. С. 97–98.

[18] *Цепелев В.Ф.* Перспективы адекватного уголовно-правового реагирования на новые виды преступлений, совершаемых с использованием электронных информационно-телекоммуникационных и иных цифровых технологий // Уголовное право: стратегия развития в XXI веке : материалы XVIII Междунар. науч.-практ. конф. М. : РГ-Пресс, 2021. С. 103.

[19] Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. Ч. 1 / под ред. А.В. Аносова. М. : Академия управления МВД России, 2019. С. 11.

[20] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15.12.2022 № 37.

[21] Перечень № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации : указание Генпрокуратуры России № 11/11, МВД России № 1 от 17.01.2023 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». URL: https://sudact.ru/

[22] Статья 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2024).

Термин «преступления, совершенные с использованием информационных технологий» предлагается, например, Г.В. Пережогиной[23]. Похожий термин используется в официальной статистике МВД[24]. В 2018 г. заключено Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий[25].

Необходимо также рассмотреть соотношение понятий «преступления в сфере информационных технологий» и «преступления против информационной безопасности». Последний термин также используется в источниках права. Например, в 2015 году заключено Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности[26]. С учетом содержания угроз международной информационной безопасности (они связаны с использованием информационно-коммуникационных технологий для совершения правонарушений и преступлений, для вмешательства во внутренние дела государства, для нанесения экономического и другого ущерба и т.п.) можно сделать вывод о допустимости отождествления понятий «преступления в сфере информационных технологий» и «преступлений против информационной безопасности». Этот вывод также подтверждается содержанием Доктрины информационной безопасности Российской Федерации[27] и определением угроз информационной безопасности в Стратегии национальной безопасности Российской Федерации[28].

Т.Л. Тропина определяет понятие «киберпреступление» как «виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные

---

[23] *Пережогина Г.В.* Указ. соч. С. 102.

[24] Преступления, совершенные с использованием информационно-телекоммуникационных технологий. – См.: Краткая характеристика состояния преступности в Российской Федерации за январь – август 2024 года. URL: https://мвд.рф/reports/item/55225633/

[25] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года (ратифицировано Федеральным законом от 01.07.2021 № 237-ФЗ с оговоркой, вступило в силу для Российской Федерации 17 июля 2022 года). URL: http://publication.pravo.gov.ru/Document/View/0001202207180005?index=3

[26] Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности (8 мая 2015 года, г. Москва). URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/43921/

[27] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 декабря 2016 г. № 646.

[28] О Стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02.07.2021 № 400.

общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству»[29].

Понятие «киберпреступления», как преступления в сфере информационных технологий, охватывает не только преступления в сфере компьютерной информации, составы которых содержатся в главе 28 УК РФ. В постановлении Пленума Верховного Суда РФ от 15.12.2022 № 37 выделено два вида киберпреступлений:

1) преступления в сфере компьютерной информации (Глава 28 УК РФ);

2) преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» (составы которых расположены в других главах и разделах УК РФ)[30].

Чтобы определить, какое именно содержание авторы вкладывают в понятия преступлений в сфере информационных технологий (киберпреступлений), нужно рассмотреть виды таких преступлений. Можно выделить огромное количество их классификаций по самым разным основаниям. Остановимся на официальных классификациях киберпреступлений.

Наиболее полной (по содержанию и правовому значению) является классификация киберпреступлений, используемая для целей статистической отчетности (несмотря на пространность, приводится в полном объеме, т.к. дает целостное представление о преступлениях в сфере информационных технологий и их видах):

1. Преступления, относящиеся к перечню без дополнительных условий (например, содержащиеся в главе 28 УК РФ, а также п. "г" ч. 3 ст. 158, ст. 159.3, 159.6, п. "в", ч. 3 и п. "в", ч. 5 ст. 222, п. "в" ч. 3 и п. "в" ч. 5 ст. 222.1, п. "в" ч. 3 и п. "в" ч. 5 ст. 222.2, п. "д" ч. 2 ст. 230, п. "г" ч. 2 ст. 242.2).

2. Преступления, относящиеся к перечню при наличии определенных условий:

2.1. Преступления, которые в соответствии с Особенной частью УК РФ имеют альтернативный квалифицирующий признак, предполагающий использование информационно-телекоммуникационных сетей, включая сеть "Интернет".

---

[29] *Тропина Т.Л.* Указ. соч. С. 9–10.

[30] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15.12.2022 № 37.

2.2. Преступления, относящиеся к перечню при наличии в статистической карточке отметок о способах совершения преступления:

– с использованием сети "Интернет" (ресурсов глобальной сети);

– с использованием сети Даркнет ("Теневая сеть"), под которой понимается скрытая сеть, соединения которой устанавливаются по типу p-2-p (peer-to-peer, децентрализованная сеть);

– использование фишингового (поддельного) сайта или ссылки;

– с использованием средств мобильной связи, под которыми понимаются технические и программные средства, служащие для передачи информации беспроводным способом, без использования сети "Интернет";

– неправомерное списание денежных средств со счетов банковских карт;

– использование вредоносных компьютерных программ, создание и распространение вредоносных компьютерных программ либо иной компьютерной информации, под которыми понимаются программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

– с использованием "программ-шифровальщиков", представляющих собой разновидность вредоносных программ, которые с помощью различных алгоритмов шифрования блокируют доступ пользователей к файлам, либо преобразуют их содержимое на компьютере до состояния, непригодного к использованию правообладателем;

– с использованием бот-сетей (ботнет), под которыми подразумевается компьютерная сеть, состоящая из узлов, зараженных вредоносным программным обеспечением с возможностью централизованного управления без ведома владельцев узлов;

– с использованием DDoS-атак, представляющих собой распределенную атаку типа "отказ в обслуживании" с одновременным использованием большого числа атакующих компьютеров, в том числе объединенных в бот-сеть, целью которой, как правило, является воспрепятствование доступу легитимных пользователей к атакуемому ресурсу, частичное нарушение штатного функционирования информационной инфраструктуры и т.д.;

– с использованием информационно-телекоммуникационных технологий (отметка проставляется при использовании различных технологий, не имеющих самостоятельных кодовых значений для отражения в статистической карточке (машинные носители, технические средства снятия информации);

– с использованием (применением) компьютерной техники, под которой понимается компьютер, а также отдельное оборудование, которое работает совместно с ним и обеспечивает его дополнительную функциональность;

– с использованием (применением) расчетных (пластиковых) карт;

– с использованием (применением) программных средств, под которыми понимается любое программное обеспечение, установленное на персональном компьютере, смартфоне или другой технике;

– с использованием (применением) фиктивных электронных платежей, под которыми понимаются поддельные электронные платежные документы, имеющие равную юридическую силу с платежными документами на бумажных носителях;

– с использованием социальных сетей, под которыми понимаются платформы, онлайн-сервисы или веб-сайты, предназначенные для построения, отражения и организации социальных взаимоотношений;

– с использованием средств мгновенного обмена сообщениями (интернет-мессенджеров), под которыми понимаются приложения или программы, установленные на смартфоне или компьютере;

– с использованием электронных платежных систем, под которыми понимаются системы расчета между финансовыми организациями и интернет-пользователями при покупке-продаже товаров и оплате услуг;

– операции с цифровой валютой, под которыми понимаются выпуск цифровой валюты и осуществление в отношении нее действий;

– с использованием SIP-телефонии, под которой понимается система звонков через сеть "Интернет" с использованием протокола IP на обычные телефонные сети передачи голосовой информации (подвижной или стационарной);

– неправомерный доступ к компьютерной информации, под которым понимается получение возможности ознакомиться и (или) воспользоваться компьютерной информацией лицом, не обладающим правами на получение и работу с данной информацией либо компьютерной системой, в отношении которых приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ (при условии уничтожения, блокирования, модификации либо копирования компьютерной информации);

– операции с цифровыми финансовыми активами, под которыми понимаются их выпуск и осуществление в отношении них действий;

– с использованием технологий "Дипфэйк", под которыми подразумеваются методика синтеза аудио- или визуальной информации, основанная на искусственном интеллекте, целью которой является создание сравнимой с оригиналом копии аудио- или видеоизображения;

– использование специальных средств и техники, предназначенной для компрометации банковских устройств самообслуживания (банкоматов, терминалов);

– с использованием информационной инфраструктуры иностранного государства (или придание такого вида), под которой в т.ч. понимаются зарубежные серверы (услуги хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменные зоны, телефонные сети и т.д.;

– с использованием информационной инфраструктуры стран – участников СНГ (или придание такого вида), под которой в т.ч. понимаются серверы стран – участников СНГ (услуги хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменные зоны, телефонные сети и т.д.[31].

Следует согласиться с тем, что «в уголовно-правовом плане преступления, совершенные с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), обладают разным характером общественной опасности»[32]. В приведенной классификации сложно определить один единственный критерий для классификации киберпреступлений (в ней присутствуют и объект посягательства, и способ, и средства, и орудие, и место совершения преступления, и субъект совершения преступления). Но следует отметить, что она отражает содержание понятия преступлений в сфере информационных технологий (киберпреступлений) в узком смысле.

Такую же узкую направленность содержания понятия «преступление в сфере информационных технологий» (киберпреступление) отражает и другая классификация (перечень) киберпреступлений, сформулированная в целях реализации Соглашения о сотрудничестве Российской Федерации и государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий, менее детальная, чем предыдущая, и предусматривает:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

---

[31] Перечень № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации : указание Генпрокуратуры России № 11/11, МВД России № 1 от 17.01.2023 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». URL: https://sudact.ru/

[32] *Лобач Д.В.* Развитие российского уголовного законодательства в сфере противодействия преступлениям, совершаемым в сети «Интернет» // Уголовное право: стратегия развития в XXI веке. 2023. № 3. М. : Издательство Проспект, 2023. С. 24.

д) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма[33].

Содержание угроз информационной безопасности Российской Федерации обосновывает именно такой подход к содержанию понятия «преступления в сфере информационных технологий» (киберпреступления).

Можно предложить другой аспект и критерий для классификации преступлений в сфере информационных технологий, прямо вытекающий из содержания Федерального закона «Об информации, информатизации и защите информации»[34]. С учетом содержания понятия «информационные технологии» можно выделить четыре вида киберпреступлений:

1. Преступления в сфере предоставления информации (например отказ в предоставлении информации или предоставление неполной или ложной информации).

2. Преступления в сфере распространения информации (например, : распространение ложной информации (фейков), запрещенных материалов, в том числе экстремистских и террористических, запрещенной к распространению инфор-мации, нарушение авторских и смежных прав и т.п.).

3. Преступления в сфере доступа к информации (например, неправомерный доступ к охраняемой и конфиденциальной информации).

---

[33] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года (ратифицировано Федеральным законом от 01.07.2021 № 237-ФЗ с оговоркой, вступило в силу для Российской Федерации 17 июля 2022 года). URL: http://publication.pravo.gov.ru/Document/View/0001202207180005?index=3

[34] Статья 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2024).

4. Преступления в сфере сбора (поиска), хранения и обработки информации (например, разглашение сведений, составляющих банковскую тайну).

Данная классификация тоже не безупречна, т.к. она основана на нарушениях требований регулятивного законодательства и, возможно, не отражает в полном объеме все виды киберпреступлений, например такой вид посягательств, как посягательства, совершаемые в отношении конкретного лица или лиц и связанные, например, с доведением до самоубийства или вовлечением в совершение преступления с использованием мессенджеров. Хотя в широком смысле такие действия могут рассматриваться как киберпреступления в сфере распространения информации. Необходимость учета регулятивного законодательства при классификации преступлений в сфере информационных технологий обусловлена и системностью в сфере противодействия им.

Кроме того, исходя из содержания угроз информационной безопасности Российской Федерации и регулятивного законодательства, можно выделить еще два направления уголовно-правового воздействия:

– направленное на защиту информации;
– направленное на защиту **от** информации.

С учетом этого можно выделить две большие группы преступлений в сфере информационных технологий:

1) посягающие на охраняемую законом (в широком смысле слова) информацию (например, : конфиденциальную, имеющую режим тайны, государственной, банковской, налоговой, персональные данные и т.д.);

2) нарушающие закон (в широком смысле слова) о защите **от** информации, запрещенной к распространению в Российской Федерации, и распространение которой может нанести вред личности, обществу или государству.

Если первой группе преступлений в законодательстве, судебной практике и специальной литературе уделяется достаточно много внимания, то вторая группа – нуждается в более тщательном изучении. Статьи 10 и 15.1 Федерального закона «Об информации, информационных технологиях и защите информации», предусмотрев свободу распространения информации, ограничили ее, установив запрет «на распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность». В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, создана ЕАИС «Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов,

позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено»[35].

Единый реестр запрещенной информации размещен на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)[36]. Для пресечения распространения противоправной информации на нем содержится перечень (не исчерпывающий) видов такой информации (запрещенной к распространению на территории Российской Федерации):

– порнография;
– суицидальный контент;
– пронаркотический контент;
– незаконные азартные онлайн-игры;
– незаконная продажа лекарственных препаратов;
– незаконная продажа оружия, взрывчатых веществ, взрывных устройств и способы их изготовления;
– информация, вовлекающая несовершеннолетних в противоправную деятельность;
– незаконная продажа алкогольной продукции в сети «Интернет»;
– информация о пострадавших в результате противоправных действий несовершеннолетних;
– ЛГБТ, педофилия и смена пола;
– клевета и оскорбление;
– средства обхода блокировок[37].

Отсутствие учета системности в определении основных правовых понятий в сфере противодействия преступлениям в сфере информационных технологий (киберпреступлениям), возможно, не так явно мешает эффективному противодействию этому виду преступлений, т.к. сложности противодействия этим преступлениям носят технический и организационный характер. Например, проблемой, связанной с противодействием преступлениям в сфере компьютерной

[35] Статьи 10, 15.1 Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2024).

[36] Единый реестр запрещенной информации. URL: https://rkn.gov.ru/activity/electronic-communications/eais/

[37] Пресечение распространения противоправной информации // Роскомнадзор. URL: https://rkn.gov.ru/activity/electronic-communications/p1568/

информации, является их анонимный характер. На этот аспект обращено внимание в Стратегии национальной безопасности РФ: «Анонимность, которая обеспечивается за счет использования информационно-коммуникационных технологий, облегчает совершение преступлений, расширяет возможности для легализации доходов, полученных преступным путем, и финансирования терроризма, распространения наркотических средств и психотропных веществ»[38]. Некоторые авторы в связи с этим предлагают ликвидировать возможность анонимного пользования публичным информационным пространством[39]. Но технические средства для реализации этого предложения ограничены. Правоприменители сталкиваются с проблемами идентификации личности преступника при совершении киберпреступлений, хотя способы идентификации устройств, с помощью которых совершаются такие преступления, установления приемов и методов их совершения и определения места совершения успешно применяются.

Следует согласиться с авторами, которые считают, что в целях повышения эффективности правового регулирования правоохранительных отношений и предупреждения преступности в информационной сфере представляется необходимым обеспечить законодательную унификацию рассматриваемого признака с учетом положений действующего регулятивного законодательства, в том числе Федерального закона «Об информации, информатизации и защите информации»[40].

Это соответствует и принципу формальной определенности уголовно-правового запрета, нашедшему закрепление в позициях Конституционного Суда РФ, неоднократно сформулированному в постановлениях и определениях: «Особую значимость требования определенности, ясности, недвусмысленности правовых норм и **их согласованности в системе общего правового регулирования** приобретают применительно к уголовному законодательству, являющемуся по своей правовой природе крайним (исключительным) средством, с помощью которого государство реагирует на факты противоправного поведения в целях охраны общественных отношений, если она не может быть обеспечена должным образом только с помощью правовых норм иной отраслевой принадлежности»[41].

---

[38] Пункт 54 Указа Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

[39] *Габеев С.В.* Проблемы реализации уголовной политики в отношении преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Уголовное право: стратегия развития в XXI веке. 2023. № 3. М. : Издательство Проспект, 2023. С. 37.

[40] *Лобач Д.В.* Указ. соч. С. 27.

[41] По делу о проверке конституционности положения части первой статьи 188 Уголовного кодекса Российской Федерации в связи с жалобой гражданки М.А. Асламазян : постановление Конституционного Суда РФ от 27.05.2008 № 8-П.

Отсутствие согласованности между положениями регулятивного законодательства и действующего Уголовного кодекса РФ в сфере противодействия преступлениям в сфере информационных технологий и отсутствие единообразия при формулировании уголовно-правовых запретов проявилось и в изменениях, внесенных в УК РФ Федеральным законом от 08.08.2024 № 218-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», который расширил сферу применения уголовного закона для противодействия распространению в информационном пространстве деструктивного контента в виде треш-стримов[42]. В ряде статей Особенной части УК РФ был введен квалифицирующий признак – «с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть "Интернет")»[43]. Понятие «публичной демонстрации» не имеет нормативного определения, и его использование в данном случае представляется неоднозначным, т.к. возникает вопрос о необходимости и критериях отграничения «публичной демонстрации» от «публичного распространения информации» (например ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан», ст. 207.2 УК РФ «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия»). Согласно положениям Федерального закона, «распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц»[44]. То есть, исходя из нормативного определения «распространения информации», оно не может быть не публичным, т.к. направлено на неопределенный круг лиц.

Таким образом, несмотря на достаточно большое количество различных понятий, которые используются для обозначения одной и той же группы преступлений, наиболее корректными являются «киберпреступления», «преступления в сфере информационных технологий» и «преступления против информационной безопасности». Перечисленные термины могут при определенных оговорках использоваться как синонимы.

---

[42] О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления ответственности за совершение преступлений с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)) : пояснительная записка к законопроекту № 506240-8. URL: https://sozd.duma.gov.ru/bill/506240-8

[43] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 08.08.2024 № 218-ФЗ.

[44] Статья 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2024).

Классификация киберпреступлений, используемая для формирования статистической отчетности, является официальной и наиболее объемной. С учетом содержания понятия «информационные технологии» в регулятивном законодательстве – Федеральном законе «Об информации, информатизации и защите информации» – можно выделить другие виды киберпреступлений.

Необходимость учета регулятивного законодательства при определении понятий и классификации преступлений в сфере информационных технологий вытекает из принципа формальной определенности уголовно-правового запрета, нашедшего закрепление в позициях Конституционного Суда РФ.

Исходя из содержания угроз информационной безопасности Российской Федерации и регулятивного законодательства, следует учитывать уголовно-правовое воздействие, направленное не только на защиту охраняемой законом информации (ее целостность, доступность и т.п.), но и направленное на защиту **от** информации, которая способна причинить существенный вред личности, обществу и государству.

Абашева Флюра Ахунзяновна,
кандидат юридических наук, доцент, доцент кафедры уголовного процесса и криминалистики

К ВОПРОСУ ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ «ОПРЕДЕЛЯЕМОЕ ФИЗИЧЕСКОЕ ЛИЦО» И ГАРАНТИИ ЕГО ПРАВ

В научной литературе и судебной практике очень часто возникают вопросы относительно того, могут ли данные о частной жизни физического лица входить в понятие «персональных данных», для обработки которых не требуется получение согласия субъекта персональных данных.

Исходя из этого, возникает вопрос: какие элементы входят в нормативное понятие «частная жизнь лица»?

Могут ли физические черты физического лица, черты его лица и телосложения являться персональными данными, для сбора и обработки которых требуется получение согласия на обработку персональных данных?

Где пролегает граница между публичными сведениями и данными, составляющими частную жизнь лица? Внутренняя обстановка места проживания – убранство, вещи, предметы, документы и факты о пребывании других лиц – являются ли персональными данными? Поскольку защита закона распространяется на персональные данные, значит, сначала нужно попытаться определить, что входит в частную жизнь лица, а затем понять входят ли подобные данные в определение персональных данных?

Под персональными данными следует понимать любые факты об определенном лице, которые позволяют собрать образ о данном лице, говорят о его политических и социальных взглядах, раскрывают состояние его здоровья, формируют деловую репутацию, а также содержат детали его семейной жизни. Некоторые факты рассматриваются законодателем как общедоступные персональные данные, другие же, наоборот, рассматриваются в качестве специальных категорий персональных данных. Подобная категоризация данных о конкретном лице визуализируется в положениях федерального закона.

Тем не менее в законе о персональных данных отсутствует упоминание частной жизни лица. Того понятия, в основе которого лежит конституционная гарантия.

Интересным представляется вопрос, связанный с нормативным толкованием понятия частной жизни лица, поскольку неприкосновенность частной жизни лица является одной из ключевых конституционных гарантий, которая имеет

основополагающее значение для развития человека. Вопрос, который стоит перед нами, может быть сформулирован следующим образом: какие факты из частной жизни лица следует отнести к персональным данным? Какие правовые гарантии защиты персональных данных применимы к фактам о частной жизни лица в том случае, если факты из частной жизни входят в понятие частной жизни?

Для ответа на данный вопрос следует рассмотреть некоторые примеры судебной практики, а также обратиться к трудам ученых правоведов, рассматривающих понятие частной жизни и определяющих конкретный смысл конституционной гарантии.

Свою позицию в вопросе об определении частной жизни лица огласил Пачелмский районный суд Пензенской области в ходе рассмотрения жалобы заявителя, связанной с запретом на проведение совместной фотосъемки отца со своим ребенком. Запрет на фотосъемку не являлся абсолютным, но был подчинен одному из условий, коим является получение согласия мамы несовершеннолетнего ребенка, поскольку фотосъемка отца с ребенком, осуществляемая в непосредственной близости от места жительства мамы ребенка, будет включать в себя обстановку по месту жительства последней. Пачелмский районный суд указывает, что без получения согласия матери ребенка, не допускается фотографирование обстановки по месту ее жительства, поскольку подобная обстановка содержит факты о частной жизни лица, сбор и сохранение которых без согласия недопустимы.

В обоснование своей позиции суд указывает, что законодательного определения частной жизни лица на момент принятия указанным судом своего решения не предусмотрено. Суд обращается к одному из принципов гражданского законодательства, указывая на недопустимость произвольного вмешательства кого-либо в частные дела другого лица. Подобный тезис закреплен в Гражданском кодексе Российской Федерации.

Далее, в доводах суда приведен аргумент о публичном характере сведений. Пачелмский суд идет от обратного, утверждая в своих тезисах, что факты о жизни лица, не имеющие в силу закона публичного характера, составляют частную жизнь лица, информация о которой не может быть собрана или использована без согласия самого лица. В подтверждение своих доводов, суд дает правовую оценку действиям лиц, участвующих в деле. Суд приходит к выводу о том, что вид и обстановка домовладения, в состав которых входят вещи, предметы и документы собственника или лица, проживающего в домовладении, не могут быть запечатлены посредством фотосъемки без получения согласия от лица, проживающего или владеющего домовладением. Кроме того, не могут быть запечатлены собственник или иные лица, находящиеся в домовладении в тот или иной момент, без согласия собственника.

Справедливо напрашивается вывод о том, что Пачелмский районный суд в понятие частной жизни лица включает место проживания лица, факт пребывания как владельца, так и иных лиц в месте проживания, а также элементы обстановки места проживания. Указанные составляющие частной жизни не являются публичными сведениями, а потому без согласия лица сбор данных в какой бы то ни было форме не допускается. Можно предположить, что несогласованные действия, в результате которых третьему лицу может стать известно об обстановке в месте проживания другого лица или может стать известно о пребывании кого-либо другого в месте проживания, приводят к нарушению охраняемого Конституцией права на неприкосновенность частной жизни.

Если отталкиваться от тезиса, что данные о внутренней обстановке места проживания конкретного лица, равно как и факты пребывания кого-либо в месте проживания, входят в понятие частной жизни, то можно сделать вывод о том, что подобные данные и факты (что к подобным данным и фактам применяются гарантии неприкосновенности, в соответствии с которыми нельзя без согласия субъекта частной жизни собирать и распространять данные) непосредственно относятся к персональным данным, поскольку обработка персональных данных, их сбор и хранение непосредственно связаны с правом каждого на неприкосновенность личной жизни. Подобный тезис является весьма логичным согласно доводам, которые использует Привокзальный районный суд города Тулы в обоснование своего решения по делу о незаконном разглашении и использовании персональных данных. Поводом для рассмотрения вопроса о защите персональных данных стал иск директора компании, осуществляющей электронную торговлю в сети «Интернет», к владельцу сообщества, созданного в информационной социальной сети «Вконтакте». Действия владельца сообщества, функционирующего на платформе социальной сети, по мнению истца, противоречат законодательству о защите персональных данных, поскольку владелец сообщества опубликовал на веб-страницах своего сообщества сведения, составляющие персональные данные о конкретном лице, не получив на то согласия субъекта персональных данных, коим является истец.

На веб-страницах сообщества его владельцем были опубликованы данные о директоре организации, указанные в выписке из единого государственного реестра юридических лиц, которая публикуется на официальном сайте Федеральной налоговой службы России в информационно-телекоммуникационной сети «Интернет». В своих доводах истец утверждает, что сведения о физическом лице, указанные в выписке из единого государственного реестра юридических лиц, следует относить к персональным данным. Для использования персональных данных о конкретном лице, а именно ИНН и ФИО, необходимо получение согласия субъекта персональных данных, тем более, что публикация подобных

данных на веб-страницах сообщества социальной сети «ВКонтакте» влечет за собой разглашение персональных данных неограниченному кругу лиц. Истец настаивает, что для осуществления подобных действий физическому лицу, осуществляющему деятельность по обработке персональных данных, надлежит зарегистрироваться в качестве оператора персональных данных и получить согласие на обработку персональных данных перед их публикацией на веб-страницах сообщества, созданного на платформе социальной сети «ВКонтакте».

Возражая против доводов истца, ответчиком указано, что на данные о физическом лице, которые содержатся в выписке из единого государственного реестра юридических лиц (ФИО и ИНН), не распространяется ограничение на распространение персональных данных, связанное с согласием субъекта персональных данных. В обоснование своих контраргументов ответчик говорит о предусмотренной федеральным законом категоризации персональных данных[45], согласно которой есть отдельная категория персональных данных, а именно общедоступные персональные данные, о которых может знать неограниченный круг лиц. Логика ответчика заключается в том, что те или иные персональные данные можно отнести к общедоступным, если подобные данные ранее были обнародованы в общедоступных источниках. К единому государственному реестру юридических лиц ответчик применяет термин «каталог организаций», стараясь подвести подобный ресурс в информационно-телекоммуникационной сети «Интернет» к общедоступным источникам, т.е. распространить определение общедоступного источника на реестр юридических лиц, зарегистрированных в Российской Федерации. В связи с тем, что данные о физическом лице, выполняющем функции генерального директора юридического лица, ранее уже были предоставлены неограниченному кругу лиц посредством опубликования на портале ФНС в единой информационно-телекоммуникационной сети «Интернет», ответчик приходит к выводу о том, что законодательством не может быть предусмотрен запрет на распространение и использование сведений, которые являются общедоступными в силу закона. В дополнение ответчик указывал, что сведения и информация, которые представлены субъектом персональных данных добровольно (хотя скорее, соблюдая императивный порядок регистрации юр. лица, закрепленный в нормах законодательства) могут быть опубликованы в общедоступных источниках персональных данных. Ответчик полагал, в случае, когда персональные данные находятся в общедоступном источнике, то при распространении и публикации указанных сведений получение согласия от субъекта на распространение не требуется.

[45] О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. 08.08.2024) // СПС «КонсультантПлюс».

Тем не менее суд в своих доводах не соглашается с позицией ответчика и не приводит в первую очередь тех сведений, которые были бы достаточны для обоснования судебной позиции. Несмотря на необходимость определения понятия общедоступного источника и общедоступных данных, надлежащих дефиниций указанных понятий судом введено или представлено в судебном решении не было. Суд подчеркивает необходимость получения согласия лица для распространения персональных данных в информационно-телекоммуникационной сети «Интернет». Довод суда состоит в том, что сам по себе факт публикации сведений о лице в общераспространенных источниках персональных данных (ЕГРЮЛ) не дает другим лицам право использовать подобные сведения без согласия субъекта персональных данных. Суд приводит законодательное определение персональных данных и говорит о том, что к персональным данным следует отнести как фамилию, так и ИНН физического лица. Кроме того, судом дается и расширенное определение персональных данных, среди которых: дата рождения субъекта, адрес проживания, социальное положение, образование, профессия, доходы и другая информация. Подобное определение закреплено в федеральном законодательстве о защите персональных данных.

Более того, в судебном решении указывается и дефиниция понятия «распространение персональных данных».

Чего в решении суда нет, так это понятия «сбор персональных данных». Сбор персональных данных является весьма важным, поскольку для осуществления деятельности по сбору персональных данных должен быть определен правовой механизм. Судом не дается надлежащая оценка действий ответчика по сбору персональных данных, который, на мой взгляд, заключается в скачивании выписки из общераспространенного источника в информационно-телекоммуникационной сети «Интернет». Деятельность по сбору персональных данных может быть направлена на получение информации о конкретном лице без дальнейшего распространения данных.

Тем не менее суд не дает однозначную оценку правомерности действий ответчика по сбору персональных данных путем скачивания выписки из общедоступного источника без согласия лица, кому указанные данные принадлежат. Мне полагается, что суд не подвергает сомнению право каждого на ознакомление с персональными данными, в том числе, когда происходит их скачивание или, говоря другими словами, копирование информации из общедоступных источников в информационно-телекоммуникационной сети «Интернет». Однако для того чтобы рассуждать о правомерности ознакомления с персональными данными в общедоступных источниках, следует указывать в судебном решении дефиниции подобных терминов. Также необходимо установление некоторых условий для допуска кого бы то ни было к персональным данным других лиц.

Наверняка было бы целесообразным получать согласие от лица, скачивающего чьи-либо персональные данные из общедоступных источников, на нераспространение персональных данных, пока не будет получено согласие собственника персональных данных. Подобное обязательство влечет за собой обязательство владельца общедоступного источника требовать с каждого, кто пытается получить персональные данные о том или ином лице, согласие на нераспространение персональных данных, полученных из общедоступного источника.

Основополагающим аргументом в доводах суда является закрепленный в законе запрет на распространение персональных данных. В решении используется законодательное определение понятия «распространение персональных данных»[46], но, как и указано мною выше, нет определения понятия «сбор персональных данных». Судом указано, что запрет на распространение персональных данных носит обязательный к исполнению характер и применяется к общедоступным персональным данным, которые находятся в общедоступных источниках. При вынесении решения суд основывается на законодательных нормах, регламентирующих порядок обработки персональных данных и условия для их распространения, ключевым из которых является согласие, выраженное в письменной или электронной форме.

Непонятным является факт использования Привокзальным районным судом г. Тулы конституционного запрета, установленного в статье 24 Конституции Российской Федерации. Запрета, связанного с охраной частной жизни лица. Постараемся изложить свой тезис посредством следующих доводов:

1. В судебных доводах усматривается явное противоречие. Вызвано оно тем, что, несмотря на упоминание конституционного запрета на хранение и разглашение сведений о частной жизни лица, судом употребляется понятие общедоступных персональных данных. Факты и информация, на наш взгляд, которые составляют частную жизнь лица, не могут быть общедоступными, равно как и не должны находиться в общедоступных источниках. Стоит отметить, что здесь в понятие частной жизни лица мы вкладываем факты и информацию о внутренней обстановке жилища физического лица, а также факты о пребывании самого лица или других лиц в жилище. По нашему мнению, информация, в состав которой входят фамилия, имя и отчество, равно как и год рождения физического лица, не является информацией, составляющей частную жизнь лица.

[46] «Под распространением персональных данных понимаются действия, направленные на раскрытие персональных данных неопределенному кругу лиц», – из материалов судебного решения.

2. При изучении судебного решения у нас сложилось впечатление о применении судом конституционной гарантии неприкосновенности частной жизни к персональным данным о лице. Тем не менее в судебном решении нет четкой регламентации нормативной связи между понятиями частная жизнь и персональные данные о физическом лице. Мы не смогли выявить аргументы, которые могли бы быть использованы для закрепления связи конституционной гарантии на неприкосновенность частной жизни с правом каждого субъекта на защиту своих персональных данных, которое закрепляется в положениях Федерального закона о защите персональных данных. Единственное, что объединяет положения статьи 24 Конституции РФ и статьи 6 Федерального закона № 152-ФЗ, – это необходимость получения согласия для сбора информации о частной жизни лица и обработки персональных данных.

Разбор судебного решения о распространении персональных данных, полученных из общедоступных источников, подталкивает нас к определенному тезису, связанному с применением термина «персональные данные». Возвращаясь к вопросу о применимости законодательства об охране персональных данных к ситуации, где в объектив видеозаписывающего устройства попадает внутренняя обстановка жилища, а также сведения о нахождении собственника и временном пребывании других физических в жилище, хотелось бы отметить следующее:

1) сведения и факты о внутренней обстановке и нахождении физических лиц в жилище следует рассматривать как данные о частной жизни лица;

2) сведения и факты о внутренней обстановке в цифровой форме следует отнести к персональным данным о лице, сбор которых без согласия субъекта персональных данных не допускается. То есть факты о частной жизни конкретного лица можно рассматривать в качестве персональных данных, как только подобные факты обретают цифровую или электронную форму;

3) несанкционированный сбор сведений о частной жизни лица в цифровой форме должен быть регламентирован в законе, равно как и порядок привлечения соответствующих лиц к ответственности за нарушение порядка обработки персональных данных.

В одном из определений Конституционного Суда[47] об отказе в принятии жалобы гражданина на нарушение его конституционного права на неприкосновенность частной жизни следует обратить внимание на аргументы суда в пользу

[47] Об отказе в принятии к рассмотрению жалобы гражданина Барабанова Виктора Валерьевича на нарушение его конституционных прав положениями п. 4 ч. 1 ст. 6 и п. 1 ч. 1 ст. 7 ФЗ «Об оперативно-розыскной деятельности» : определение Конституционного Суда РФ от 23.04.2015 № 873-О // СПС «КонсультантПлюс».

обоснованного и уместного ограничения указанного права. По мнению заявителя, праву на неприкосновенность частной жизни лица противоречит законодательная норма, которая допускает проведение проверочной закупки. В дополнение заявителем утверждается, что норма Закона об оперативно-розыскной деятельности, допускающая проведение проверочной закупки при наличии возбужденного уголовного дела, также противоречит конституционному праву лица.

В своем определении суд обращает внимание, что положения Федерального закона «Об оперативно-розыскной деятельности» не противоречат конституционным нормам и гарантиям (право на неприкосновенность частной жизни), поскольку в нормах закона есть конкретные ограничения для проведения оперативно-розыскных мероприятий. Более того, закон возлагает на уполномоченные органы обязанность соблюдения прав и свобод человека. Суд напоминает, что осуществление оперативно-розыскных мероприятий возможно лишь при соблюдении ограничений, коими являются:

1) достижение одной из целей, указанной в законе (выявление, раскрытие, предупреждение и пресечение преступлений)[48], а также

2) наличие оснований, которые регламентированы законом (возбужденное уголовное дело, поручение следователя, сведения о признаках подготавливаемого преступления)[49].

Так, для проведения контрольной закупки, в рамках которой предполагается сбор и использование данных о частной жизни лица, необходимо не только наличие конкретных оснований, но выполнение конкретной задачи[50], указанной в законе. Подводя к выводу о возможности ограничения права на неприкосновенность частной жизни, суд исходит из того, что в случае если вышеназванные ограничения соблюдаются органами государственной власти, уполномоченными на осуществление оперативно-розыскных мероприятий, подобные мероприятия не противоречат конституционным правам граждан. Несмотря на конституционный запрет, Федеральный закон об оперативно-розыскной деятельности все же предусматривает возможность разглашения фактов и информации о частной жизни лица, указывая, что случаи распространения могут быть изложены в других нормативно-правовых актах.

---

[48] Решение о проведении оперативно-розыскных мероприятий должно и может быть принято для достижения целей, перечисленных в статье 4 Федерального закона «Об оперативно-розыскной деятельности» № 144-ФЗ от 12.08.1995.

[49] Перечень оснований для проведения оперативно-розыскных мероприятий закреплен в статье 7 Федерального закона «Об оперативно-розыскной деятельности» № 144-ФЗ от 12.08.1995.

[50] Возможность разглашения органами, осуществляющими оперативно-розыскные мероприятия, информации о частной жизни лица, регламентирована статьей 5 Федерального закона «Об оперативно-розыскной деятельности» № 144-ФЗ от 12.08.1995.

Поскольку в рамках настоящего исследования мы стараемся выделить общие черты, присущие как частной жизни, так и персональным данным, полагаем, что весьма целесообразным будет обратить внимание на определение частной жизни, которое используется Конституционным Судом в решении по жалобе лица на нарушение его права на неприкосновенность частной жизни положениями Закона об оперативно-розыскной деятельности, предусматривающими возможность сбора данных в ходе осуществления контрольной закупки. Для толкования понятия «частная жизнь», Конституционный Суд обращается к принятому ранее своему определению[51]. Согласно более раннему определению под частной жизнью лица следует понимать «ту область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она не носит противоправный характер». Данная область жизнедеятельности или часть жизни лица должна защищаться от своевольного вмешательства государственной власти.

Возвращаясь к конкретному случаю установки и использования видеозаписывающего устройства, собирающего данные о внутренней обстановке жилища, равно как и данные о предметах, документах и лицах, пребывающих в жилище, полагаем, что целесообразным в данном случае будет характеризовать подобные действия как вмешательство в ту область жизнедеятельности человека, которая не подлежит контролю со стороны государства и общества, и которая должна быть защищена от постороннего вмешательства. Развивая подобный тезис, необходимо сказать и о том, что к лицу (несанкционированный владелец), в распоряжении которого окажутся данные о частной жизни других лиц, при условии, что несанкционированным владельцем не было получено согласие других лиц, следует применять такие правовые последствия, которые предусмотрены в случае наступления ответственности за нарушение конституционного права на неприкосновенность частной жизни.

Нам также следует задаться вопросом, а какие данные позволяют определить физическое лицо. Данный вопрос обусловлен самой дефиницией персональных данных, которая определяется в законе. Согласно нормативным положениям под персональными данными следует понимать «любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»[52]. Следует проводить

[51] Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» ч. 3 ст. 125 и ч. 3 ст. 127 Уголовно-исполнительного кодекса РФ : определение Конституционного Суда РФ от 09.06.2005 № 248-О // СПС «КонсультантПлюс».

[52] Статья 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» вводит определения понятия «персональные данные».

различия между такими понятиями, как информация, которая позволяет прямо определить физическое лицо, и информация, благодаря использованию которой можно лишь косвенно определить физическое лицо, то есть с достаточной долей вероятности определить личность (установить лицо) за счет использования или обращения к косвенным признакам. В судебной практике не встречается тех доводов, которые позволили бы дать характеристику информации в части того, является ли информация, выступающая предметом спора, тем признаком, благодаря которому можно прямо или косвенно установить физическое лицо. Подобный вопрос является важным, поскольку нам в рамках настоящего исследования хотелось бы понять, к какому типу информации следует отнести внутреннюю обстановку жилища физического лица, равно как и факты пребывания других лиц в жилище физического лица.

Следует начать с изучения вопроса о том, какая информация позволяет прямо определить физическое лицо. Информация, которая относится к определенному или позволяет прямо определить конкретное физическое лицо? Любая информация, которая относится к прямо или косвенно определяемому физическому лицу? На сегодняшний день в российской правоприменительной практике отсутствуют рекомендации, позволяющие выделить критерии для отнесения информации к такой, которая относится к прямо определяемому физическому лицу. Для ответов на подобные вопросы мы постарались изучить данные, представленные на информационной платформе в информационно-телекоммуникационной сети «Интернет», которая называется «Портал персональных данных уполномоченного органа по защите прав субъектов персональных данных». Органом государственной власти, уполномоченным на размещение материалов на данной информационной платформе, является Федеральная служба по надзору в сфере связи, информационных технологий и массовых телекоммуникаций. Тем не менее на данной платформе отсутствует информация, позволяющая ответить на вопрос: что является информацией, относящейся к прямо определяемому физическому лицу.

Следует отметить, что в российском законодательстве, равно как и в российской правоприменительной практике, отсутствует определение понятия «определяемое физическое лицо». Например, Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Уральскому федеральному округу дается разъяснение понятия «персональные данные»[53]. В указанном разъяснении всего лишь

[53] Разъяснение понятия «персональные данные» опубликовано Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Уральскому федеральному округу на своей официальной веб-странице в информационно-телекоммуникационной сети «Интернет». URL: https://66.rkn.gov.ru/directions/p18760/p20284/

цитируется определение, закрепленное в Федеральном законе о персональных данных. После цитирования законодательной нормы происходит перечисление конкретной информации (перечень переменных), с помощью которой можно однозначно определить физическое лицо – субъекта персональных данных. Указанные переменные и признаются персональными данными (ФИО, адрес места жительства, данные СНИЛС, номер банковских счетов и вкладов). Разъяснения или дефиниции понятия «определяемое физическое лицо» на официальном сайте Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационной сети «Интернет» не представлено. Если говорить о получении изображения конкретного лица, включая черты лица и его телосложения, за счет использования видеозаписывающего устройства, то на странице с разъяснениями уральского Управления Роскомнадзора отсутствует информация, которая позволила бы ответить на вопрос: **возможно ли определить физическое лицо за счет использования фото- или видеоизображения физического лица и номера квартиры, в которой физическое лицо проживает**. Будет ли считаться сбор подобных сведений обработкой персональных данных, если нет возможности четко определить, есть ли у оператора персональных данных намерение определить физическое лицо за счет сбора указанных сведений. Тем не менее на той же странице с разъяснением Управления Роскомнадзора по Уральскому округу сказано, что размещение изображения физического лица на страницах в информационно-телекоммуникационной сети «Интернет» без публикации какой-либо сопроводительной информации о лице на изображении не является обработкой персональных данных[54].

При попытке найти определение понятия «определяемое физическое лицо» на страницах официального сайта Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, авторами настоящей статьи обнаружено, что в целях разъяснения положений федерального законодательства о персональных данных и обобщения практики рассмотрения споров, связанных с персональными данными, на официальном сайте Роскомнадзора размещается и наполняется информационно-справочная платформа – Портал персональных данных Уполномоченного органа по защите прав субъектов персональных данных. Данный портал можно найти на странице официального сайта Роскомнадзора в информационно-телекоммуникацион-

[54] Ответ Управления Роскомнадзора по Уральскому федеральному округу на вопрос: является ли обработкой персональных данных размещение на сайтах в сети «Интернет» фотографий без иной дополнительной информации? URL: https://66.rkn.gov.ru/directions/p18760/p20284/

ной сети «Интернет»[55]. Так, для поиска определения понятия «определяемое физическое лицо» проведено исследование материалов, опубликованных Роскомнадзором в конкретном разделе портала – «Электронная библиотека по защите прав субъектов персональных данных» (подраздел «Методические рекомендации»). В материалах, опубликованных на страницах электронной библиотеки, не представлено определение понятия «определяемое физическое лицо». В ходе изучения информации и данных, представленных в других разделах информационно-справочного портала по защите прав субъектов персональных данных, определения вышеназванного понятия не найдено.

[55] URL адрес Портала персональных данных Уполномоченного органа по защите прав субъектов персональных данных (страница веб-сайта Роскомнадзора): https://pd.rkn.gov.ru/

Татьянина Лариса Геннадьевна,

доктор юридических наук, профессор, заведующая кафедрой уголовного процесса и криминалистики,

Решетнева Татьяна Васильевна,

кандидат юридических наук, доцент, заведующая кафедрой теории и истории государства и права,

Решетникова Гульнара Аликовна,

кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии

ПРИНЦИПЫ ПРАВОСУДИЯ КАК ПРАВОВЫЕ БАРЬЕРЫ ОГРАНИЧЕНИЯ ДЕЯТЕЛЬНОСТИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Создание технологий искусственного интеллекта, их внедрение и использование в разнородных областях общественной жизни, всевозрастающая зависимость человека от современных технологий порождают ряд научных дискуссий, связанных с трансформацией правовых концепций, ввиду необходимости правового регулирования и этой сферы. Динамично укореняются названные технологии и во внутригосударственной юридической практике некоторых государств, куда также входит сфера правосудия.

Современные общественные отношения, в которых задействованы системы искусственного интеллекта, имеют начавшуюся формироваться правовую основу. В настоящее время документы, регулирующие отношения в сфере разработки и применения систем искусственного интеллекта, с одной стороны, устанавливают задачи по созданию условий для развития основ правового режима этих общественных отношений, а с другой стороны, определяют правовые барьеры, препятствующие этому процессу.

Обеспечительные меры развития правовых отношений в сфере систем искусственного интеллекта ставят перед наукой вопросы о будущем процесса отправления правосудия в ситуации его автоматизации, в том числе и о его полной автоматизации – замены судьи системой сильного (или универсального) искусственного интеллекта, сравнимого с человеческим интеллектом или превосходящим его, то есть способного проанализировать фактические обстоятельства дела, дать им правовую оценку и вынести соответствующее (адекватное) решение.

Существующие подходы отечественных и зарубежных ученых, разработанные рядом международных межправительственных организаций концептуальные идеи (принципы), направленные на обеспечение безопасного развития и использования искусственного интеллекта, позволяют осуществить правовое моделирование пределов внедрения технологий искусственного интеллекта в систему отправления российского правосудия, установить ключевые факторы, препятствующие этому процессу, спрогнозировать основные риски внедрения рассматриваемых технологий.

На современном этапе – уровне начального правового регулирования применения технологий искусственного интеллекта – в российском правосудии актуализируется вопрос о способности закрепленных и действующих в российском законодательстве принципов правосудия влиять на ограничение деятельности систем искусственного интеллекта в контексте социального предназначения правосудия, что, в свою очередь, требует установления влияния социальной среды, и, следовательно, социальной обусловленности внедрения систем искусственного интеллекта в сферу правосудия, исследования мирового опыты и существующих в современной науке подходов к внедрению систем искусственного интеллекта в сферу правосудия, изучения международных документов, устанавливающих основные принципы допустимости, пределы и безопасность использования систем искусственного интеллекта, рассмотрения деятельности систем искусственного интеллекта на предмет способности этой деятельности соответствовать содержанию принципов правосудия и возможных угроз в случае легализации и легитимации этой деятельности.

Правовая основа использования технологий искусственного интеллекта в России заложена в Федеральном законе от 23.06.2016 № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти»[56], Указе Президента РФ № 490 от 10.10.2019 «О развитии искусственного интеллекта в Российской Федерации» вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»[57] (*далее* – Стратегия), распоряжении Правительства РФ № 2029-р от 19.08.2020 «Об утверждении Концепции развития регулирования отношений в сфере технологий

[56] О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти : Федеральный закон № 220-ФЗ от 23.06.2016. URL: https://www.consultant.ru/document/cons_doc_LAW_200008/

[57] О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ № 490 от 10.10.2019. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/

искусственного интеллекта и робототехники до 2024 года»[58] (далее – Концепция), Федеральном законе № 123-ФЗ от 24.04.2020 «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»[59] (*далее* – Закон).

В соответствии со ст. 2 Закона искусственный интеллект определяется как комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру (в том числе информационные системы, информационно-телекоммуникационные сети, иные технические средства обработки информации), программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений[60].

Согласно Стратегии использование технологий искусственного интеллекта в Российской Федерации обусловлено целью обеспечения национальных интересов и реализации стратегических национальных приоритетов, в том числе в области научно-технологического развития[61], которое, в соответствии с Концепцией, должно опираться на надлежащее правовое регулирование новых общественных отношений, складывающихся в связи с разработкой и применением технологий искусственного интеллекта и робототехники и систем на их основе, а также на определение правовых барьеров, препятствующих разработке и применению указанных систем[62].

---

[58] Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года : распоряжение Правительства РФ № 2029-р от 19.08.2020. URLhttps://www.consultant.ru/document/cons_doc_LAW_360681/

[59] О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : Федеральный закон № 123-ФЗ от 24.04.2020. URL: https://www.consultant.ru/document/cons_doc_LAW_351127/

[60] Там же.

[61] О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ № 490 от 10.10.2019. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/

[62] Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года : распоряжение Правительства РФ № 2029-р от 19.08.2020.

В современных условиях для развития и использования технологий искусственного интеллекта, с одной стороны, необходима адаптация нормативного регулирования в части, касающейся взаимодействия человека с искусственным интеллектом, а с другой стороны, выработка соответствующих норм. При этом необходимо соблюдение баланса, то есть недопущения избыточного регулирования, которое может существенно замедлить темп развития и внедрение технологических решений[63]. В то же время правовое регулирование должно исключать возникновение случаев, связанных с риском причинения вреда жизни и здоровью граждан, с нарушением прав и свобод человека, создающих явную угрозу обороне страны и безопасности государства[64]. Можно заключить, что:

1) внедрение технологий искусственного интеллекта в судебную систему государств, в том числе и в судебную систему России, свидетельствует о способности уже действующих в государстве процессуальных норм осуществлять регулятивное правовое воздействие на осуществление (отправление) правосудия при помощи технологий искусственного интеллекта и выступать одновременно правовым барьером, не допускающим отправление правосудия системой искусственного интеллекта;

2) в любом государстве его основной обязанностью является обеспечение им безопасности личности, общества и самого себя. Преобразование этой концептуальной основы произойдет лишь с изменением экономического и политического строя. Но этого не предвидится, по крайней мере, в ближайшие десятилетия, исходя из базовых документов, определяющих национальные интересы Российской Федерации. Следовательно, никакой трансформации не будет, а будет органичное сочетание существующей концептуальной идеи с новыми реалиями (развитие систем искусственного интеллекта), в наши дни уже ставшими неотъемлемой, социально обусловленной частью как общественных, так и правовых отношений;

3) в случаях, когда технологии искусственного интеллекта внедряются в судебную правоприменительную деятельность, необходимо обеспечить, чтобы использование технологий искусственного интеллекта:

– не создавало препятствий при осуществлении права на доступ к правосудию и права на справедливое судопроизводство;

---

[63] См. Указ Президента РФ № 490 от 10.10.2019 «О развитии искусственного интеллекта в Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_335184/

[64] См. распоряжение Правительства РФ № 2029-р от 19.08.2020 «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года». URLhttps://www.consultant.ru/document/cons_doc_LAW_360681/

– в процессе принятия решений в полной мере осуществлялось бы в полном соответствии с принципами верховенства права, независимости судей;

– являлось лишь вспомогательным средством для достижения юридической справедливости.

В Стратегии сфера правосудия не значится в числе приоритетных направлений развития и использования технологий искусственного интеллекта, тем не менее, начиная с 2017 года, в России заработала система внедрения технологий искусственного интеллекта, которая связана с возможностью подачи электронных документов, закрепленной в обновленных редакциях процессуальных кодексов РФ.

Несмотря на то, что использование технологий искусственного интеллекта в правосудии – это объективная реальность, тем не менее в научном мире ведутся активные дискуссии о пределах допустимого использования данных технологий в практике судов, возможности внедрения в практику «киберсудов» и «делегировании им полномочий» по принятию решений[65].

Многие авторы придерживаются позиции, что система электронного правосудия не должна быть направлена лишь на внешнее функционирование суда. По их мнению, в России система искусственного интеллекта при отправлении правосудия может быть использована судами уже сегодня[66], например по делам, где деятельность человека носит контролирующий (ревизионный) характер, в частности по делам о долговых обязательствах[67], гражданских и административных дел по бесспорным требованиям[68], дела приказного

---

[65] См.: *Анисимова А.С., Спиридонова М.П.* К вопросу о возможностях использования технологий искусственного интеллекта в правосудии // Юридический вестник ДГУ. 2021. Т. 39, № 3. С. 163, 164; *Бирюков П.Н.* Искусственный интеллект и «предсказанное правосудие: зарубежный опыт // Lexrussica. 2019. № 11 (156). С. 85; *Луценко Е.П.* Применение искусственного интеллекта при осуществлении правосудия в России и за рубежом // Образование и право. 2022. № 6. С. 221; *Чистилина Д.О.* Использование возможностей искусственного интеллекта в уголовном процессе // Вестник Удмуртского университета. Серия «Экономика и право». 2021. Т. 31, вып. 4. С. 708–710.

[66] См.: *Новикова К.С.* Искусственный интеллект как элемент электронного правосудия: смарт – решение и электронные весы правосудия // Образование и право. 2020. № 3. С. 240–242.

[67] *Макутчев А.В.* Современные возможности и пределы внедрения искусственного интеллекта в систему правосудия // Актуальные проблемы российского права. 2022. Т. 17, № 8 (141). С. 56.

[68] *Момотов В.В.* Искусственный интеллект в судопроизводстве: состояние, перспективы использования // Вестник университета имени О.Е. Кутафина (МГЮА). 2021. № 5. С. 190.

производства, дела о расторжении брака, если отсутствует спор о детях[69]. К.С. Новикова[70] отмечает, что в указанных случаях, искусственный интеллект, проанализировав обстоятельства дела, предлагает на утверждение судьи «смарт-решение» или даже несколько вариантов, возможно, даже с резолютивной частью. Ценность этого подхода видится К.С. Новиковой в повышении качества правосудия, поскольку с помощью искусственного интеллекта будут рассматриваться несложные, однотипные дела, что позволит высвободить время судье и создаст условия для его подготовки к рассмотрению более сложных дел[71]. О.А. Степанов и Д.А. Басангов[72] считают, что, в сущности, использование таких систем не подменяет судью, поскольку их использование способствует ускорению сбора и обработки материалов по делу, большей объективности, лучшему контролю подлинности информации, полученной при рассмотрении дела. Они пишут: «Современные возможности искусственного интеллекта позволяют не только достаточно точно распознавать юридические ситуации, но, и что еще более важно, без потерь описать законы на логическом, а соответственно, и программном языках. При этом предполагается, что алгоритмы искусственного интеллекта будут всегда оставаться объективными, беспристрастными, сохранять нейтралитет и безупречную репутацию, что способно существенно облегчить работу судьи, то есть позволит снизить нагрузку на судебный аппарат, ускорить и усовершенствовать отправление правосудия, исключить судебную волокиту и коррупцию»[73].

Отсутствие единообразного подхода в вопросах использования технологий искусственного интеллекта в правосудии отразилось и на практике их внедрения в государствах, которые, по мнению А.В. Макутчева, могут оперировать несколькими концепциями: консервативной, экстенсивной или интенсивной. Для первой концепции характерно лишь расширение внедрения цифровизации в судебную систему и распространение электронного правосудия. Во втором случае происходит ограничение в системе правосудия технологий искусственного интеллекта. При использовании экстенсивной концепции решения принимаются судьей без непосредственного участия систем искусственного интеллекта. Целью названной концепции является облегчение деятельности

---

[69] *Степанов О.А., Басангов Д.А.* О перспективах влияния искусственного интеллекта на судопроизводство // Вестник Томского государственного университета. 2022. № 475. С. 232.

[70] *Новикова К.С.* Указ. соч. С. 242.

[71] Там же.

[72] *Степанов О.А., Басангов Д.А.* Указ. соч. С. 231.

[73] Там же. С. 231.

судьи. Наконец, использование интенсивной концепции предполагает глубокое использование технологий искусственного интеллекта в системе правосудия, то есть когда происходит какая-либо и (или) полная замена судьи искусственным интеллектом при принятии решения[74].

В настоящее время наиболее привлекательным, к которому приковано внимание большинства ученых и практиков, является опыт Китая по использованию технологий искусственного интеллекта в правосудии, позволивший к настоящему времени подготовить более 3 млн решений. Так, еще в 1999 году в Китае был составлен поэтапный план внедрения в систему народного суда технологий искусственного интеллекта. Первые два этапа были связаны с компьютеризаций, информатизацией, цифровизацией и коснулись делопроизводства и документооборота, а также создания национальной электронной системы правосудия. На третьем этапе, начиная с 2016 года стали применяться технологии искусственного интеллекта – судьи-робота, способного к самообучению, вынесению судебных решений и умеющего исправлять судебные ошибки. Однако деятельность судьи-робота носит подконтрольный характер, то есть вынесенное судебное решение всегда может быть изменено судьей – человеком. Научная общественность Китая пользу в описанном эксперименте видит главным образом для решения проблемы загруженности судей. Но к вопросу о передаче искусственному интеллекту возможности вынести судебное решение относится крайне настороженно. К 2025 году в Китае планируется создание системы искусственного интеллекта для поддержки судебной системы, но при этом не предполагается замена «живых» судей искусственным интеллектом, применение последнего направлено будет только на решение рутинных задач, а все решения будут принимать только сами судьи.

Сложно предугадать, как будут развиваться технологии искусственного интеллекта в будущем, и насколько сильна будет зависимость человека от искусственного интеллекта. Тем не менее с учетом тех негативных последствий, которые могут наступить в случае бесконтрольного использования этих технологий, уже сейчас обнаруживают важность разработки, официального признания и внедрения в юридическую практику этических норм использования искусственного интеллекта. Об этом неоднократно говорилось отдельными государствами и озвучивалось на международных площадках.

Так, соответствующие предложения по созданию системы принципов были предложены в рамках международных межправительственных организаций. Подготовленные международными организациями документы содержат нормы

[74] *Макутчев А.В.* Указ. соч. С. 51–53.

международного «мягкого» права, по природе своей являющиеся рекомендательными. Однако государства могут их использовать через механизм имплементации (включения) разработанных принципов во внутригосударственные источники права. На универсальном уровне все 193 государства-члена ЮНЕСКО одобрили документ, определяющий общие ценности и принципы, необходимые для обеспечения безопасного развития и использования искусственного интеллекта. При этом особо подчеркивается, что разработка нормативно-правовой базы, призванной регулировать отношения, связанные с использованием технологий искусственного интеллекта, должна быть ориентирована на человека, способствовать уважению его прав[75]. За разработку соответствующей нормативной основы и минимальных нормативных стандартов по использованию технологий искусственного интеллекта выступают и зарубежные ученые[76].

На региональном уровне в ряде международных межправительственных организаций также были приняты соответствующие документы. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств в своем Постановлении № 53-12 (от 26.11.2021) сформулировала принципы, лежащие в основе разработки и внедрении цифровых технологий: 1) универсальная значимость. Данный принцип предполагает, что используемые цифровые технологии для общественности должны быть понятны и внедряться и распространяться таким образом, «чтобы в равной степени способствовать благополучию отдельных людей и общества в целом» [пункт 4.1]; 2) устойчивость развития, как принцип, связан с безопасностью, этичностью исследовательской деятельности и преобразований в сфере цифровых технологий, с внесением вклада в развитие государства, в целях устойчивого развития общества, ненанесения вреда не только людям, но и животным, растениям и окружающей среде, исключая возникновение биологической, физической или нравственной угрозы как в настоящем, так и в будущем [пункт 4.2]; 3) снижение рисков означает, что внедрение цифровых технологий осуществляется с осторожностью, исходя из возможных воздействий на окружающую среду, здоровье и безопасность людей, с принятием всех необходимых мер информационной безопасности, стремясь к прогрессу во благо общества и природной среды [пункт 4.3];

[75] Этические аспекты искусственного интеллекта // UNESCO. URL: https://www.unesco.org/ru/artificial-intelligence/recommendation-ethics

[76] Ponce del Castillo, Aida, A Law on Robotics and Artificial Intelligence in the EU? (October 3, 2017). ETUI Research Paper – Foresight Brief #02-September 2017, Available at SSRN: https://ssrn.com/abstract=3180004 or http://dx.doi.org/10.2139/ssrn.3180004; Leenes, Ronald E. and Leenes, Ronald E. and Lucivero, Federica, Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design (November 28, 2014). Law, Innovation and Technology (2014) 6(2) LIT 194–222, Available at SSRN: https://ssrn.com/abstract=2546759

4) открытость управления при применении цифровых технологий связана «с установкой на прозрачность и законным правом личности на доступ к информации», с правом участия в принятии решений всех субъектов, которые действуют в этой сфере или соприкасаются с ней, при обязательном гарантировании при использовании, применении цифровых технологий уважения к частной жизни и конфиденциальность [пункт 4.4]; 5) в основе принципа научности лежит соответствие цифрового развития «высоким стандартам», основанным на добросовестной научной деятельности при разработке цифровых технологий [пункт 4.5]; 6) инновационность связана с тем, что «управление деятельностью в сфере цифрового развития должно быть направлено на всевозможное поощрение творческой активности, а также выработку способности к адаптации и планированию для поддержания инновационного характера и дальнейшего развития цифровых технологий» [пункт 4.6]; 7) ответственность предполагает, что «как отдельные исследователи и технологии, так и организации должны нести ответственность за социальные и экологические последствия, равно как и воздействие на здоровье (прежде всего когнитивные нарушения), которые могут возникнуть в результате внедрения цифровых технологий, не только перед ныне живущими людьми, но и перед будущими поколениями» [пункт 4.7].

В марте 2023 года в рамках СНГ завершена работа над «проектом Рекомендаций по нормативному регулированию использования искусственного интеллекта, включая этические стандарты для исследований и разработок для стран Содружества», которые должны выполнить функцию «дорожной карты для формирования системы законов в сфере искусственного интеллекта на территории СНГ»[77]. При этом подчеркивается, что при использовании систем искусственного интеллекта не должна быть допущена возможность «манипуляции поведением человека и дискриминации граждан».

В пункте 57 Пекинской декларации XIV саммита БРИКС (от 23.06.2022) государства признали «огромный потенциал технологий искусственного интеллекта», который необходимо направить на максимальное его использование на благо общества и человечества, одновременно выразив «обеспокоенность рисками и этическими дилеммами, связанными с искусственным интеллектом, такими как, в частности, неприкосновенность частной жизни, манипулирование, предвзятость, взаимодействие человека и робота, последствия и сингулярность»[78]. В связи с чем государства-члены БРИКС высказали намерение и далее

[77] Парламентарии стран СНГ приняли рекомендации по регулированию использования искусственного интеллекта (iacis.ru) // URL: https://iacis.ru/novosti/postoyannye_komissii/parlamentarii_stran_sng_prinyali_rekomendatcii_po_regulirovaniyu_ispolzovaniya_iskuss%20tvennogo_intellekta?ysclid=ln7cvudlk5844984316

[78] Пекинская декларация XIV саммита БРИКС // Президент России (kremlin.ru). URL: http://www.kremlin.ru/supplement/5819

осуществлять совместную работу, направленную на «устранение этих озабоченностей» и разработку «общего подхода к управлению», который будет служить руководством «в отношении этического и ответственного использования искусственного интеллекта»[79].

Заслуживает внимания Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях (Страсбург, 3 декабря 2018 года)[80], принятая в рамках Совета Европы Европейской комиссией по эффективности правосудия и содержащая пять принципов использования искусственного интеллекта для повышения качества правосудия, а именно: 1) принцип уважения основополагающих прав: обеспечить разработку и внедрение инструментов и услуг, основанных на искусственном интеллекте, соответствующих основным правам; 2) принцип недискриминации; принцип качества и безопасности: определенным образом препятствовать развитию или усилению любой дискриминации между отдельными лицами или группами лиц; 3) принцип качества и безопасности: при обработке судебных решений и данных необходимо использовать сертифицированные источники и нематериальные данные с применением моделей, разработанных на междисциплинарной основе, в безопасной технологической среде; 4) принцип прозрачности, беспристрастности и достоверности: сделать методы обработки данных доступными и понятными, разрешить проведение внешнего аудита; 5) принцип контроля пользователем: избегать предписывающего подхода и позволить пользователю выступать в роли информированного лица, ответственного за свой выбор. Безусловно, все названные принципы имеют определяющее значение для использования технологий искусственного интеллекта в правосудии, однако в их иерархии ключевое место занимает пятый принцип – «принцип пользовательского контроля», как его определил В.В. Момотов. Суть принципа состоит в том, что судья может иметь собственное мнение по решению, вынесенному искусственным интеллектом. Кроме того, стороны спора не утрачивают права

[79] Пекинская декларация XIV саммита БРИКС // Президент России (kremlin.ru). URL: http://www.kremlin.ru/supplement/5819

[80] Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. Принята на 31-м пленарном заседании ЕКЭП 3–4 декабря 2018 г. URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4. Несмотря на то, что с 16 марта 2022 года прекращено членство России в Совете Европы, сравнительно-правовой анализ, изучение документов Совета Европы, других международных организаций, включая акты, связанные с технологиями искусственного интеллекта, государствами, не являющимися членами организаций могут быть полезны в части использования тех положений, которые с учетом национальных интересов государств, включая и Россию, допустимы к имплементации во внутригосударственную правовую систему.

непосредственного обращения в суд и рассмотрения их дела без использования искусственного интеллекта. Также стороны не утрачивают права обжаловать решение, вынесенное искусственным интеллектом. Принцип «пользовательского контроля», – считает В.В. Момотов, – ясно показывает, что авторы документа, принятого в Совете Европы, отчетливо осознают бесперспективность альтернативы искусственного интеллекта судье[81]. Названная позиция в науке является основной.

В концентрированном виде суть этического регулирования отношений, возникающих при использовании технологий искусственного интеллекта, разработанных в рамках международных организаций, можно представить следующим образом: *использование технологий искусственного интеллекта:* 1) должно обеспечивать права человека, безопасность и благополучие человека; 2) необходимо осуществлять таким образом, чтобы не причинять вред человеку, обществу, человечеству; 3) должно быть подконтрольно человеку на всех стадиях его использования; 4) невозможно без признания юридической ответственности лиц, ответственных за действия конкретных систем искусственного интеллекта.

Возвращаясь к проблеме полной замены судьи системой искусственного интеллекта, в подавляющем большинстве случаев в научной и профессиональной среде высказываются аргументы «против». В частности, по мнению противников, технологии искусственного интеллекта не способны учесть: все детали дела, в том числе человеческий фактор[82]; нормы морали и этики, эмоциональное состояние, детали обстановки и другие характеристики, относящиеся только к человеческой жизнедеятельности[83]. Кроме того, у искусственного интеллекта отсутствует чувство ответственности, самоанализа и самоконтроля[84], а также способность оценить абстракцию, понять смысл[85] и фабулу дела[86], отсутствует

---

[81] *Момотов В.В.* Доклад на пленарном заседании участников Глобальной сети обеспечения честности и неподкупности судебных органов (GlobalJudicialIntegrityNetwork) под эгидой Управления ООН по наркотикам и преступности на тему: «Перспективы использования искусственного интеллекта в судебной системе Российской Федерации» ; Катар, 26 февраля 2020 г. URL: http://www.ssrf.ru/news/lienta-novostiei/36912

[82] *Степанов О.А., Басангов Д.А.* Указ. соч. С. 233.

[83] Там же. С. 233.

[84] *Новикова К.С.* Указ. соч. С. 242.

[85] *Макутчев А.В.* Указ. соч. С. 55.

[86] *Момотов В.В.* Доклад на пленарном заседании участников Глобальной сети обеспечения честности и неподкупности судебных органов (GlobalJudicialIntegrityNetwork) под эгидой Управления ООН по наркотикам и преступности на тему: «Перспективы использования искусственного интеллекта в судебной системе Российской Федерации» ; Катар, 26 февраля 2020 г. URL: http://www.ssrf.ru/news/lienta-novostiei/36912

умение использовать ценностные критерии оценки[87], а также навык восполнения пробела в законодательстве исходя из аналогии права, когда в случае отсутствия конкретной правовой нормы, возникает необходимость вынесения решения по делу, используя общий смысл законодательства. Технологии искусственного интеллекта на данном уровне своего развития не имеют внутреннего убеждения[88], позволяющего принимать решения. И, конечно, присутствуют опасения вытеснения искусственным интеллектом человека из конкретной области[89], в том числе и из сферы правосудия. Кроме того, в современных цивилизационных условиях искусственный интеллект пока не получил массовой поддержки среди населения[90], и легальное использование технологий искусственного интеллекта в той или иной сфере не делает их легитимными.

Думаем, что ни один из перечисленных факторов сам по себе не является прочным и неподдающимся опровержению аргументом, убеждающим в неспособности отправления правосудия системой искусственного интеллекта[91]. Непрерывное развитие систем искусственного интеллекта, масштабы его развития и глубина свидетельствуют о его вероятной способности преодолеть и эти барьеры.

Ближе к таким факторам, преодолеть которые для отправления правосудия системой искусственного интеллекта не получится, являются принципы правосудия как отправные идеи, отображающие основные черты политического, экономического, культурно-нравственного и правового развития общества и государства[92].

В этой связи реальное внедрение технологий искусственного интеллекта в судебную систему государств, в том числе и в судебную систему России, ставит справедливый вопрос о способности уже действующих в государстве

---

[87] *Момотов В.В.* Доклад на пленарном заседании участников Глобальной сети обеспечения честности и неподкупности судебных органов (GlobalJudicialIntegrityNetwork) под эгидой Управления ООН по наркотикам и преступности на тему: «Перспективы использования искусственного интеллекта в судебной системе Российской Федерации» ; Катар, 26 февраля 2020 г. URL: http://www.ssrf.ru/news/lienta-novostiei/36912

[88] Там же.

[89] *Закиров Р.Ф.* Цит. по: *Макутчев А.В.* Современные возможности и пределы внедрения искусственного интеллекта в систему правосудия // Актуальные проблемы российского права. 2022. Т. 17, № 8 (141). С. 14.

[90] *Степанов О.А., Басангов Д.А.* Указ. соч. С. 233.

[91] *Решетникова Г.А.* Факторы, препятствующие оправлению правосудия системой искусственного интеллекта // Процессуальные гарантии современного правосудия: к 100-летию Судебной системы в Удмуртской Республике : сб. ст. Ижевск : Удмуртский университет, 2023. С. 254.

[92] *Решетникова Г.А.* Указ. соч. С. 255.

процессуальных норм осуществлять регулятивное правовое воздействие на осуществление (отправление) правосудия при помощи технологий искусственного интеллекта и выступать одновременно правовым барьером, не допускающим отправление правосудия системой искусственного интеллекта. Так, при использовании технологий искусственного интеллекта важно исходить из того, что недопустимость осуществления правосудия системой искусственного интеллекта изначально обеспечивается самим понятием правосудия как вида государственной деятельности, в процессе которой реализуется судебная власть. Законодатель четко определил принципы правосудия, которые и выступают препятствием для использования искусственного интеллекта при осуществлении правосудия. При этом следует иметь ввиду, что отправление правосудия и порядок судебного разбирательства по рассмотрению и разрешению дела не являются тождественными. Правосудие осуществляется судом, который принимает решение на основе исследованных доказательств, то есть в основе принятия решения лежит мыслительная деятельность человека. Порядок судебного разбирательства связан с собиранием и проверкой доказательств. Законодатель не ограничивает форму судебного разбирательства и допускает возможность использования информационных технологий в ходе судебного заседания, в том числе при проведении судебных действий. Учитывая современные реалии, президент КСЕС указал: « …правосудие в современный период может быть осуществлено только в рамках судебной системы, которая организована как доступная для граждан и организаций цифровая платформа, функционирующая эффективно, безопасно и прозрачно. При этом суды должны иметь достаточные ресурсы, программное обеспечение и системы видеоконференции, чтобы адаптироваться к новым вызовам и угрозам, включая отсутствие возможности физического доступа в здание суда»[93]. Однако это не предполагает возможность замены суда искусственным интеллектом.

Одним из принципов правосудия является осуществление его только судом. Судебная власть в Российской Федерации принадлежит только судам в лице судей. Судьями являются лица, наделенные в конституционном порядке полномочиями осуществлять правосудие и исполняющие свои обязанности на профессиональной основе[94]. Соответственно, правосудие вершит судья, в качестве

[93] Консультативный Совет европейских судей (CCJE). Заявление президента КСЕС «Роль судей во время и после пандемии по COVID-19: уроки и проблемы». Страсбург, 24 июня 2020 г. URL: file:///C:/Users/Администратор/Downloads/CCJE (2020)2%20-%20Statement%20of%20the%20CCJE%20President%203%20-%20Lessons%20and%20challenges%20COVID%2019%20-%2024%20June%202020.pdf (дата обращения: 02.07.2021).

[94] О статусе судей в Российской Федерации : Закон РФ № 3132-1 от 26.06.1992. URL: https://www.consultant.ru/document/cons_doc_LAW_648/

которого выступает только человек. Подменить интеллектуальную деятельность человека искусственным интеллектом недопустимо, поскольку любое решение будет основано на использовании машиной определенной программы, созданной для принятия решения, при этом за ее качество создатели не смогут нести ответственность, поскольку просчитать возможности искусственного интеллекта, связанные с собственным перепрограммированием, весьма проблематично.

Одним из основополагающих принципов правосудия является независимость судей, которая обеспечивается Конституцией Российской Федерации, федеральным законодательством, действующим процессуальным законодательством. Независимость судей предполагает исключение конфликта интересов при осуществлении судебной деятельности, наличие юридических гарантий, применение мер безопасности и т.д. Судья при осуществлении правосудия зависит только от закона и принимает решения на основе судейского усмотрения, сформированного у каждого судьи и имеющего индивидуальный характер. Искусственный же интеллект не является независимым, поскольку изначально он формируется на основе созданной и заложенной программы, его функционирование связано с развитием технологий и т.д.

Принцип законности может соблюдаться только человеком, который применяет в своей деятельности нормы права. Учитывая, что нормы закона регулируют отношения между людьми, группами людей, деятельность людей и т.д., то применительно к искусственному интеллекту регламентируется нормами закона возможность его применения человеком, но не самостоятельное функционирование машины.

Сочетание коллегиальности и единоличности предполагает возможность осуществления правосудия единолично судьей или коллегиальным составом суда. Суд может использовать при производстве по делу в качестве технической помощи искусственный интеллект, но в данном случае речь будет идти не о деятельности искусственного интеллекта, а о использовании технических возможностей различных машин.

Состязательность и равноправие сторон, как принцип правосудия, однозначно исключают использование искусственного интеллекта. Состязательность сторон – участников конфликта исключает возможность выступления одной из сторон искусственного интеллекта. Сторона может использовать машину, иную технику в конфликте, но стороной конфликта будет человек. Равноправие сторон исключает изначально возможность равенства между человеком и машиной, поэтому речь может идти только о человеке.

Обязательность судебных решений заключается в том, что любое судебное решение обязательно для исполнения человеком, к которому оно обращено. Машина может быть использована в качестве вспомогательного объекта при исполнении решения, но она не может быть субъектом его реализации.

Гласность судебного заседания заключается в проведении открытого судебного заседания. Искусственный интеллект не может самостоятельно вести процесс и может быть использован в качестве технического средства, обеспечивающего возможность получения информации.

Равенство перед законом и судом может рассматриваться только в отношении сторон, в качестве которых выступают люди или группы людей. Машина не может иметь изначально равных прав с человеком независимо от ее качества.

Участие граждан в осуществлении правосудия связано с функционированием суда с участием коллегии присяжных заседателей. Данный состав суда рассматривается как гарантия защиты прав участников сторон конфликта, когда независимые присяжные граждане дают оценку произошедшего конфликта с учетом обыденного его восприятия. Вряд ли можно согласиться, что присяжных заседателей может заменить несколько машин, учитывая особенности их программирования, они не смогут дать различную оценку произошедшему, в противном случае необходимо будет искать ошибки в программе, но в которой – не совсем понятно.

Использование русского языка в судопроизводстве предполагает не формальный перевод слов, а знание тонкостей языка, выражений, которые позволят определить развитие конфликта. Ни одна машина с самой продвинутой программой не сможет определить тонкости языкового общения.

В заключении отметим, что теоретическое построение чего-либо должно быть подчинено основной идее. Все другие, пусть и значительные идеи, должны лишь ее конкретизировать. В любом государстве этой идеей является обеспечение государством безопасности личности, общества и самого себя. Преобразование обозначенной концептуальной основы произойдет, как было отмечено ранее, лишь с изменением экономического и политического строя.

Проведенное исследование позволило прийти к следующему основному результату: внедрение технологий искусственного интеллекта в судебную систему государств, в том числе и в судебную систему России, свидетельствует о способности уже действующих в государстве процессуальных норм осуществлять регулятивное правовое воздействие на осуществление (отправление) правосудия при помощи технологий искусственного интеллекта и выступать одновременно правовым барьером, не допускающим отправление правосудия системой искусственного интеллекта. Имеющиеся в научной литературе точки зрения о неспособности систем искусственного интеллекта осуществлять правосудие сами по себе не являются прочными и неподдающимися опров-жению аргументами. Непрерывное развитие систем искусственного интеллекта, масштабы его развития и глубина свидетельствуют о его вероятной способности преодолеть и эти барьеры, а факторами, препятствующими

отправлению правосудия системой искусственного интеллекта, являются именно принципы правосудия как отправные идеи, отображающие основные черты политического, экономического, культурно-нравственного и правового развития общества и государства.

Сформулированные выводы ориентированы на дальнейшую разработку предложений теоретического характера.

Татьянин Дмитрий Владимирович,

кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО УГОЛОВНОМУ ДЕЛУ В ДОСУДЕБНОМ ПРОИЗВОДСТВЕ

Досудебное производство по уголовному делу связано с большим количеством информации, которую получает следователь/дознаватель в процессе проведения доследственной проверки и предварительного расследования.

УПК РФ не содержит понятия «информация», но в ч. 2 ст. 84 УПК РФ указано: «Документы могут содержать сведения как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном ст. 86 УПК РФ», при этом понятие «носитель информации» в законе также отсутствует.

Согласно информационного подхода к понятию «доказательство», именно информация составляет его содержание[95]. В науке нет единого подхода к понятию «информация», согласно теории отражения информация может быть представлена как отражаемое разнообразие, а именно разнообразие, которое один объект содержит о другом объекте[96]. По мнению О.П. Аксаментовой, «в уголовном процессе способность информации к отражению выражается в процессе познания, когда речь идет о расследовании события преступления в поиске его следов в действительности»[97].

Исходя из процесса формирования информации, следует отметить, что она не существует в едином и неизменном виде. В зависимости от лица, которое ей обладает, его психофизических и интеллектуальных способностей, информация может быть преобразована им в процессе ее осмысления, оценки. На информацию, содержащуюся в иных источниках, может воздействовать внешняя среда ее нахождения, а также лица, заинтересованные в ее изменении, таким образом, информация может быть преобразована как естественным, так и искусственным путем.

---

[95] См.: *Балакшин В.С.* Доказательства в российском уголовном процессе: понятие, сущность, классификация : монография. Екатеринбург : УрГЮА, 2002.

[96] См.: *Урсул А.Д.* Природа информации : философский очерк. 2-е изд. Челябинск, 2010. С. 176–177.

[97] См.: *Аксаментова О.П.* О понятии информации в уголовном судопроизводстве // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 1. С. 29.

Информация о произошедшем событии вовлекается в уголовный процесс с момента начала проверки произошедшего, при этом временной период между событием и началом исследования может быть достаточно большим, поэтому в зависимости от указанного промежутка времени будет зависеть и информация, которая будет отражать произошедшее событие максимально или минимально приближённо к действительности; все будет зависеть от факторов, влияющих на сохранение информации.

В ходе доследственной проверки до установления длительных сроков производства в стадии возбуждения уголовного дела, на изменение первоначальной информации, отражающей событие, влияли в основном внешние факторы: время, погода, условия нахождения информации, ее содержание и т.п. В последующем при увеличении срока проведения проверки в указанной стадии, кроме внешних факторов, на изменение информации стал влиять и человеческий фактор, поскольку появилась возможность уже в ходе доследственной проверки повлиять на заявителя таким образом, чтобы он изменил выданную им информацию, в связи с чем преступление может быть оценено как административное правонарушение или гражданско-правовое отношение, что особенно остро поставило вопрос о необходимости принятия мер по обеспечению сохранения первоначальной информации.

В ходе предварительного расследования на информацию влияет более всего человеческий фактор, поскольку начинается противостояние между сторонами обвинения и защиты, а также обеспечение личных интересов участников процесса.

Для получения максимально объективной информации следует решить вопрос о принятии мер по ее сохранению. Наличие принципов, направленных на обеспечение защиты прав и законных интересов, тайны личной жизни и т.п., к сожалению, не обеспечивает реальное равенство граждан и единство при производстве по уголовному делу, что приводит к возможности не просто по уничтожению информации, но и ее преобразованию. Учитывая, что следователь в исключительных случаях начинает работать с потерпевшим, подозреваемым изначально, получая от них первоначальную информацию; в большинстве случаев проверка сообщений начинается с деятельности органа дознания, который уже влияет на содержание имеющейся информации, ее изменения.

Ни в коем случае не ставлю под сомнение профессионализм и порядочность оперативных работников, но следует учитывать, что в настоящее время многие оперативные работники не имеют достаточного опыта, умения, их психология направлена на обеспечение формального раскрытия преступления, применения гл. 40 УПК РФ при рассмотрении уголовного дела в суде, а последствия подобного раскрытия и расследования не имеют для них значения. Следователи

в указанном случае оказываются заложниками ситуации, когда осуществляют расследование, не имея возможности получить и проверить первоначальную информацию; ошибки могут привести к необоснованному привлечению к уголовной ответственности невиновного лица.

При проведении доследственной проверки и в последующем производства предварительного расследования не допустимо разглашение информации, которая составляет основу имеющихся доказательств и используется при принятии процессуальных решений.

Законодатель предусмотрел в ст. 144 УПК РФ право следователя, дознавателя предупреждать по своему усмотрению участников стадии возбуждения уголовного дела о недопустимости разглашения данных досудебного производства, а в ст. 161 УПК РФ – о недопустимости разглашения данных предварительного расследования. Изначально следует обратить внимание на то, что законодатель неудачно разделил понятие данных, разглашение которых недопустимо. Исходя из положений ч. 1.1 ст. 144 УПК недопустимо разглашение данных всего досудебного производства, которое включает и стадию предварительного расследования, но о каких данных, полученных в ходе ее производства может идти речь, если уголовное дело еще не возбуждено, а применительно к сохранению данных в процессе производства предварительного расследования законодатель указал только данные, которые получены в указанной стадии, а данные доследственной проверки, исходя из содержания указанной нормы, не должны сохраняться, но ведь именно они являются отправной точкой в процессе расследования преступления. В этой связи заслуживает поддержки предложение А.П. Липинского, предлагающего понимать под недопустимостью разглашения данных досудебного производства « ...запрет передачи информации, в том числе полученной в процессе участия в следственных или процессуальных действиях в ходе доследственной проверки или предварительного расследования, а также из материалов проверки или уголовного дела иным лицам под угрозой привлечения к установленной законом ответственности»[98].

Информация, которая содержится в материалах проверки и материалах уголовного дела не должна быть достоянием гласности, поскольку может повлиять на решение по уголовному делу как на отдельных этапах его производства, так и в целом. В современный период одним из наиболее сложных моментов является сохранение информации, полученной с использованием различных технологий, поскольку она является производственным процессом преобразования поступающих сигналов и их сохранения в доступной для дальнейшего

[98] См.: *Липинский А.П.* Обеспечение недопустимости разглашения данных досудебного производства : автореф. дисс. … канд. юрид. наук. Ижевск, 2023. С. 11.

воспроизведения форме. Технология сохранения полученных сигналов существенно различается, что позволяет выделить различные подвиды[99].

Информация, полученная с использованием различных технологий в ходе досудебного производства, может иметь как официальный, так и неофициальный характер. Возникают вопросы обеспечения сохранения информации, недопустимости ее уничтожения, искажения.

В целях обеспечения безопасности на улицах города, во дворах домов, подъездов и т.п. осуществляется видеозапись конкретных объектов, отрезков местности, которая сохраняется на различных носителях, принадлежащих тем предприятиям, организациям и т.д., которые осуществляли указанную запись. Допуск к указанной записи в определенных случаях доступен через отдел охраны конкретного предприятия, в некоторых случаях доступ можно получить достаточно просто, договорившись с лицом, которое обеспечивает сохранение, изъятие информации, замену носителей информации. В связи с чем возникает вопрос о недопустимости выдачи носителей информации либо копирования их лицами, которые не имеют отношения к устройствам видеофиксации.

Учитывая, что все виды видеофиксаторов направлены на получение данных, которые необходимы для установления фактических обстоятельств произошедшего в случае возникновения какой-либо спорной ситуации, предполагается, что передача ее может иметь место только в случае официального запроса от соответствующего органа, который в силу полномочий должен разрешить возникшую конфликтную ситуацию. При отсутствии официального запроса выдача информации/ее копии может иметь место только официальному лицу по предъявлении документов, подтверждающих право на ее получение, и официальной расписки указанного лица о получении соответствующего носителя информации, либо копирование последней на предоставленный лицом носитель. Необходимо в должностных инструкциях сотрудников охраны, работающих с техническими средствами, предназначенными для видеофиксации, установить обязанность о недопустимости передачи имеющейся на указанных носителях информации частным лицам. Следует указать также о недопустимости копирования указанной информации. В случае если на носителе информации сохранены данные, связанные с очевидным фактом совершения преступления, то указанная информация должна быть передана в органы предварительного расследования или дознания, при этом разглашение информации о ее наличии должно быть недопустимо. Вопрос об очевидности преступления определяется посредством оценки сохранившейся информации: если зафиксирован удар ножом, выстрел

[99] См.: *Глимейда В.В.* Применение технических средств и цифровых технологий при производстве следственных действий : дисс. ... канд. юрид. наук. Краснодар, 2024. С. 50.

в человека, наезд автомобиля на человека и т.п., то информация, бесспорно, не будет иметь частного характера. Ее необходимо сохранить для передачи сотрудникам правоохранительных органов.

Также существует проблема сохранения информации при утрате её источников информации. На стадии возбуждения уголовного дела многие данные получаются с помощью объяснений. Само объяснение в уголовном процессе может быть доказательством, только если предварительное расследование проводилось в форме упрощённого дознания. Возникает логичный вопрос: как нам быть, если опрошенное лицо умерло, сошло с ума, переехало в неизвестном направлении и по иным причинам не способно повторить информацию из объяснения на допросе? Формально данные у нас есть, но юридически их использовать невозможно. Для подобной ситуации считаю необходимым внести в УПК РФ специальную оговорку, добавив в пункт 5 часть 2 статьи 74 слово процессуальных в перечень протоколов, которые могут быть доказательствами по уголовному делу.

В целом можно сделать вывод о том, что при огромном значении информации для уголовных дел требуются адекватные меры для обеспечения её безопасности.

Тенсина Елена Фанавиевна,

кандидат юридических наук, доцент, доцент кафедры уголовного процесса и криминалистики

УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ РЕГУЛИРОВАНИЕ ЦИФРОВИЗАЦИИ ДОСУДЕБНОГО ПРОИЗВОДСТВА ПО УГОЛОВНОМУ ДЕЛУ

Термин «цифровизация», связанный со становлением цифровой экономики в России, широко используется в правовом, экономическом, психолого-педагогическом, социальном и гуманитарном секторах[100]. Разнообразие подходов объединяет главное – эффективность деятельности.

Перед юридической наукой и законодательством ставятся новые задачи, обусловленные развитием цифровых технологий, требующих новых подходов в правовом регулировании искусственного интеллекта, цифровых активов, цифровизации правоохранительной деятельности и судопроизводства и др. На современном этапе данная сфера условно определена Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2026 г., а также системой Указов Президента Российской Федерации: от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы», от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», № 490 «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 г.[101] И ряд других. Отчасти некоторые вопросы вскользь упоминаются в отраслевом законодательстве.

Развитие цифровых отношений так или иначе коснулось и уголовного процесса, который в науке и практике признается одним из самых консервативных. За последнее время в уголовно-процессуальное законодательство было внесено достаточно большое количество дополнений в части цифровизации: появление электронных носителей в уголовном деле и особенности их изъятия и хранения, разрешение проведения допроса в досудебном производстве с использованием видео-конференц-связи, возможность использования электронных документов и бланков и другое. Однако адаптацию уголовного судопроизводства к цифровой трансформации еще стоит осмыслить.

---

[100] *Катрин Е.В.* Цифровизация: научные подходы к определению термина // Вестник Забайкальского государственного университета. 2022. Т. 28, № 5. С. 49–54.

[101] Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/

Уголовное судопроизводство по своему содержанию является, пожалуй, самым сложным и жестко формализированным видом процесса. Соблюдение процессуальной формы, как проявление принципа законности, выступает одной из ключевых гарантий обеспечения прав и свобод участников уголовного судопроизводства. Поэтому вопросы цифровизации уголовно-процессуальной деятельности очень осторожно воспринимаются и учеными, и правоприменителем.

В уголовно-процессуальной науке цифровизация процесса рассматривается в различных аспектах: с позиций доказывания[102], с позиций эффективности доступа к правосудию[103], с позиций уголовно-процессуальной деятельности конкретных участников уголовного судопроизводства[104] и др. Интересным представляется подход А.Б. Семушкина, который предлагает: « …В рамках экосистемы… выделение как минимум трех основных направлений (блоков) – уголовно-процессуального, организационного (делопроизводство) и криминалистического»[105].

Используя вышеприведенный подход, хотелось бы уделить внимание некоторым вопросам правового регулирования цифровизации досудебного уголовного судопроизводства и его эффективности.

Правовым основанием для применения цифровых технологий в уголовном судопроизводстве выступает ст. 166 УПК РФ, которая допускает применение технических средств и способов при проведении следственных действий. В судебном производстве возможность их использования упоминается в ст. 259, 303 УПК РФ. Однако уголовно-процессуальный закон не раскрывает содержание указанного термина, ограничиваясь лишь условиями для их применения. Хрестоматийно «технические средства» выступали и являются предметом исследования криминалистов. Так, Р.С. Белкин рассматривал технико-криминалистическое средство как устройство, приспособление или материал, используемый для собирания и исследования доказательств или для создания условий, затрудняющих совершение преступления[106].

---

[102] Основы теории электронных доказательств : монография / под ред. д-ра юрид. наук *С.В. Зуева.* М. : Юрлитинформ, 2019.

[103] Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий (ГАС «Доступ к правосудию) : монография / отв. ред. Л.Н. Масленникова. М. : Норма, Инфра-М, 2022.

[104] *Таболина К.А., Таболин В.П.* Надзор прокурора в уголовном судопроизводстве в условиях развития цифровых отношений // Актуальные проблемы российского права. 2023. № 4. С. 115–123.

[105] *Семушкин А.Б.* Экосистема предварительного расследования // Актуальные проблемы российского права. 2023. № 7. С. 143–158.

[106] Криминалистика : учебник / *П.Н. Аленичев, Р.С. Белкин, Е.М. Лившиц, И.М. Лузгин* [и др.] ; под ред. Р.С. Белкина. М. : Юрид. лит., 1974. С. 37.

В последующем содержание термина расширялось. На современном этапе криминалисты включают в содержание понятия «техническое средство» и программные продукты[107].

С учетом активного развития технологий в современном мире и стране, полагаем обоснованным подход законодателя абстрактного изложения в уголовно-процессуальном законодательстве категории «технические средства и способы». Однако в целях обеспечения соблюдения прав и свобод участников уголовного судопроизводства при применении технических средств в ходе производства следственных действий необходимо нормативно закрепить их параметры и критерии для использования. Пока они достаточно хаотично закреплены в разных правовых источниках[108], чаще в ведомственных актах, а положения ч. 5 ст. 166 УПК РФ создают условия для широкого проявления судейского усмотрения.

Проблемы недостаточности правового регулирования цифровизации правоохранительной деятельности и судопроизводства достаточно остро отражаются в решениях по конкретным уголовным делам. Так, в условиях современной геополитической ситуации актуальным становится вопрос о допустимости использования программного продукта «недружественных стран». Например, когда необходимо проведение исследований в рамках уголовного дела о преступлениях в сфере компьютерной информации с использованием иностранного программного обеспечения из «санкционного списка»[109] при отсутствии российского аналога. Вероятно, это одна из причин низкой раскрываемости преступлений в IT-сфере. Согласно данным МВД России за первое полугодие 2024 года органы внутренних дел уже зарегистрировали информацию о 59 000 преступлений, что в полтора раза больше, чем за 2023 год. При этом раскрываемость в 2023 году составила только 4 %[110].

---

[107] См., например: *Иванов В.В., Цой В.А.* Понятие, виды и правила применения технических средств в уголовном процессе // Технологи в инфосфере. 2021. № 2 (4). С. 109–124.

[108] Например: Конституция РФ, гл. 2 УПК РФ, ст. 3 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года[108], а также раздел 3 Указа Президента РФ № 490 «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 года.

[109] О применении ответных специальных экономических мер в связи с недружественными действиями некоторых иностранных государств и международных организаций : Указ Президента РФ от 03.05.2022 № 252 (ред. от 22.12.2022); О мерах по реализации Указа Президента Российской Федерации от 3 мая 2022 г. № 252 : постановление Правительства РФ от 11.05.2022 № 851 (ред. от 05.11.2022).

[110] Сайт Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/reports/item/54040412

Полагаем, в данной ситуации в рамках уголовного дела судебная экспертиза назначена и проведена быть не может, иное бы противоречило принципу законности в уголовном процессе. Возможным выходом для формирования доказательственной базы могут послужить сведения, полученные в рамках оперативно-розыскных мероприятий, предусмотренных пп. 5, 15 ч. 1 ст. 6 Федерального закона № 144-ФЗ «Об оперативно-розыскной деятельности» от 12.08.1995[111]. Конечно, при соблюдении всех требований, предъявляемых к доказательствам, установленных УПК РФ.

Очень активная работа ведется по внедрению искусственного интеллекта в социально-экономические процессы. Согласно п. 5 Указа Президента РФ № 490 «О развитии искусственного интеллекта в Российской Федерации» от 10 октября 2019 года «Искусственный интеллект – комплекс технологических решений, позволяющий *имитировать когнитивные функции человека* (*включая поиск решений без заранее заданного алгоритма*) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений»[112].

Полагаем, что уголовное судопроизводство не должно переходить на использование машинного решения в разрешении уголовно-правового конфликта и решении вопроса о виновности или невиновности *человека*. Разнообразие видов производств, обусловленных дифференциацией уголовно-процессуальной формы, наполнение содержания принципов уголовного процесса судебной практикой, наконец, реализация уголовной политики на конкретном этапе развития общества не позволит искусственному интеллекту в конкретном уголовном деле выбрать оптимальное решение, которое бы отвечало социальной ценности уголовного судопроизводства, его назначению.

Полагаем, что вовлечение искусственного интеллекта в уголовный процесс через категорию «технические средства» недопустимо. Искусственный интеллект в уголовном процессе должен быть подконтролен субъектам уголовного судопроизводства. На современном этапе использование искусственного интеллекта, на наш взгляд, возможно исключительно в рамках оперативно-розыскной и административной деятельности правоохранительных органов[113]. Так, МВД России запланировано использование нейросети к 2025 году путем запуска двух

---

[111] Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/

[112] Там же.

[113] Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 года № 144-ФЗ; О полиции : Федеральный закон от 7 февраля 2011 года № 3-ФЗ.

систем: «Первая система получила предварительное название «Конъюнктура» – в ее задачи войдет прогнозирование различных чрезвычайных ситуаций и негативных происшествий и моделирование сценариев реагирования на них. Вторая система – «Клон» – нужна для выявления «фактов подделки видеоизображений в интересах правоохранительных органов»[114].

Применение технических средств в уголовном судопроизводстве с позиций доказывания затрагивает еще один очень важный аспект о компетентности в цифровых технологиях субъекта его использования. Действующее законодательство не устанавливает формализированных критериев к уровню профессионального образования, профессиональному опыту, которые предъявлялись бы к субъектам уголовно-процессуальной деятельности в части цифровой компетенции. Профессиональные стандарты отсутствуют, за исключением «Следователь-криминалист»[115].

Анализ судебной практики показывает, что решение этого вопроса вновь находится в пределах усмотрения судьи. Так, в ходе исследования доказательств, полученных с применением технических средств, судья в каждом отдельном случае определяет необходимость наличия специальных знаний для их использования. Если специальные знания необходимы, то обязательно привлечение специалиста. Например, использование цифрового фотоаппарата в ходе проведения проверки показаний на месте с участием подозреваемого самим следователем признано законным, тогда как проведение цифровой видеозаписи допроса подозреваемого следователем суд признал недопустимым доказательством. Требовалось привлечение специалиста для осуществления видеозаписи[116].

Приведенный пример судебной практики в системном толковании положений ст. 58 и 164.1 УПК РФ дает основания полагать, что в каждом случае проведения *следственного действия* с применением технических средств, в основе которых выступают цифровые технологии, требуется необходимость наличия у должностного лица соответствующих профессиональных компетенций, что обуславливает на современном этапе обязательное участие специалиста в указанной сфере. Лишь при соблюдении данного правила результаты следственного действия выступят допустимыми доказательствами по уголовному делу.

---

[114] Искусственный интеллект выходит на борьбу с преступностью в России. Правонарушителей будут искать хитрые нейросети. URL: https://corp.cnews.ru/news/top/2024-01-11_iskusstvennyj_intellekt

[115] Об утверждении профессионального стандарта «Следователь-криминалист» : приказ Министерства труда и социальной защиты РФ от 23 марта 2015 г. № 183н.

[116] Апелляционное определение Судебной коллегии по уголовным делам Верховного суда РФ от 05.09.2017 № 56-АПУ17-18. URL: https://vsrf.ru/lk/practice

Это требование распространяется и на проводимые следственные действия с использованием видео-конференц-связи в порядке, установленном ст. 189.1 УПК РФ: допрос, очная ставка, опознание. Участие специалиста должно обеспечивать техническое сопровождение хода проведения указанных следственных действий, что должно быть отражено в протоколе следственного действия.

Приведенные тезисы подводят к интересному выводу: действующее уголовно-процессуальное регулирование механизма доказывания позволяет вводить сведения, добытые с использованием «цифровых средств и способов», либо через легализацию сведений, добытых в ходе оперативно-розыскной деятельности, либо в рамках уголовно-процессуальной деятельности, но с обязательным участием специалиста в IT-сфере. Это, в свою очередь, свидетельствует об «утяжелении процесса», накладывая дополнительные временные и финансовые затраты, что вряд ли отвечает эффективности уголовного судопроизводства.

Современные реалии требуют необходимости более четкого законодательного подхода в решении вопроса об использовании цифровых технологий в уголовно-процессуальном доказывании.

Цифровую трансформацию уголовного судопроизводства, на наш взгляд, необходимо рассматривать с позиций *организации управления* работой следователей, дознавателей, их оперативного взаимодействия между оперативными подразделениями и контрольно-надзорными органами, медицинскими учреждениями и адвокатурой.

***Хуснутдинов Рашид Марсович*,**

старший преподаватель кафедры уголовного права и процесса, Ижевского института (филиал) Всероссийского государственного университета юстиции (РПА Минюста России)

ИСПОЛЬЗОВАНИЕ В ДОКАЗЫВАНИИ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ О БЕЗДОКУМЕНТАРНЫХ ЦЕННЫХ БУМАГАХ

Противоправные действия с бездокументарными ценными бумагами осуществляются как в электронном виде, часто в режиме удаленного доступа (например через терминалы брокеров для доступа к биржам), так и путем оформления бумажных документов. Однако даже при использовании бумажного распорядительного документа, его исполнение проводится путем совершения электронной операции. И наоборот, если есть необходимость в «бумаге» получить сведения о бездокументарных ценных бумагах и операциях с ними, то соответствующий отчет или выписка формируются в электронном виде, затем переводятся «на бумагу».

Доказательственное значение электронной информации о бездокументарных ценных бумагах состоит в способности этой информации гарантировать восстановление хронологии событий и действий, связанных с изменениями, внесенными в электронные базы данных, а также обеспечить возможность определения лиц или программно-технических средств, ответственных за эти изменения (п. 4.4. Положения Банка России от 27.12.2016 № 572-П[117]). Эти сведения, достоверно отражая действительность и имея связь с предметом доказывания, в порядке, установленном УПК РФ, могут быть использованы в качестве доказательств, отвечающих требованиям допустимости, относимости и достоверности.

Следователь, расследуя уголовное дело о преступлении с бездокументарными ценными бумагами, неизбежно сталкивается с ситуацией, когда наряду с бумажными документами значительный массив сведений, имеющих доказательственное значение, представляет из себя электронную информацию; собирание, закрепление, проверка и оценка которой позволяет выявить круг лиц, причастных к совершению преступления, степень их вины, способ совершения преступления, обстановку и прочие обстоятельства.

[117] О требованиях к осуществлению деятельности по ведению реестра владельцев ценных бумаг : положение Банка России от 27.12.2016 № 572-П (ред. от 08.06.2021) // СПС «КонсультантПлюс». 2024.

Данные сведения находятся на принадлежащих профессиональным участникам рынка ценных бумаг (далее – профучастники) электронных носителях информации: серверы, накопители информации для резервного копирования электронных баз и т.д. При этом данные организации аккумулируют в своем распоряжении и бумажные документы, на основе которых происходит распоряжение бездокументарными ценными бумагами. Профучастники ведут деятельность на основании закона и нормативных актов Банка России. К примеру, регистратор ведет реестр ценных бумаг на основании ряда отраслевых законов, нормативных актов Банка России, а также правил ведения реестра, которые он разрабатывает и обязан утвердить (ч. 1 ст. 8 Федерального закона от 22.04.1996 № 39-ФЗ[118]). Требования к указанным правилам установлены Банком России[119]. Также Банком России утверждены перечни документов, которые обязаны хранить профучастники, и порядок хранения документов[120].

Проблема процессуальной природы электронной или цифровой информации, имеющей доказательственное значение в уголовном судопроизводстве, остается остро дискуссионной. Как справедливо замечают А.А. Балашова и А.И. Жмурова, законодатель не предусматривает отнесение доказательств, основанных на информации в электронной форме, к определенной категории доказательств, указанной в ч. 2 ст. 74 УПК РФ[121]. В юридической литературе обсуждается вопрос о дополнении системы уголовно-процессуальных доказательств новым элементом – «компьютерная информация и ее носители», «цифровая информация» и т.д.; к сторонникам этой идеи следует отнести: Е.А. Гамбарову[122], В.Н. Григорьева и О.А. Максимова[123], О.М. Ефремову[124],

---

[118] О рынке ценных бумаг : Федеральный закон от 22.04.1996 № 39-ФЗ (ред. от 14.07.2022) // СПС «КонсультантПлюс». 2024.

[119] Требования установлены Положением Банка России от 27.12.2016 № 572-П.

[120] Об обязательных для профессиональных участников рынка ценных бумаг требованиях, направленных на выявление конфликта интересов, управление им и предотвращение его реализации : указание Банка России от 23.08.2021 № 5899-У // Вестник Банка России. 03.11.2021. № 75; Положение Банка России от 27.12.2016 № 572-П и др.

[121] *Балашова А.А., Жмурова А.И.* К вопросу об электронных доказательствах в уголовном процессе России // Глава 2. Цифровизация как основа конвергенции частного и публичного права // Частноправовые и публично-правовые проблемы современной юриспруденции : коллективная монография / отв. ред. С.Ю. Морозов, О.А. Зайцев. М. : Проспект, 2022. С. 98.

[122] *Гамбарова Е.А.* Социальные сети как источник цифровых доказательств // Криминалистическое обеспечение расследования преступлений: проблемы, перспективы и инновации : материалы Междунар. науч.-практ. конф. Минск : БГУ, 2017. С. 189.

[123] *Григорьев В.Н., Максимов О.А.* Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел // Полицейская деятельность. 2018. № 1. С. 1–8.

[124] *Ефремова О.М.* Реализация полномочий следователя, направленных на получение и использование компьютерной информации при производстве следственных действий : дисс. ... канд. юрид. наук. Орел, 2021. С. 61.

А.И. Зазулина[125], Н.А. Зигуру[126], Д.Н. Маринкина и В.А. Костыреву[127], П.С. Пастухова[128] и др. Противники данного предложения, среди которых О.Г. Григорьев[129], Ю.А. Ионова и С.В. Калитин[130], Л.Б. Краснова[131], С.И. Кувычков[132], А.Ю. Федюкина[133] и др., обсуждают отнесение таких доказательств к уже устоявшимся в доктрине и законодательстве видам доказательств (вещественным доказательствам, иным документам). Здесь в контексте нашего исследования необходимо заметить, что стандартный порядок обработки электронной информации о бездокументарных ценных бумагах устанавливает ее обязательное резервное копирование ежедневно[134], что означает возможность копирования информации без изменения содержания и без утраты (изменения) юридического значения информации. Из этого следует, что электронная информация о бездокументарных ценных бумагах не обладает свойством незаменимости. Резервная копия информации или, иначе говоря, дубликат «оригинальной» электронной информации без ущерба для доказывания удостоверяет те же факты, что и «оригинальная» информация. Электронная информация о ценных бумагах, а равно ее дубликат или копия, отвечает всем признакам «иного документа» – исходит от уполномоченных организаций, содержит сведения, имеющие доказательственное значение, обладает идентифицирующими авторство, время создания

---

[125] *Зазулин А.И.* Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу : автореф. дисс. ... канд. юрид. наук. Екатеринбург, 2018. С. 11–13.

[126] *Зигура Н.А.* Компьютерная информация как вид доказательств в уголовном процессе России : дисс. … канд. юрид. наук. Челябинск, 2010. С. 18.

[127] *Маринкин Д.Н., Костарева В.А.* Цифровые доказательства в уголовном судопроизводстве // Вестник Пермского института ФСИН России. 2019. № 1(32). С. 33–36.

[128] *Пастухов П.С.* Электронное вещественное доказательство в уголовном судопроизводстве // Вестник Томского государственного университета. 2015. № 396. С. 151.

[129] *Григорьев О.Г.* Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства : дисс. … канд. юрид. наук. Тюмень, 2003. С. 15.

[130] *Ионова О.А., Калитин С.В.* Понятие доказательств, имеющих электронную форму и цифровое содержание: проблемы и перспективы // Вестник Хабаровской государственной академии экономики и права. 2013. № 1. С. 59–60.

[131] *Краснова Л.Б.* Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 254–260.

[132] *Кувычков С.И.* Использование в доказывании по уголовным делам информации, представленной в электронном виде : дисс. ... канд. юрид. наук. Нижний Новгород, 2016. С. 12.

[133] *Федюкина А.Ю.* О месте электронных носителей информации в системе доказательств по уголовным делам // Вестник Московского университета МВД России. 2020. № 3. С. 81–83.

[134] Пункт 4.5 положения Банка России от 27.12.2016 № 572-П.

и т.д. реквизитами, защищена от произвольного искажения; в связи с чем необходимость отграничения ее от данного вида доказательств и выделение в отдельный вид доказательств представляется неоправданным.

Более того, информация, представленная в электронной форме и заверенная квалифицированной электронной подписью, признается эквивалентом бумажного документа, подписанного личной подписью, и применяется в любых правовых отношениях в соответствии с законодательством, за исключением случаев, когда федеральными законами или соответствующими нормативными актами требуется исключительное составление документа, выполненного на бумаге[135].

Электронный документ защищен от изменения его содержания, передается по информационно-телекоммуникационной сети, хранится на электронных носителях, которые, хотя и содержат сведения об электронном документе, в отношении содержания электронного документа не имеют индивидуального незаменимого значения. В связи с этим электронный документ, являясь нематериальным объектом, может быть приобщен к уголовному делу на электронном носителе в качестве иного документа. Также в качестве иного документа к уголовному делу может быть приобщена надлежащим образом заверенная бумажная копия электронного документа или выписка из него.

Аргументы сторонников выделения электронных носителей информации в отдельный вид доказательств представляются недостаточно убедительными. Будет неверным отождествлять электронный носитель информации (сервер, внешний накопитель информации, флэш-карта и т.д.) и содержащуюся на нем электронную информацию, так как последняя без ущерба для доказывания может дублироваться (копироваться) и переноситься с одного носителя на другой. Доказательственное значение самих носителей информации, связанных с событием преступления, в том, что данные устройства, могут содержать следы воздействия на хранимую (ранее хранимую) электронную информацию. К примеру, жесткий диск ПК может содержать следы удаления электронной информации. То есть электронные носители информации могут использоваться в доказывании именно как вещь, как предмет, при этом нести на себе непосредственно отображение преступления и, соответственно, обладают незаменимостью и другими свойствами вещественных доказательств[136]. Специфичность, техническая сложность электронных носителей информации как физических предметов, а также наличие некоторых специальных уголовно-процессуальных

---

[135] Об электронной подписи : Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) // СПС «КонсультантПлюс». 2022.

[136] *Строгович М.С.* Курс советского уголовного процесса. Т. 1. Основные положения науки советского уголовного процесса. М. : Издательство «Наука», 1968. С. 453–455.

правил, относящихся к электронным носителям информации (чч. 1 и 4 ст. 81.1, ч. 2.1. ст. 82, ст. 164.1 УПК РФ и др.), не должны вводить в заблуждение. Уголовное судопроизводство на практике сталкивается с самыми разнообразными предметами, имеющими доказательственное значение: холодным и огнестрельным оружием, ювелирными изделиями, наркотическими веществами, биологическими объектами и т.д. Собирание и закрепление каждого из таких доказательств, их проверка и оценка обладают значительной спецификой. И тем не менее все эти предметы (объекты) признаются вещественными доказательствами с распространением на них соответствующих уголовно-процессуальных правил.

Нормативные требования к ведению реестра владельцев ценных бумаг, введенные Банком России, предусматривают формирование регистратором на основе имеющихся у него электронных баз данных, в которых содержатся и хранятся учетные записи о бездокументарных ценных бумагах, отчетов (уведомлений) о проведении транзакций на лицевых счетах, составление выписок по лицевым счетам, составление отчетов (справок) о проведенных операциях на лицевых счетах, выгрузку уведомлений об отказе в проведении операции и т.д.[137] Аналогичные документы, связанные с операциями с бездокументарными ценными бумагами, оформляют другие профучастники. Данные документы могут оформляться как в электронном, так и в бумажном виде.

С учетом изложенного с точки зрения объективных познавательных свойств сведения о бездокументарных ценных бумагах существуют как в виде электронной информации – электронных баз данных, отображающих массив информации о действиях широкого круга клиентов профучастников, так и в виде бумажных документов, каждый из которых, как правило, отображает информацию локально (выписка по лицевому счету, договор купли-продажи, передаточное распоряжение и пр.), а также существуют в виде электронных носителей информации, которые могут выступить доказательством о действиях с находящейся или находившейся на них электронной информацией. В этом случае электронные носители информации должны признаваться вещественными доказательствами.

С.А. Шейфер обоснованно утверждает, что при выборе надлежащего следственного действия необходимо исходить из УПК РФ, определяющим обязательность проведения следователем одних следственных действий, которые он провести обязан, и оставляющим на усмотрение следователя проведение других следственных действий. С.А. Шейфер называет это «нормативным фактором выбора»[138]. В данном случае уголовно-процессуальный закон

---

[137] Пункт 2.6 положения Банка России от 27.12.2016 № 572-П.

[138] *Шейфер С.А.* Следственные действия. Основания, процессуальный порядок и доказательственное значение : монография. Самара, 2008. С. 39.

не содержит предписаний, которые обязывают следователя произвести определенные следственные действия, предусматривая, однако, особенности их проведения с электронными носителями информации, на которых располагаются электронные базы данных (ст. 164.1 УПК РФ). Следователь вправе получить искомую доказательственную информацию путем направления запроса в порядке ч. 4 ст. 21 УПК РФ о предоставлении бумажных или электронных документов (отчетов, выписок, справок и т.д.), сформированных в установленном порядке на основе электронных баз данных, а также при необходимости вправе изъять доказательственную информацию, например резервные копии электронных баз, путем производства осмотра, обыска или выемки.

Шамсеева Алина Маратовна,
ассистент кафедры уголовного процесса и криминалистики
Удмуртского государственного университета

О ВОЗМОЖНОСТИ ВВЕДЕНИЯ НОВОГО «ЭЛЕКТРОННОГО ДОКАЗАТЕЛЬСТВА» В УПК РФ

В современном мире повседневная жизнь социально активного человека связана с использованием различных индивидуальных устройств с доступом к информационно-телекоммуникационной сети «Интернет». Информация, передаваемая лицами чаще всего путём использования мобильных устройств, обретает важное значение не только для межличностного общения, но и при наличии конфликтных ситуаций, приводящих к вовлечению органов правоохранительной деятельности, судебной системы РФ. В частности, информация, содержащаяся на просторах Интернета, фиксирующая определённые высказывания или побуждения, а также действия лиц, направленные на передачу и (или) распространение данной информации, может иметь доказательственное значение в рамках конкретного уголовного дела. Именно поэтому представляется актуальным рассмотреть некоторые вопросы, связанные с использованием в уголовном судопроизводстве информации, находящейся в Интернете, а также содержащейся на различных внешних носителях в целях доказывания по уголовному делу.

Предметом дискуссии большинства учёных-теоретиков и исследователей является вопрос о существовании электронного доказательства как отдельного вида доказательства и необходимости его введения в Уголовно-процессуальный кодекс РФ. Так, первая группа исследователей считает, что электронное доказательство должно быть закреплено в качестве отдельного вида доказательства в УПК РФ (Агибалов В.Ю.[139], Зигура Н.А.[140]), а другая – что имеющую значение для дела информацию на внешнем носителе можно отнести к вещественным доказательствам или к иным документам (Рыбин А.В.[141], Оконенко Р.И.[142]).

---

[139] *Агибалов В.Ю.* Виртуальные следы в криминалистике и уголовном процессе : монография. М. : Юрлитинформ, 2012. С. 35–40.

[140] *Зигура Н.А.* Компьютерная информация как вид доказательств в уголовном процессе : дисс. … канд. юрид. наук. Челябинск, 2010. С. 50–73.

[141] *Рыбин А.В.* Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации: процессуальные и криминалистические аспекты : дисс. ... канд. юрид. наук. Краснодар, 2005. С. 11–13.

[142] *Оконенко Р.И.* «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ

Существование различных точек зрения по данному вопросу обуславливает необходимость в подробном изучении теоретических исследований и правоприменительной практики, складывающейся ввиду использования данных, содержащихся в Интернете и на различных устройствах для целей расследования уголовного дела.

В научных публикациях всё чаще употребляется термин «электронное доказательство», не имеющий легального закрепления. Под ним подразумеваются сведения, закрепленные в электронной или цифровой форме, позволяющие установить в ходе уголовного судопроизводства обстоятельства, предусмотренные ст. 73 УПК РФ[143]. Однако истинное содержание электронного доказательства не всегда раскрывается исследователями правильно, что ставит некоторые выводы, предлагаемые ими, под сомнение. Фактически при упоминании электронного доказательства речь идёт об электронной информации. В условиях отсутствия законодательно предусмотренного порядка признания доказательства электронным более корректным представляется употребление термина «электронная информация». Правовую природу, отличительные признаки и свойства электронной информации и обоснование применения такого термина подробно рассмотрел в своём исследовании В.С. Черкасов[144]. Под электронной информацией им понимаются сведения, передача, обработка, воспроизведение которых осуществляется посредством электронных аппаратно-программных средств. Следует обратить внимание на такие её свойства, как возможность копирования неограниченное количество раз и неразрывность связи информации с физическим носителем. Стоит отметить и тот факт, что сама информация шифруется в специальной системе знаков (двоичные системы и другие), конечный итоговый вариант её отображения в том виде, который может быть воспринят – результат шифрования и де-шифрования, осуществляемый благодаря специальным технико-технологическим достижениям и системам. В связи с этим различают логический и семантический уровни представления электронно-цифровой информации (изображение, звук, текст). Для установления обстоятельств, имеющих значение для уголовного дела, в большинстве случаев будет важным именно семантический уровень представления электронно-цифровой информации. Логический уровень будет иметь

законодательства Соединенных Штатов Америки и Российской Федерации : дисс. … канд. юрид. наук. М., 2016. С. 20.

[143] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.05.2024) // Собрание законодательства РФ. 24.12.2001. № 52 (ч. I), ст. 4921.

[144] *Черкасов В.С.* Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса : дисс. ... канд. юрид. наук. Хабаровск, 2022. С. 62–63.

значение в том случае, если объектом преступления является компьютерная информация, или если вредоносная программа была использована в качестве орудия или средства совершения преступления, когда посредством вредоносных программ происходит какое-либо вмешательство в работу программно-аппаратных средств или модификация компьютерной информации.

Изображения, звуки и текст, позволяющие фиксировать определённые юридические факты, сами по себе имеют значение для уголовного дела без необходимости получения их цифрового кода, который может быть и нарушен в результате умышленных действий человека. Отдельного порядка изъятия для них не предусмотрено. Законодательно обязанность следователя в привлечении к участию специалиста предусмотрена при изъятии электронных носителей информации. При этом копирование информации допускается и без участия специалиста единолично следователем. Так, в большинстве случаев в рамках уголовного дела приобщаются электронные почтовые переписки к уголовному делу как приложение к протоколу осмотра[145]; как вещественное доказательство приобщаются диски, содержащие электронную переписку[146]. Данный порядок процессуальной деятельности обусловлен существующими нормами, в соответствии с которыми в качестве иного вида доказательства фактически к материалам дела приобщается электронная информация. В признании таких доказательств по делу недопустимыми ввиду несоблюдения специального порядка изъятия информации, необходимости привлечения специалистов, судами высшей инстанции отказывается. Соответственно, сложившаяся практика не требует участия специалиста при приобщении к делу электронной информации, получаемой следователем. Риск утраты первоначально заложенного кода или возможности обнаружения умышленного его повреждения в преступных целях при участии квалифицированного участника данных действий при этом не учитывается. Достаточно актуальным также является вопрос о достаточности квалификации следователя и даже специалиста, которые потенциально могут быть привлечены. Работа с электронной информацией вызывает необходимость в повышении уровня знаний, улучшении навыков лиц, которые должны параллельно с возникающими методиками и технологиями по повреждению и (или) уничтожению информации развиваться и совершенствоваться.

---

[145] Апелляционное постановление Московского городского суда от 22.11.2021 по делу № 10-13507/2021 // СПС «Консультант Плюс».

[146] Кассационное определение Второго кассационного суда общей юрисдикции от 12.05.2022 по делу № 77-1555/2022 // СПС «Консультант Плюс».

Также достаточно часто обсуждается сущность скриншота экрана устройства, его значение. В некоторых случаях его причисляют к электронному доказательству[147]. Не вдаваясь в подробности изучения природы и содержания скриншота, оговоримся, что это изображение снимка экрана устройства, сделанное для его фиксации. Отнесение скриншота к числу электронных доказательств представляется ошибочным. Скриншот не представлен в специальной знаковой системе, может быть распечатан на бумажный носитель и по своей характеристике в системе доказательств может быть отнесён, например, к иному документу.

Электронная информация по своей характеристике является качественно отличной от вещественных доказательств и иных документов. Рассмотрение различий между ней и иными видами доказательств, закреплёнными в ст. 74 УПК РФ, необходимо осуществлять по нескольким критериям: по доказательственному значению, механизму образования доказательства, по признаку восприятия и среды существования доказательства.

Вещественное доказательство всегда представляет собой предмет материального мира, который имеет доказательственное значение сам по себе, содержит определённую, значимую для дела информацию. Отсутствие данного предмета влечёт и отсутствие доказательства. Электронная информация, существующая в закодированной форме, связана со своим носителем, но такой накопитель самостоятельно никакого значения не имеет. Электронная информация может существовать, например, в специальном облачном хранилище. В УПК РФ упоминается лишь электронный носитель информации, потому что именно он приобщается к материалам дела, выступая формой фиксации значимой электронной информации[148]. По механизму образования вещественное доказательство носит в себе след, образованный механическим воздействием, отражает факты. Электронная информация, воспринимаемая нами, определяется алгоритмом, который задан разработчиком и реализуется в конкретной программе. Таким образом, программа является средством отражения фактов. По признаку восприятия в вещественном доказательстве информация содержится в своем естественном, некодированном виде, и преобразование ее с помощью технических средств для восприятия не нужно. Компьютерная информация всегда опосредована через машинный (физический) носитель

[147] *Денисов Е.А.* Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Скиф. 2017. № 15. С. 35–39. URL: https://cyberleninka.ru/ (дата обращения: 07.10.2024).

[148] *Карташов И.И., Лесников О.А.* Цифровая информация в уголовно-процессуальном доказывании: понятие и свойства // Наука. Общество. Государство. 2020. Т. 8, № 4. С. 77–78. URL: http://esj.pnzgu.ru/

информации, вне которого она не может существовать, и восприятие её (компьютерной информации) возможно только посредством технического средства (компьютера)[149].

Согласно существующей теории уголовного процесса доказательства должны обладать тремя свойствами: допустимости, относимости, достоверности.

Допустимость доказательства определяется надлежащей процедурой их получения, соблюдением требований, предъявляемых к источникам, условиям и способам его получения. Достоверность доказательства определяется точностью и правильностью, соответствием данных действительности, исходя из формы и содержания[150]. Специфичность содержания электронного доказательства, то есть самой электронной информации и способов её существования, предполагает необходимость особого способа её получения при соблюдении определённых условий. В противном случае высока вероятность утери и (или) искажения информации, которая должна быть получена и приобщена к уголовному делу.

В настоящий момент УПК РФ не предусмотрен порядок обнаружения, сбора, изъятия электронных доказательств. Подобная ситуация означает, что соответствие полученной электронной информации требованиям допустимости и достоверности в условиях действующего уголовно-процессуального законодательства для целей рассмотрения её в качестве отдельного вида доказательства недостижимо. В УПК РФ упоминается лишь «электронный носитель информации» (ст. 81 УПК РФ), который не может отождествляться с электронной информацией. Как показывает судебная практика, таким носителем может быть DVD-диск или флеш-накопитель[151]. Введение данного понятия в УПК РФ, безусловно, говорит о стремлении привести в соответствие уголовный процесс с бурно развивающимся информационным обществом. Однако однозначного понимания относительно сущности и критериев для отнесения какого-либо накопителя информации к такому внешнему носителю нет. Не закреплено в УПК РФ определение понятия и содержания, видов электронного внешнего носителя. Вместе с тем обоснованные ранее особенности информации, содержащейся на таком носителе, дают все основания для закрепления особого порядка обращения с электронным носителем для сохранения сведений

---

[149] *Зигура Н.А.* Указ соч.

[150] *Шейфер С.А.* Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования : монография. 2-е изд., испр. и доп. М. : Норма : ИНФРА-М, 2024. С. 31–34.

[151] Кассационное определение Судебной коллегии по делам военнослужащих Верховного суда Российской Федерации от 04.07.2024 по делу № 222-УД24-41-А6 // СПС «Консультант Плюс».

в их первоначальном виде. Дальнейшая перспектива по использованию электронной информации в уголовном процессе должна быть связана с развитием правового регулирования электронных носителей информации и только в дальнейшем – с постепенным, последовательным переходом к новой концепции электронного доказательства.

Соответственно, введение «электронного доказательства» в уголовный процесс предполагает не только законодательное закрепление отдельных процедур по обнаружению, фиксации, изъятию и сохранению информации с последующей возможностью их реализации в правоприменительной практике, но и освоение всех навыков по воспроизведению, прочтению и восприятию данной информации в неискажённом, первоначальном виде[152]. Более того, введение данного вида доказательства потребует качественно иного подхода к осуществлению его оценки с учётом специфичных свойств самой информации и формы её существования. Исходя из изложенного считаем, что нововведения в уголовном судопроизводстве, касающиеся возникновения нового «электронного доказательства», являются преждевременными.

[152] *Воронин М.И.* Электронные доказательства в УПК: быть или не быть? // Lex Russica. 2019. № 7 (152). С. 75. URL: https://cyberleninka.ru/ (дата обращения: 22.10.2024).

Каминский Александр Маратович,

доктор юридических наук, профессор, профессор кафедры уголовного процесса и криминалистики

О НЕКОТОРЫХ ТЕНДЕНЦИЯХ И ПЕРСПЕКТИВАХ РАЗВИТИЯ КРИМИНАЛИСТИЧЕСКИХ ИССЛЕДОВАНИЙ В ОБЛАСТИ IT-ТЕХНОЛОГИЙ

Бесспорная тенденция вторжения компьютерных технологий во все сферы жизни социума закономерно не могла не коснуться взаимовоздействия, взаимовлияния двух видов человеческой деятельности – преступной и деятельности по выявлению, раскрытию и расследованию преступлений, отражательно-информационный аспект которого и образует объект исследования криминалистики. Можно с уверенностью констатировать, что в нем появилась еще одна грань, определяющая это взаимовоздействие сквозь призму компьютерных технологий.

Анализ правоохранительной практики последних десятилетий наглядно демонстрирует потребность деятельности выявления, раскрытия и расследования преступлений в эффективных криминалистических рекомендациях, методиках борьбы как с преступлениями, предусмотренными гл. 28 УК РФ, так и с «традиционными» видами преступлений, где компьютерные технологии предоставляют широкие возможности совершенствования способов совершения преступлений, их механизмов. И практика расследования преступлений также использует возможности компьютерной техники и компьютерных технологий во всем их многообразии для решения своих профессиональных задач.

В ответ на запросы практики криминалистика достигла определенных результатов: «описан и исследован новый криминалистический объект – «кибернетическое пространство», определяемый как среда совершения преступлений в сфере компьютерной информации и существования нового вида виртуальных следов»[153]. Развивается сформировавшаяся частная криминалистическая теория информационно-компьютерного обеспечения криминалистической деятельности[154].

---

[153] *Мещеряков В.А.* Основы методики расследования преступлений в сфере компьютерной информации : автореф. дисс. … д-ра. юрид. наук. Воронеж, 2001. С. 9.

[154] *Россинская Е.Р.* К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия ТулГУ. Экономические

В теории криминалистики решен важнейший методологический вопрос о природе цифровых следов. Это положение видится крайне важным, так как плодотворные криминалистические исследования возможны только при наличии развитой методолого-теоретической базы по исследуемому вопросу – той парадигмы, на основе которой и будут решаться отдельные теоретические и прикладные вопросы. Строя отдельное учение в рамках конкретной науки, исследователь объективно должен решить ряд методологических задач общего характера. Общего, ибо «кто берется за частные вопросы без предварительного решения общих, тот неминуемо будет на каждом шагу бессознательно для себя «натыкаться» на эти общие вопросы»[155].

Логика любого исследования в качестве первого и главного шага требует выделения единицы анализа в теоретическом исследовании объекта, тем более такого специфичного. Такой единицей в криминалистике выступает категория «след преступления». Эта категория, по утверждению В.Г. Коломацкого[156], является «модулем» теоретических криминалистических конструкций.

При этом « … след должен браться не как оттиск, царапина, деформация и т.д. и т.п., а как единство двух противоречий: кодового преобразования информации, отражающей определенную сторону преступной деятельности (информации, существующей объективно, но в потенциальной форме), и обратного кодового преобразования, в результате которого возникает понимание механизма тех преобразований в преступной деятельности, которые и отразили первичную информацию»[157].

Научный анализ категории «след преступления» особенно необходим потому, что цифровизация в системе преступная деятельность – деятельность по выявлению и раскрытию преступлений – вызвала к жизни и новый вид следов. « …Отрасль «криминалистическое следоведение» пополнилась научными исследованиями, связанными с исследованием природы, видов, образования, выявления и закрепления виртуальных следов при проведении отдельных следственных действий. Появились исследования по проблемам так называемых цифровых и электронных следов и доказательств»[158].

и юридические науки. Вып. 3, ч. 2: Юридические науки. Тула : Изд-во Тульского гос. ун-та, 2016. С. 110.

[155] *Ленин В.И.* Полн. собр. соч. Т. 15. С. 368.

[156] Криминалистика. Т. 1. История, общая и частные теории / под ред. Р.С. Белкина, В.Г. Коломацкого, И.М. Лузгина. М., 1995. С. 50.

[157] *Каминский М.К.* Что есть, что может быть и чего быть не может для системы «криминалистика». С. 11.

[158] *Волчецкая Т.С.* Современная криминалистическая наука: реалии и перспективы развития // Казанские уголовно-процессуальные и криминалистические чтения :

Недавняя ситуация неразработанности целого ряда теоретических положений приводила к тому, что не только не был выработан единый терминологический аппарат, хотя дело даже не в том, что для обозначения одного и того же явления использовались разные термины, а в том, что за этими терминами стоит, какое содержание вкладывается в термин. Поэтому вопрос о природе цифровых следов требовал особого рассмотрения.

Следует отметить, что поэтапное решение наиболее сложных теоретических вопросов вполне закономерно, оно характеризует начальный этап становления большой и многообещающей части криминалистики. Весьма наглядно такое положение дел отражалось в подходах к терминологии и, главное, к содержанию терминов этой части криминалистики.

Г.М. Шаповалова справедливо констатировала по данному поводу, что « …в научной литературе отсутствует формулировка понятия «информационные следы»… Ученые в своих исследованиях используют термины: «виртуальный след», «информационный след» (Милашев В.А., Григорьев О.Г., Егорышев А.С.). Порожденный реалиями практики новый вид преступлений способствовал появлению нетрадиционных для следственной практики «информационных следов», требующих криминалистического научного изучения»[159]. По мнению В.А. Мещерякова, виртуальные следы являются промежуточными между материальными и идеальными.

Эта же ситуация вызвала то положение дел, которое позволило некоторым ученым говорить о «Цифровой криминалистике» («Цифровая криминалистика: вызовы XXI века»: конференция в БФУ им. Канта), Ю.Л. Дяблова – «Цифровая криминалистика – будущее науки, или тренд современности?». В.Б. Вехов – «Электронная криминалистика: основные направления развития» (Минские криминалистические чтения) и др.

Сказанного вполне достаточно, чтобы всерьез задуматься о природе цифровых следов и о месте этой части криминалистики в структуре криминалистической науки. Описанная ситуация делала понятным интерес криминалистов к природе и информативному содержанию следов преступлений, совершенных с применением преступниками цифровой техники и цифровых технологий.

Представляется, что данный вопрос был окончательно решен в ходе Международной научно-практической конференции «Цифровой след как объект судебной экспертизы» (17 января 2020 года, г. Москва). «Цифровые следы – это следы материальные, поскольку отражаются на материальных объектах,

---

материалы Междунар. науч.-практ. конф., Казань, 28 апр. 2022 г. : в 2 ч. Казан. ин-т (фил.) ВГУЮ. Казань : ЮрЭксПрактик, 2022. Ч. 1. С. 19.

[159] *Шаповалова Г.М.* Возможность использования информационных следов в криминалистике (вопросы теории и практики) : автореф. дисс. … канд. юрид. наук. Владивосток., 2006.

хотя в некоторых случаях период их существования невелик. Формирование данных следов обусловлено спецификой реализации информационных технологий, и для их преобразования в доступную для восприятия форму также используются информационные технологии»[160].

Материальную природу этих следов подтверждает мысль Р.С. Белкина о том, что «информация, как мера связи события и вызванных этим событием изменений в среде, не может существовать без материальной основы, или, как принято говорить, вне информационного сигнала, под которым понимают единство материального носителя и средства передачи информации»[161].

Аналогичная картина наблюдается и в области уголовного процесса. Большой интерес внедрение цифровых технологий в практику вызывает и у той части ученых, которые говорят о высокотехнологичном уголовном процессе (Зуев С.В., Масленникова Л.М.), о цифровизации уголовного судопроизводства, цифровой среде уголовного судопроизводства и т.п. Представляется, что эта ситуация в терминологии уголовного процесса вызвана теми же причинами.

Возвращаясь к вопросу о многообразии терминов в криминалистике, обозначающих по сути одно явление, независимо от вида цифровых следов, можно показать, как стремление авторов выпукло представить объект исследования вступает в противоречие с методологическими положениями криминалистики: « …явно неудачен термин «информационный след», что можно понимать так, что есть еще и следы неинформационные. Между тем любой след информативен. Он содержит в себе некоторое количество информации (вопрос стоит лишь о мере информации) о личности преступника, его движениях и действиях, и она содержится в следах любой природы потенциально, задача следствия – эту информацию актуализировать... Следовательно, следов, не содержащих информацию, не существует, вопрос в количестве информации и умении следователя или оперативного работника эту информацию актуализировать»[162].

«Судить об отражаемом по информации о преступлении можно только в том случае, если отражение обладает содержательной стороной, если связь изменений с событием можно обнаружить, выявить, понять по содержанию этих изменений»[163].

---

[160] *Россинская Е.Р.* Проблемы исследования цифровых следов в судебной экспертизе // Цифровой след как объект судебной экспертизы : материалы Междунар. науч.-практ. конф. М., 17 января 2020 г., С. 165.

[161] *Белкин Р.С.* Курс криминалистики : в 3 т. Т. 1: Общая теория криминалистики. М. :Юрист, 1997. 408 с.

[162] *Каминский А.М.* О системе следов преступной деятельности в сфере компьютерной информации // Казанские уголовно-процессуальные и криминалистические чтения : материалы Междунар. науч.-практ. конф., Казань, 22 апр. 2022 г. : в 2 ч. С. 33.

[163] *Белкин Р.С.* Указ. соч.

Иначе может сложиться мнение, что эти следы – следы некой иной природы, они возникают и бытийствуют по иным закономерностям, чем, например, следы выстрела, следы орудий совершения преступления, т.е. не подчиняясь в полной мере закономерностям возникновения других групп следов, а это уже вопрос методологии и теории криминалистики. При этом необходимо подчеркнуть, что такое, казалось бы, «безобидное» явление может иметь следствием серьезные теоретические заблуждения, а отсюда и ошибки практики.

По аналогии с этими рассуждениями следует подходить и к термину «цифровая криминалистика», существование которого дает основания предполагать, что наряду с цифровой существует еще какая-то иная криминалистика, которая живет по иным законам. Этот термин дает основания также ставить вопрос о том, как работают в «цифровой» криминалистике такое всеобщее свойство материи как отражение, как идея деятельности и другие теоретические положения «классической» криминалистики. Не считая себя специалистом в области уголовного процесса, автор полагал бы нужным по тем же основаниям обратиться к термину «цифровой уголовный процесс».

Борьба с современной преступностью требует не только совершенствования информационного и компьютерно-технического оснащения правоохранительной деятельности, разработки методик расследования современных преступлений, модернизации системы тактических рекомендаций, создания новых и совершенствования имеющихся экспертных методик.

На повестке дня в явном виде стоит вопрос об использовании технологий искусственного интеллекта в практике борьбы с преступностью[164]. Речь должна идти не столько о замене ручного труда машинным и даже не о замещении человека в производстве множества однотипных, алгоритмических операций компьютером, а о создании систем, способных формировать задачи и эффективно решать их на основе накопленного опыта и имеющихся возможностей и ресурсов. Представляется, что научные исследования подобного рода должны проводиться в особом ракурсе, требующем разработки не только теоретических вопросов криминалистического мышления (оформление которых далеко от завершения) и искусственного интеллекта, но и

– научного обоснования принципиальной возможности связи двух компонентов, образующих систему следователь – техническое (цифровое) устройство искусственного интеллекта, без исследования которой подобная работа была бы лишена всякого смысла;

---

[164] *Бахтеев Д.В.* Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений : дисс. … д-ра. юрид. наук. Екатеринбург, 2022.

– научного обоснования разработанной принципиальной модели механизма функционирования системы следователь – техническое (цифровое) устройство искусственного интеллекта;

– форм взаимовоздействия, взаимовлияния элементов указанной системы друг на друга в весьма специфичной области человеческой деятельности выявления, раскрытия и расследования преступлений;

– наконец, исследование вышеперечисленных моментов логично должно найти завершение в выявлении ряда особенностей, определяющих специфику функционирования системы следователь – техническое (цифровое) устройство искусственного интеллекта. Должны быть выявлены особенности, устойчивые закономерности как собственно криминалистического мышления, так и закономерности в области полидисциплинарных исследований объекта.

Становится ясно, что решение этих крупных научных вопросов в русле криминалистики, во-первых, невозможно без привлечения данных иных наук, то есть исследование должно носить комплексный, полидисциплинарный характер; во-вторых, необходимо исследовать феномен криминалистического мышления под совершенно новым, «нетрадиционным» углом зрения.

Следует констатировать и то положение, что изучение криминалистического мышления сталкивается с рядом проблем как объективного, так и субъективного характера: от методологических подходов к принципиальной возможности исследования криминалистического мышления самой криминалистикой (а отсюда и объективности полученных результатов исследования), до трудностей объективного характера, связанных с особенностями объекта исследования – скрытостью мыслительных процессов от внешнего наблюдения. Нельзя не отметить и имеющие место технические и технологические проблемы внедрения систем искусственного интеллекта в повседневную практику правоохранительных органов, в том числе и по обучению сотрудников работе с ними.

Эти объективно существующие проблемы не помешали криминалистам определить направления, в которых могут быть реализованы возможности искусственного интеллекта по типу искусственных нейронных сетей, среди которых видится весьма востребованным направление выявления признаков серийности в условиях информационной недостаточности; автоматизация экспертных исследований, ведение и расширение системы криминалистических учетов.

Весьма перспективным в прикладном аспекте представляется эксперимент по алгоритму создания и проверки функциональности искусственной нейронной сети, суть которого состоит в выявлении признаков подлога рукописных подписей, выполненных без использования механических и компьютерных устройств, проведенный Д.В. Бахтеевым[165].

[165] *Бахтеев Д.В.* Указ. соч.

Рассуждая о создании криминалистических программ искусственного интеллекта необходимо констатировать, что существенным элементом криминалистического мышления выступает рефлексия, причем рефлексия в особых формах. Как в форме теории рефлексивных игр в приложении к практике раскрытия преступлений, так и в форме методологической рефлексии. Применительно к созданию криминалистических программ искусственного интеллекта следует констатировать, что это не рефлексия уровня субъект деятельности по раскрытию преступлений – субъект преступной деятельности, а иной тип рефлексии. Рефлексии уровня субъект деятельности по раскрытию преступлений – техническое устройство искусственного интеллекта. Трудно будет обойтись без рефлексивных методик как при создании систем искусственного интеллекта, предназначенных для практического использования в раскрытии преступлений, так и при работе с ними на уровне повседневной практической деятельности. Такой подход позволит создателю систем анализировать свое мышление и свою практическую деятельность, находить и устранять самый широкий спектр ошибок и недостатков в ней.

Развитие криминалистических исследований по применению возможностей искусственного интеллекта закономерно привело к тому, что предпринимаются успешные попытки использовать специально созданные компьютерные программы для установления отдельных составляющих профиля неустановленного преступника[166].

Следует также отметить, что сделаны некоторые шаги по созданию и исследованию электронных криминалистически неупорядоченных учетов. «В условиях информатизации всех сфер жизнедеятельности субъекты общественных отношений, в том числе субъекты преступной деятельности, оказываются вовлеченными в информационное общество, существуя и функционируя в условиях постоянного информационного обмена с окружающим миром. Каждое социально значимое действие субъекта влечет за собой не только появление информации, но и ее сохранение, накопление и систематизацию в составе различных учетов, имеющих вид информационных систем – основного инструментария информационных технологий. Использование системы таких учетов, как криминалистических, так и криминалистически неупорядоченных, является одним из эффективнейших способов информационного обеспечения субъекта ДВРП в условиях недостаточности собственно следовой информации»[167].

---

[166] *Бессонов А.А.* Географическое профилирование как метод установления серийных преступников: фантом или реальность? // Эксперт – криминалист. Москва, 2021. № 4. С. 3–6.

[167] *Каминский А.М., Овчинникова Д.А.* Использование электронных криминалистически неупорядоченных банков данных в раскрытии преступлений // Вестник Удмуртского университета. Серия «Экономика и право». 2020. Т. 30, № 1. С. 92.

Анализ практики также показывает, что для успешного раскрытия преступлений в указанной сфере следователю, оперативному работнику, помимо знаний и навыков в области компьютерной техники, необходимо владение терминологическим аппаратом «продвинутых пользователей» – компьютерным сленгом[168].

Исходя из того положения, что следов, не содержащих информацию, не существует, а вопрос в количестве информации и умении следователя или оперативного работника эту информацию актуализировать, можно констатировать, что, в свою очередь, требуется владение следователя или оперативного работника:

– знаниями об особенностях механизма следообразования в различных ситуациях разных областей;

– знаниями, умениями и навыками по обнаружению и фиксации этой информации и восстановлению по ней в идеальной модели хода всего преступления либо его фрагмента. На основе этой модели и выдвигаются в дальнейшем версии, направленные на раскрытие конкретного преступления. Специфичность механизма образования цифровых следов, особенность следовых картин этого вида преступлений затрудняют теоретическую работу, в частности выработку оснований их классификации, выявления их содержания и сущности.

Поэтому сложившаяся ситуация разрешается таким путем, что вначале на теоретическом уровне должна быть создана общая, а значит, высокой степени абстракции модель преступной деятельности в сфере информационных технологий, которая должна охватывать все частные случаи. Передавать ее главные «узлы», то есть отражать структуру преступной деятельности, задачи которой достигаются либо использованием компьютерных технологий, либо их изменения. На основе этой модели возможно эффективное и планомерное исследование специфики данного вида следов и механизмов их образования.

В исходных константах создания данной модели выступают те положения, что любая технология строится из субъектов деятельности, сырья, оборудования, энергоресурсов и технологий обработки. Деятельность в области информационных технологий осуществляют системные операторы, программисты, администраторы, инженеры и техники, пользователи. Производящие мощности – это совокупность взаимосвязанных компьютеров, технологические каналы, приборы, механизмы, оборудование, рабочая среда, программы, обеспечивающие информационные технологии системой алгоритмов. Изменяя информацию, манипулируя с ней, можно воздействовать на такие объекты,

[168] *Каминский А.М., Русских Ж.А.* Некоторые аспекты использования компьютерного сленга для решения задач расследования преступлений в сфере компьютерной информации // Пермский юридический альманах. 2019. № 2. С. 665–672.

как сама информация, материальные ценности, финансы, услуги. Имея в виду особенности и качества этих объектов, арсенал преступников и способы и технологии их действий, ясно, что в результате этого возникает очень разноплановая следовая картина.

По такому основанию можно сделать значимый вывод о том, что эта модель должна содержать не перечень конкретных следов, а их типологию. Представляется возможным рассмотреть три типа следов:

– отражающие изменения собственно субъекта;

– отражающие изменения состояния работы компьютерной техники;

– отражающие изменения полученного в процессе работы информационных технологий продукта.

Весьма важным, на наш взгляд, является то предположение, что цифровые следы имеют двойную природу – материальную и виртуальную. Возникновение конечного состояния цифрового следа невозможно без действий, операций или простых движений человека (оператора, пользователя) при работе с компьютером, мышью, клавиатурой, флэш-картой и т.п.

Таким образом, помимо виртуальной составляющей, такой след содержит и «традиционную» криминалистическую составляющую – следы пальцев рук, записки, запаховые следы, микрочастицы, окурки и другие вещества и предметы, локализованные на рабочем месте оператора (пользователя). Этот перечень при желании можно существенно расширить. Закономерно, что в силу своей новизны и неисследованности внимание ученых приковано в основном к виртуальной составляющей данной группы следов, но следует помнить о том, что эти изменения возможны только как результат первоначального физического контакта оператора (пользователя) с механизмами, приборами и оборудованием компьютерной техники.

Поэтому представляется, что взятый в своем синкретичном виде след, характерный для данной группы преступлений, – это составной, сложный след, результат воздействий и преобразований объектов как материальной, так и виртуальной природы, результат приложения к ним воли преступника. Теоретической базой, иллюстрирующей механизм возникновения этих следов, выступает теория отражения. В рассматриваемых ситуациях кисть руки, пальцы оператора (пользователя), контактирующего с компьютерной техникой, выступают в качестве следообразующего объекта. Следовоспринимающими выступают как те составляющие комплекса компьютера, с которыми проводятся операции, а также как материальные объекты, включенные в деятельность оператора, так и собственно виртуальное пространство, например: электронная почта, поисковые системы, сайты сети «Интернет» и т.д.

Изложенные теоретические положения могут быть использованы в создании криминалистических рекомендаций различного уровня для практики раскрытия преступлений в сфере компьютерной информации. В общении с компьютером индивидуальность пользователя проявляется так же, как при письме на бумаге: скорость, привычка использовать основную или дополнительную части клавиатуры, характер «сдвоенных» и «строенных» нажатий клавиш, излюбленные приемы управления компьютером и т.д., с помощью которых можно выделить конкретного человека среди всех работавших на данной машине.

Представленные в различных источниках материалы по данной теме свидетельствуют, что предпринимаются попытки решить задачу идентификации оператора (пользователя) по признакам клавиатурного почерка решением системы задач установления и анализа признаков индивидуальных особенностей воздействий оператора (пользователя) на клавиатуру. В силу автоматизации процесса набора текста на клавиатуре и в результате многократных повторений и длительных упражнений, у субъекта вырабатывается устойчивый двигательный навык. При этом даже сознательные попытки изменить свой клавиатурный почерк не приводят к положительному результату, благодаря выработанному динамическому стереотипу и эти группы следов оказываются источниками криминалистически значимой информации. Опытным путем выявлено, что пальцы и руки оператора (пользователя) индивидуально и неповторимо контактируют с клавишами клавиатуры, что является индивидуальным признаком[169].

Изучение материальной составляющей цифрового следа в сочетании с виртуальной его составляющей в процессе расследовании этой группы преступлений будет весьма перспективно.

Однако, наряду с очевидными результатами, криминалисты отмечают, что: « …технико-криминалистическое и информационно-компьютерное обеспечение раскрытия, расследования и предупреждения этих преступлений находится в стадии разработки; не закончен процесс формирования криминалистических рекомендаций по тактике подготовки и производства отдельных следственных действий, связанных с обнаружением, фиксацией, изъятием и исследованием электронных следов и их материальных носителей»[170].

---

[169] *Каминский А.М., Рубцов В.Г.* Возможности идентификации пользователя компьютера по следам – отображениям на клавиатуре // Вестник Удмуртского университета. Сер. «Экономика и право». 2022. Т. 32, вып. 5. С. 906–910.

[170] *Вехов В.Б.* Преступления в сфере цифровой экономики: совершенствование расследования на основе положений электронной криминалистики // Пермский юридический альманах. Ежегодный научный журнал. 2019. С. 630–639.

Следует учитывать, что для решения отдельных задач любой из фаз (информационно-поисковой, подготовительной, деятельностно-операционной, сокрытия и маскировки) полноструктурного преступления, то есть преступления, развивающиеся на уровне деятельности (преступления, совершаемые организованными преступными формированиями, преступления в сфере экономики, незаконного оборота наркотиков, в сфере движения, в сфере компьютерной информации и др.), преступники охотно и эффективно используют IT-технологии. Это положение ярко иллюстрируется положением дел в расследовании преступлений в сфере незаконного оборота наркотиков, совершаемых с применением цифровых технологий.

Распространение наркотических средств, их объемы и последствия создают существенную угрозу здоровью населения, подрывают экономический потенциал, негативно влияют на демографическую ситуацию в мире и правопорядок в государстве. Анализ статистических данных и результатов изучения практики расследования уголовных дел, связанных с незаконным оборотом наркотических средств, свидетельствует о неблагополучной динамике показателей, характеризующих рассматриваемый вид преступности. И это при том, что данные официальной статистики не отражают объективную картину наркоситуации ввиду повышенной латентности наркопреступлений.

В настоящее время отмечается интенсивный рост преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием сети «Интернет». Можно констатировать, что это принципиально новый вид преступной деятельности, существенно усложняющий выявление, раскрытие и расследование этого вида преступлений.

Интернет позволяет совершать преступления, связанные с незаконным оборотом наркотических средств, дистанционно, анонимно, быстро и бесконтактно. Потребитель через мессенджеры, такие как Jabber, Signal, VIPole, Telegram и др., либо через интернет-площадки Hydra (в апреле 2022 г. ликвидирована полицией Германии), либо Kraken устанавливает контакт и уславливается о приобретении наркотического средства со сбытчиком через сеть «Интернет». Через электронные платежные системы, такие как Bitcoin и др., либо через аккаунт на площадке Kraken производится оплата приобретаемого наркотического средства. Сбытчик сообщает приобретателю о местонахождении наркотического средства («закладка») также через сеть «Интернет». Таким образом, непосредственного контакта сбытчика и приобретателя нет.

В свою очередь, внутри преступной группы информация о перемещении наркотических средств передается между ее участниками через организатора с использованием сети «Интернет». Лицо, осуществляющее закладку наркотического средства, с использованием приложения NoteCam и др., представляющих

собой приложения камеры мобильного телефона в сочетании с информацией GPS (в том числе широты, долготы, высоты и точности), фотографирует местонахождение тайниковой закладки с наркотическим средством. Далее, фотографиям с использованием Ботов (программы, которые автоматизируют определенные задачи) присваиваются интернет-ссылки, которые через интернет-мессенджеры, либо вышеуказанные интернет-площадки отправляются организатору для последующей отправки покупателю. Это позволяет избежать личных контактов между отдельными участниками преступной группы. В самом общем виде такими мерами обеспечивается конспирация преступной деятельности. Этот преступный механизм исключает возможность применения оперативными сотрудниками отработанных ранее на практике приемов для установления фигурантов преступных групп.

Следует учитывать и еще один принципиальный момент – преступная деятельность с использованием информационно-телекоммуникационных сетей является ведущим видом деятельности в сфере незаконного оборота наркотиков, и осуществляться она может лишь организованными преступными формированиями. Организованная наркопреступность представляет собой многопрофильную структуру, включающую организацию производства, переработки, транспортировки и распространения наркотических средств в общенациональных масштабах. Такая форма преступной деятельности позволяет избежать наиболее уязвимых для преступников ситуаций, существенно повысить ее конспиративность. Ввиду своей сложности и масштабности эта преступная деятельность требует особой организации. Соответственно, и деятельность по выявлению и расследованию данной группы преступлений требует эффективной криминалистической методики расследования преступлений в сфере незаконного оборота наркотиков с учетом обозначенных современных реалий.

В этой связи необходимо отметить два принципиальных момента:

1. С начала роста преступности в сфере незаконного оборота наркотиков методика расследования этого вида преступлений стала объектом пристального внимания и практических работников и ученых-криминалистов. За указанный период было защищено существенное количество диссертаций различного уровня, посвященных как вопросам методики выявления и расследования преступлений в сфере незаконного оборота наркотиков, так и тактике производства отдельных следственных действий.

Так, С.И. Земцова исследовала вопросы участия специалиста в раскрытии и расследовании преступлений, связанных с незаконным оборотом наркотических средств, психотропных и сильнодействующих веществ (диссертация на соискание ученой степени кандидата юридических наук, Москва, 2017). Я.С. Карповым была рассмотрена методика расследования незаконного оборота

прекурсоров наркотиков на первоначальном этапе (диссертация на соискание ученой степени кандидата юридических наук, Москва, 2018). О.А. Решняк раскрывала вопросы использования компьютерных технологий при расследовании преступлений в сфере незаконного оборота опасных психоактивных веществ (диссертация на соискание ученой степени кандидата юридических наук, Волгоград, 2019). О.Ю. Введенской были раскрыты особенности предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий (диссертация на соискание ученой степени кандидата юридических наук, Краснодар, 2022). Кроме того, вопросы методики расследования незаконного оборота наркотических средств неоднократно рассматривались различными авторами в научных статьях, монографиях, учебных пособиях. В частности, немало важных рекомендаций по указанной тематике содержится в учебном пособии «Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием Интернет-магазинов», подготовленном С.И. Земцовой, О.А. Суровым, П.В. Галушиным (Красноярск, 2019).

2. Таким образом, на сегодняшний момент криминалистикой разработана в целом удовлетворительная система криминалистических рекомендаций по выявлению и расследованию преступлений в сфере незаконного оборота наркотиков, однако подавляющее большинство из них ориентированы на ситуации «контактного» сбыта, транспортировки и т.п. наркотических средств, где субъекты преступной деятельности, потребители вынуждены реально контактировать друг с другом.

Но анализ оперативно-розыскной и следственной практики свидетельствует, что организованные преступные формирования, специализирующиеся на совершении преступлений в сфере незаконного оборота наркотиков посредством информационно-телекоммуникационных сетей организовываются таким образом, чтобы обойти наиболее уязвимые звенья в этой сфере преступной деятельности.

Ими до недавнего времени являлись приобретение наркотика потребителем у сбытчика, которое было невозможно без той или иной формы физического, личного контакта, транспортировка оптовых партий наркотиков, личные контакты членов организованных преступных формирований между собой. На этом объективном положении во многом строилась методика раскрытия данного вида преступлений. Но нынешняя ситуация отличается тем обстоятельством, что механизм преступной деятельности ориентирован на бесконтактный способ его функционирования, что автоматически повышает его конспиративность, а, следовательно, и латентность. В явном виде наметилась тенденция перехода к бесконтактным формам преступной деятельности в сфере незаконного оборота наркотиков.

Современные, постоянно совершенствующиеся технические возможности информационно-телекоммуникационных сетей открывают перед членами организованных преступных формирований широкие возможности совершенствования механизма преступной деятельности. Однако ввиду сложности вопроса, в том числе и технической, до сих пор не создана полноструктурная криминалистическая методика расследования этого вида преступлений в сфере незаконного оборота наркотиков. Такая методика может существовать как самостоятельный вид методики, так и выступать частью уже разработанной методики.

Объем статьи не позволяет даже бегло рассмотреть многие направления и тенденции развития криминалистики, но и изложенного достаточно для того, чтобы сделать вывод о том, что цифровизация криминалистики выступает в качестве одного из главных направлений ее развития и за ней будущее науки.

Хомяков Эдуард Геннадьевич,
кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ В ИНТЕРНЕТ-МАГАЗИНАХ (НА МАРКЕТПЛЕЙСАХ[171])

В последние годы стремительный рост электронной коммерции[172] и популярность онлайн-платформ для торговли привели к тому, что значительная часть товаров и услуг стала доступна в интернет-пространстве. Вместе с тем растет и количество преступлений, совершаемых в цифровой среде.

Так, если в 2020 году, когда в отчетности МВД России появились преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, было зарегистрировано 510396 (24,97 % от общего количества зарегистрированных в России преступлений), то в 2021 году – 517722 (25,83 %), в 2022 году – 522065 (26,54 %), в 2023 году – 676951 (34,77 %); раскрываемость данных преступлений по приведенным годам составила соответственно: 20 %, 20 %, 23,4 %, 27,8 %; по официальным данным свыше 98 % подобных преступлений выявляются органами внутренних дел[173].

В январе-августе 2024 года зарегистрировано 500,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 16,4 % больше, чем за аналогичный период прошлого года; в общем числе зарегистрированных преступлений их удельный вес составил на указанный период 39,2 %, раскрываемость 25,9 %[174].

---

[171] Маркетплейс – это онлайн-площадка, собирающая и систематизирующая информацию о товарах и услугах разных компаний, зарегистрированных в системе, и предоставляющая такую информацию по запросу покупателя в структурированном виде, пригодном для сравнения, выбора и осуществления покупки выбранного товара. URL: https://www.gorkilib.ru/events/novoe-slovo-ot-tsentra-nauki2506 (дата обращения: 04.11.2024).

[172] Электронная коммерция (англ. E-commerce, e-commerce) – синоним: онлайн-торговля.

[173] По данным с официального сайта МВД РФ (раздел «Статистика и аналитика»). URL: https://мвд.рф/folder/101762 (дата обращения: 04.11.2024).

[174] Там же.

10 октября 2024 года на координационном совещании в Генеральной прокуратуре Российской Федерации рассматривались вопросы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, цифровой валюты и компьютерной информации[175]. В ходе данного совещания Генеральный прокурор Российской Федерации И.В. Краснов, отмечая низкую раскрываемость данных преступлений и недостаточную эффективность их расследования, указал на то, что «повышение раскрываемости ИКТ-преступлений во многом зависит от эффективности деятельности оперативных и следственных подразделений, оснащения их необходимым программным обеспечением, оборудованием и квалифицированными специалистами».

При этом глава надзорного ведомства констатировал, что ситуация усугубляется нарушениями в деятельности органов расследования и оперативных служб. По его словам, «Отмечается шаблонность и безынициативность проводимой оперативной работы, отсутствие наступательности, недостаточная эффективность предварительного расследования. Во многих делах, как говорится, между двумя корочками больше ничего и нет. И таких дел в масштабах страны тысячи»[176].

По данным международных исследований, каждый год фиксируется рост случаев дистанционного мошенничества, нацеленного на пользователей интернет-магазинов и маркетплейсов. Только за последние два года количество жалоб на онлайн-мошенничество увеличилось более чем на 30 % в странах Европейского Союза и на 25 % в США, что говорит о высокой распространенности данного явления[177]. По России подобная статистика не приводится.

Эти данные подчеркивают актуальность проблемы, поскольку обман пользователей в Интернете подрывает доверие к цифровой торговле и ставит под угрозу безопасность персональных данных и финансовых ресурсов граждан. Более того, дистанционное мошенничество в онлайн-торговле становится

---

[175] Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/events-and-meetings?item=98418092 (дата обращения: 04.11.2024).

[176] Там же.

[177] As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public. URL: https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public (дата обращения: 04.11.2024); Annual number of incoming complaints about internet crime on the IC3 website from 2000 to 2023. URL: https://www.statista.com/statistics/267546/number-of-complaints-about-us-internet-crime/ (дата обращения: 04.11.2024); FBI Releases Internet Crime Report. URL: https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report (дата обращения: 04.11.2024).

значительной проблемой не только для отдельных покупателей, но и для самих платформ, которые вынуждены тратить значительные ресурсы на разработку систем защиты и обработку жалоб от пострадавших.

Под дистанционным мошенничеством в электронной коммерции подразумеваются действия, направленные на обман пользователей через различные цифровые каналы: сайты, социальные сети, мессенджеры и мобильные приложения. Главная сложность таких преступлений – это использование цифровых технологий и анонимных инструментов, что затрудняет их обнаружение и расследование.

Данный вид преступной деятельности не находит непосредственного закрепления в уголовном законодательстве РФ, но может быть криминализован путем применения квалифицированных составов традиционного мошенничества (статья 159 УК РФ) либо составов статьи 159.3 УК РФ «мошенничество с использованием электронных средств платежа» и статьи 159.6 УК РФ «мошенничество в сфере компьютерной информации»[178].

Эти преступления имеют широкий спектр форм и проявлений и направлены на манипуляцию пользователями с целью хищения их денежных средств и личных данных. К основным видам дистанционного мошенничества можно отнести следующие.

Фишинг (фишинговые атаки). Этот вид мошенничества подразумевает рассылку поддельных электронных писем или сообщений, имитирующих официальные уведомления от известных интернет-магазинов (онлайн-платформ) или платежных систем, с целью получения доступа к банковским картам, учетным записям (аккаунтам) или другим конфиденциальным данным пользователей. Часто такие письма содержат ссылки на поддельные страницы авторизации, где пользователь вводит свои данные, которые затем попадают к мошенникам. Фишинг остается одной из самых распространенных угроз в сфере киберпреступности[179].

---

[178] *Говердовская Т.В., Крайнюкова Л.М.* Анализ правовых механизмов противодействия мошенничеству в сфере электронной торговли: европейский и российский опыт // Правопорядок: история, теория, практика. 2021. № 3 (30). С. 134. URL: https://cyberleninka.ru/article/n/analiz-pravovyh-mehanizmov-protivodeystviya-moshennichestvu-v-sfere-elektronnoy-torgovli-evropeyskiy-i-rossiyskiy-opyt (дата обращения: 04.11.2024).

[179] Спам и фишинг в 2023 году (отчет «Лаборатории Касперского» по спаму и фишингу за 2023 год). URL: https://securelist.ru/spam-phishing-report-2023/109104/ (дата обращения: 04.11.2024); Фишинговые сайты в России. URL: https://www.tadviser.ru/index.php/ (дата обращения: 04.11.2024); Количество жертв фишинговых атак в США с 2018 по 2023 год. URL: https://www.statista.com/statistics/1390362/phishing-victim-number-us/ (дата обращения: 04.11.2024).

Фальшивые (поддельные, фейковые) сайты и онлайн-магазины. Мошенники создают сайты-клоны, визуально напоминающие известные торговые площадки, с целью ввести покупателей в заблуждение, заставить их оплатить покупку на поддельном ресурсе. Такие сайты действуют ограниченное время, после чего закрываются, оставляя пользователей без товара и денег. Такие сайты нередко используют доменные имена, близкие к известным брендам. При этом услуги или товары предлагаются, как правило, с большими скидками.

Фальшивые объявления и поддельные профили. На маркетплейсах злоумышленниками могут создаваться фальшивые объявления с указанием привлекательных цен на товары (услуги) или описаниями, направленными на привлечение покупателей. После перевода денег товар либо не отправляется вовсе, либо отправляется с существенными отклонениями от заявленного качества. Такие профили часто имеют малое количество отзывов или предлагают товары по значительно заниженной цене, что само по себе является одним из сигналов возможного мошенничества.

Подмена товара. В данном случае мошенничество связано с тем, что пользователь получает товар, существенно отличающийся от заявленного описания: подделку, низкокачественную копию или поврежденный товар (товар с недостатками). Мошенники могут предлагать брендовые товары, но отправляют дешевые подделки, используя лазейки в политике возврата средств на платформе или анонимные учетные записи для сокрытия своих действий.

Использование взломанных аккаунтов. Мошенники нередко используют взломанные учетные записи реальных пользователей с высоким рейтингом для размещения объявлений или предложений товаров. Пользователи, доверяя рейтингу и репутации учетной записи, могут легко стать жертвами мошенничества, не подозревая о взломе.

Мошенничество с отзывами. Некоторые продавцы манипулируют отзывами и рейтингами, создавая фальшивые положительные отзывы для привлечения покупателей и повышения доверия к своим товарам. Это затрудняет покупателям адекватно оценить качество товара или надежность продавца.

Подобные виды мошенничества создают существенные трудности для расследования, так как зачастую злоумышленники используют методы сокрытия своих действий, такие как фальшивые аккаунты, онлайн-оплаты через VPN[180] и криптовалютные платежи.

[180] VPN (англ. Virtual Private Network – «виртуальная частная сеть») – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх какой-либо другой сети.

К типичным признакам мошенничества на платформах электронной коммерции и маркетплейсах можно отнести следующие.

Низкие цены. Одним из основных признаков мошенничества является предложение товаров по сильно заниженным ценам. Такие предложения могут казаться выгодными, но обычно направлены на привлечение максимального числа потенциальных жертв.

Отсутствие отзывов или подозрительные отзывы. На многих платформах можно встретить объявления без отзывов или с рядом позитивных, но схожих по структуре и содержанию комментариев. Мошенники нередко используют поддельные профили для создания фальшивых отзывов, чтобы повысить доверие к своим предложениям.

Отсутствие контактных данных. Мошеннические сайты часто не предоставляют контактную информацию или предлагают только электронную почту и формы обратной связи, исключая номер телефона или физический адрес. Это усложняет возможность проверить надежность продавца.

Необычные запросы. Например, когда продавец требует перевода средств на карту напрямую либо просит подтвердить личные данные или банковские реквизиты.

Сложность возврата и отказ от гарантии. Продавцы могут уклоняться от предоставления информации о возврате товара или гарантии. Это может служить сигналом о ненадежности продавца и повышенных рисках для покупателя.

Эти типичные признаки и характеристики дистанционных мошенничеств позволяют пользователям заранее выявить возможные угрозы. Важность повышения осведомленности покупателей о подобных признаках и мошеннических схемах является ключевой задачей для платформ, так как это способствует более высокой безопасности и снижению числа успешных мошенничеств в электронной коммерции.

Следует также отметить, что борьба с дистанционным мошенничеством осложняется множеством правовых аспектов. Так, многие онлайн-платформы зарегистрированы в других странах (с более благоприятными для них налоговыми и правовыми условиями) и не обязаны сотрудничать с российскими правоохранительными органами, например предоставлять по их запросу данные о транзакциях, логах или IP-адресах пользователей. Более того, различные страны имеют свои подходы к защите персональных данных. Например, Общий регламент о защите данных ЕС (GDPR)[181] накладывает строгие ограничения на обработку (в том числе передачу кому-либо) персональных данных граждан ЕС.

[181] О GDPR на русском. Информация об Общем регламенте по защите данных. URL: https://ogdpr.eu/ru (дата обращения: 04.11.2024).

В случае с Россией отдельные интернет-магазины могут ссылаться на национальные законы для отказа в сотрудничестве или требовать соблюдения сложных международных процедур, таких как судебные запросы, что замедляет расследования и усложняет оперативное получение информации.

Эти аспекты подчеркивают необходимость разработки специальных криминалистических методов и технологий, которые позволяли бы эффективно выявлять и расследовать дистанционные мошенничества, связанные с онлайн-торговлей.

Для успешного расследования дистанционных мошенничеств необходимо четкое следование алгоритмам, которые систематизируют сбор и анализ цифровых (электронных) доказательств. Разработка и применение подобных алгоритмов помогают упорядочить процесс расследования, повысить эффективность взаимодействия между следователями и интернет-магазинами, а также минимизировать риски ошибок и потерь данных (цифровых следов).

Такие алгоритмы должны обеспечивать унифицированный подход к сбору и анализу цифровых (электронных) доказательств; в них должен быть отражен специализированный инструментарий, необходимый для работы с цифровыми следами.

Без сомнения, разработка и применение надежных методов борьбы с дистанционным мошенничеством не только способствует выявлению лиц, совершающих подобные преступления, но и укрепляет доверие пользователей к электронной коммерции.

На начальном этапе расследования дистанционных мошенничеств рассматриваемого вида должен проводиться сбор и фиксация всех возможных цифровых следов, оставленных преступниками в ходе совершения преступления, к которым можно отнести записи чатов, электронные письма, переписки на платформах, историю браузера, а также транзакционные данные.

Следователь со специалистом производит фиксацию скриншотов страниц, на которых были размещены мошеннические объявления, переписки с подозреваемыми или транзакции, а также сопутствующих метаданных, таких как время создания файлов, информация об устройстве, данные о местоположении и другие технические параметры, которые могут помочь в дальнейшем анализе, а также подтвердить или опровергнуть версии подозреваемого.

Далее по IP-адресам, использованным для входа в аккаунты, размещения объявлений или отправки сообщений, устанавливается реальное географическое положение (геолокация) цифрового устройства подозреваемого; при этом в отдельных случаях возможно получение данных об интернет-провайдере, услугами которого пользовался подозреваемый, или о его цифровом устройстве.

Логи с серверов и веб-сайтов, используемых подозреваемыми, могут содержать данные о времени входа, изменениях в учетных записях, IP-адресах

и их действиях на конкретных сайтах. Эти данные позволяют определить возможные маршруты, по которым были получены доступы или выполнены транзакции.

Не менее важной является задача по определению типа платежной системы (электронные кошельки, карты, криптовалюты), использованной для перевода и обналичивания средств; это необходимо для отслеживания платежных потоков. Для этого могут применяться специализированные аналитические инструменты; к ним можно отнести, например, такие программные продукты, как Chainalysis, Elliptic, CipherTrace, TRM Labs, Crystal Blockchain и другие[182], которые используют методы анализа блокчейна, сопоставления данных и выявления связей между адресами кошельков, что позволяет обнаруживать связь между криптокошельками, транзакциями и платежными аккаунтами.

Для фиксации цифровых следов, оставленных в сети, могут использоваться специализированные программы, например: FTK Imager, Autopsy, Wireshark или их отечественные аналоги, которые помогают зафиксировать переписку и передаваемые данные, сохранив их целостность и достоверность.

При расследовании подобных преступлений в адрес интернет-магазинов, компаний сотовой связи, банковских учреждений, провайдеров услуг и т.п. направляются соответствующие запросы о предоставлении информации, имеющей доказательственное значение по уголовным делам данной категории; при этом длительность получения ответа на запросы в их адрес может достигать нескольких месяцев. Полученные при подобных запросах официальные документы могут признаваться вещественными доказательствами и приобщаться к материалам уголовного дела.

Методика сбора и анализа данных из открытых источников информации (OSINT-разведка[183]) позволяет собирать информацию о подозреваемом из открытых источников – социальных сетей, форумов, блогов и т.д.

Современные инструменты OSINT позволяют выявлять связи между учетными записями – профилями пользователя – на различных цифровых платформах и сервисах и могут помочь в построении более полной картины деятельности подозреваемого[184].

---

[182] Лучшие инструменты для блокчейн-анализа и как они работают. URL: https://investfuture.ru/articles/id/luchshie-instrumenty-dlya-blokcheyn-analiza-i-kak-oni-rabotayut (дата обращения: 04.11.2024).

[183] OSINT (англ. Open Source Intelligence, «разведка по открытым источникам»). См., например, OSINT или разведка по открытым источникам. URL: https://habr.com/ru/companies/deiteriylab/articles/595801/ (дата обращения: 04.11.2024).

[184] *Бессонов А.А.* Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности : сборник научных трудов Межведомственной

Сопоставление данных о входе с разными учетными записями может позволить выявить связь между различными аккаунтами, используемыми подозреваемым. Это позволяет связать подозреваемого с другими случаями мошенничества на той же или других торговых онлайн-платформах.

Особого внимания заслуживает проблема с определением места проведения расследования подобных преступлений, поскольку место совершения преступления и место наступления последствий, как правило, не совпадают. На повышение оперативности раскрытия преступлений, предусмотренных статьями 158, 159–159.3, 159.5, 159.6 УК РФ, а также в целях полноты возмещения причиненного им вреда, соблюдения разумного срока уголовного судопроизводства направлен приказ МВД РФ от 03.04.2018 № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений». Однако в данной работе указанная проблема в силу ее объемности (масштабности) не рассматривается.

Описанный выше примерный алгоритм расследования дистанционного мошенничества, связанного с электронной коммерцией (интернет-торговлей), помогает последовательно собирать и анализировать цифровые следы, что значительно повышает вероятность успешного раскрытия преступления.

Интересен пример проведения подобного расследования на основе реального события[185].

В 2023 году неустановленное лицо разместило в социальной сети «ВКонтакте» в сообществе «Рыбацкая барахолка» объявление о продаже эхолота (которым лицо в действительности не обладало) за 6000 рублей. Потерпевший У., проживающий в Пермском крае, увидев это объявление и решив эхолот приобрести, вступил в переписку с пользователем данной сети под соответствующим именем (В.). В ходе переписки пользователь В. указал, что условием покупки эхолота является полная предоплата товара, с чем потерпевший У. согласился и перевел указанную сумму со своего счета на счет, указанный пользователем В., используя приложение «Сбербанк Онлайн» (оба счета были привязаны к соответствующим банковским картам ПАО «Сбербанк»).

научно-практической конференции, Москва, 16 сентября 2022 года. Москва : Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя, 2022. С. 40–45; *Головин А.Ю.* К вопросу собирания криминалистически значимой информации по открытым цифровым данным // Актуальные проблемы криминалистики и судебной экспертизы : сборник материалов Международной научно-практической конференции, Иркутск, 16–17 марта 2023 года. Иркутск : Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2023. С. 29–32.

[185] По материалам уголовного дела № 12301570077000019, возбужденного в следственном отделении МВД России «Куединский» по Пермскому краю.

После чего пользователь В., не выполнив взятые на себя обязательства, полученные денежные средства в сумме 6000 рублей похитил и распорядился по своему усмотрению.

На первоначальном этапе расследования после возбуждения уголовного дела (по ч. 2 ст. 159 УК РФ) был допрошен потерпевший У. В ходе допроса был установлен банковский счет, на который были отправлены денежные средства. По установленному банковскому счету был направлен запрос в ПАО «Сбербанк» посредством электронного документооборота. Банковским учреждением в течение этого же дня была предоставлена информация о принадлежности банковского счета с указанием паспортных данных конкретного лица, месте открытия банковского счета и движении денежных средств по данному счету, что подтвердило факт поступления денежных средств от потерпевшего У. Также была получена информация по банковскому счету потерпевшего и движению денежных средств на нем. Полученные из банка выписки были осмотрены в установленном законом порядке и признаны вещественными доказательствами.

После установления личности владельца банковского счета (им оказалась жительница Калининградской области П.), на который поступили 6000 рублей, в отдел полиции по месту его проживания было направлено поручение о допросе данного лица в качестве свидетеля по существу уголовного дела. Оперативными сотрудниками отдела полиции данное лицо было установлено и следователем данного отдела допрошено по существу уголовного дела. В ходе допроса в качестве свидетеля П. рассказала о том, что данная банковская карта находится в пользовании у ее брата Т. В процессе розыска Т. было установлено, что он находится в г. Санкт-Петербурге, где Т. был задержан и допрошен в качестве подозреваемого по существу уголовного дела; при этом им были даны признательные показания. В дальнейшем гражданину Т. было предъявлено обвинение.

Срок предварительного следствия по данному уголовному делу составил не более 2 месяцев. Это стало возможным в связи с налаженной между МВД России по Пермскому краю и ПАО «Сбербанк» системой электронного документооборота по оперативному предоставлению запрашиваемой информации.

Данная система позволяет автоматически обмениваться 11 типами запросов с заверением электронной подписью, а именно в отношении сведений о:

– счетах (карточных, вкладах), принадлежащих указанному в запросе лицу на дату/период;
– владельце указанного счета/вклада;
– картах и счетах, принадлежащих указанному в запросе лицу на дату/период;
– владельце указанной карты;
– номере телефона, привязанного к карте на дату/период;
– картах, к которым привязан указанный номер телефона на дату/период;

– движении денежных средств по счету за период;
– движении денежных средств по карте за период;
– наличии арендованных банковских ячеек;
– IP-адресах входа в удаленные каналы обслуживания;
– смс-сообщениях на указанный номер телефона/карту за период.

Следует отметить, что не со всеми банковскими учреждениями у территориальных подразделений МВД налажен электронный документооборот, вследствие чего соответствующие запросы (согласно части 4 статьи 21 УПК РФ) могут выполняться в течение значительного времени (до 2–3 месяцев); при этом установленный законом двухмесячный срок предварительного следствия необходимо продлевать.

При подготовке запроса руководителям интернет-магазинов следователя может интересовать:

– информация о совершенной операции (в конкретный день и время, на конкретную сумму);
– информация о товаре, который был оплачен посредством конкретной банковской карты;
– полные анкетные данные лица (покупателя, продавца), которому принадлежит аккаунт;
– абонентский номер и адрес электронной почты покупателя (продавца), указанные при регистрации аккаунта;
– с каких IP-адресов покупателем был совершен вход на конкретную страницу интернет-магазина, информация о его цифровом устройстве, включая IMEI (с которого был выполнен вход), его географическое местоположение за определенный период;
– адрес, на который была оформлена доставка товара.

Результаты применения предложенного алгоритма показывают его высокую эффективность в выявлении и расследовании случаев дистанционного мошенничества в сфере онлайн-торговли, однако борьба с подобными преступлениями требует комплексного подхода и постоянного совершенствования методов расследования.

Необходимо также отметить, что с развитием электронной коммерции и повсеместным использованием онлайн-платформ для покупок дистанционные мошенничества стали серьезной угрозой не только для покупателей, но и для самих платформ.

Электронные коммерческие платформы играют важную роль в предотвращении и выявлении мошенничества, поскольку они обладают техническими возможностями для мониторинга активности пользователей (покупателей и продавцов), внедрения современных систем безопасности и сотрудничества с правоохранительными органами.

Под мониторингом активности на электронных коммерческих платформах подразумевается отслеживание действий пользователей для выявления подозрительных или потенциально мошеннических схем.

Платформы могут отслеживать, как пользователи пользуются ее сервисом. Например, подозрительная активность может проявляться в виде повторяющихся действий, таких как частое размещение объявлений с необычно низкими ценами, постоянные попытки избегать безопасных платежных систем или многочисленные отмены сделок.

Также платформы отслеживают финансовые операции и используют антифрод-системы[186], чтобы обнаружить аномалии в действиях пользователей. Например, система может сигнализировать, если для нескольких аккаунтов используется один и тот же способ оплаты или если происходит большое количество переводов с недавно созданных учетных записей.

Современные антифрод-системы применяют машинное обучение и искусственный интеллект для выявления подозрительных транзакций и поведения пользователей. Например, такие системы могут автоматически блокировать аккаунты, демонстрирующие нехарактерные схемы покупок или действий, отклоняющиеся от стандартного поведения. На крупных платформах эти системы могут анализировать тысячи транзакций в реальном времени, минимизируя риски и позволяя незамедлительно предпринимать соответствующие меры.

Анализ IP-адресов, геолокаций и идентификаторов цифровых устройств помогает выявлять аномалии или отклонения от обычного поведения пользователя. Если пользователь внезапно заходит на онлайн-платформу из различных стран или с разных IP-адресов, то это может быть признаком взлома или использования учетной записи для мошенничества.

Указанные данные собираются для обнаружения и предотвращения мошеннической активности своих пользователей, при этом платформы также могут применять технологии машинного обучения и алгоритмы для распознавания моделей мошенничества. Такой мониторинг помогает своевременно выявлять риски и защищать добросовестных пользователей.

Платформы взаимодействуют с правоохранительными структурами не только для передачи данных, но и для информирования пользователей о безопасных методах покупок и рисках мошенничества. Платформы, как правило, обязуются сохранять конфиденциальность данных пользователей, передавая информацию лишь по запросу компетентных органов.

---

[186] Антифрод-системы (англ. anti-fraud – борьба с мошенничеством) – программные комплексы для предотвращения мошеннических транзакций, например, Kount, Riskified, Fraud.net, Sift, ClearSale и другие. См., например, 15 Лучших программ и инструментов для выявления мошенничества в 2023 году (рейтинг и сравнение). URL: https://dzen.ru/a/ZS2F1-kCs2hIdkAX (дата обращения: 04.11.2024).

Важным аспектом является также разработка обучающих материалов для правоохранителей, что позволяет им лучше понимать внутренние процессы работы платформы и эффективнее запрашивать нужную информацию.

Одним из ключевых элементов в борьбе с дистанционным мошенничеством в онлайн-торговле является внедрение эффективных политик безопасности. Эти политики включают обязательную проверку учетных записей продавцов, мониторинг транзакций и постоянное обновление условий использования для усиления ответственности и предупреждения рисков.

Например, платформы все чаще используют двухфакторную аутентификацию и биометрические данные для повышения уровня безопасности. Эти методы защищают учетные записи от взломов и минимизируют вероятность неправомерного доступа.

Еще один эффективный способ противодействия мошенничеству – проверка новых продавцов и их контактных данных, что исключает возможность мгновенного создания фальшивых аккаунтов для проведения разовых мошеннических транзакций.

Многие компании, связанные с электронной коммерцией, утверждают, что, попав в ситуацию, связанную с мошенничеством, они ускоряют внедрение новых технологий, в том числе, таких как искусственный интеллект и машинное обучение, и в результате количество повторных инцидентов заметно снижается[187].

В 2022 г. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации запустило систему «Антифишинг», которая предназначена для автоматического выявления мошеннических (фишинговых) сайтов – копий официальных порталов госорганизаций, маркетплейсов и социальных сетей; разработка платформы данной системы была проведена в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика»[188]. В этом же году Роскомнадзором была запущена единая платформа верификации телефонных вызовов (ЕПВВ) «Антифрод», предназначенная для блокировки мошеннических звонков с подменных номеров[189].

---

[187] Всемирный обзор экономических преступлений за 2020 год. URL: https://roscongress.org/materials/vsemirnyy-obzor-ekonomicheskikh-prestupleniy-za-2020-god/ (дата обращения: 04.11.2024).

[188] Как бы не атака: власти запустят ИТ-систему для борьбы с мошенниками. URL: https://digital.gov.ru/ru/events/41512/ (дата обращения: 04.11.2024); В России запущена система автоматической борьбы с мошенническими сайтами. URL: https://corp.cnews.ru/news/top/2022-06-06_v_rossii_zapushchena_sistema (дата обращения: 04.11.2024); Минцифры анонсировало систему «Антифишинг»: что это значит. URL: https://www.rbc.ru/life/news/62f4c3e39a7947b635c8bf91 (дата обращения: 04.11.2024).

[189] Роскомнадзор запустил платформу для борьбы с телефонным мошенничеством. URL: https://digital.gov.ru/ru/events/42390/ (дата обращения: 04.11.2024); Роскомнадзор начал подавать на операторов связи в суд за отказ подключаться к «Антифроду». URL: https://www.tadviser.ru/index.php/ (дата обращения: 04.11.2024).

В 2024 году появились сообщения о планах создания единой цифровой платформы для обмена данными между участниками финансового рынка, Банком России, Минцифры, компанией «Ростелеком» и МВД в целях борьбы с мошенничеством[190].

Данную платформу «ТелекомЦерта» планируют создать в 2025 году для автоматизации взаимодействия уполномоченных органов и организаций. В том числе она будет использоваться для мониторинга утечек персональных данных. К 2030 году к ней планируют подключить все финорганизации, операторов связи и «цифровые платформы». В их число могут войти владельцы соцсетей, маркетплейсов и разработчиков мобильных приложений. В системе создадут «единое окно» для приема обращений граждан и компаний о мошенничестве. Согласно задумке авторов документа, это позволит к 2030 году сократить время блокировки фишинговых и мошеннических ресурсов с восьми часов до четырех[191].

Сотрудничество между российскими платформами электронной коммерции и правоохранительными органами находится на стадии развития.

Создание и развитие автоматизированных систем, таких как «Антифишинг» и «Антифрод», а также разработка единой платформы «ТелекомЦерта» подчеркивают важность межведомственного взаимодействия и модернизации средств защиты в условиях цифровой экономики.

Эти инициативы нацелены на повышение оперативности блокировки мошеннических ресурсов и создание более безопасной среды для пользователей различных онлайн-ресурсов.

Ожидается, что в ближайшие годы интеграция всех участников на единой платформе значительно упростит процесс обмена информацией между коммерческими платформами, правоохранительными органами и регуляторами (в лице Банка России, Минцифры, Роскомнадзора, Ростелекома и др.).

Современные технологии и тесное сотрудничество с правоохранительными структурами позволят минимизировать ущерб от дистанционных мошенничеств и обеспечить доверие граждан к электронной коммерции.

---

[190] Минцифры поддержало создание цифровой платформы для борьбы с мошенниками. URL: https://ria.ru/20240418/platforma-1940820242.html (дата обращения: 04.11.2024).

[191] На единую госплатформу по противодействию мошенничеству в интернете планируют выделить более 6 млрд рублей из бюджета. URL: https://habr.com/ru/news/847338/ (дата обращения: 04.11.2024).

Соболев Сергей Владимирович,
старший преподаватель кафедры уголовного процесса
и криминалистики

ИНФОРМАЦИОННЫЕ СИСТЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Отечественная и зарубежная практика деятельности правоохранительных органов по предотвращению, выявлению и раскрытию преступлений свидетельствует о связи между уровнем информационной поддержки мероприятий по борьбе с преступностью и их результатами.

В научно-технической литературе часто используются термины: «система», «система управления», «автоматизированная система управления», «автоматизированные информационные системы».

Под системой понимается совокупность связанных между собой и с внешней средой элементов или частей, функционирование которых направлено на получение конкретного полезного результата.

Информационная система (ИС) – это совокупность внутренних и внешних потоков прямой и обратной информационной связи объекта, методов, средств, специалистов, участвующих в процессе обработки информации и выработке управленческих решений.

Информационная система представляет собой систему, функционирование которой во времени заключается в сборе, хранении, обработке и распространении информации о деятельности какого-то объекта реального мира. Информационная система создается для конкретного экономического объекта и должна в определенной мере копировать взаимосвязи элементов объекта.

Информационные системы предназначены для решения задач обработки данных, автоматизации конторских работ, выполнения поиска информации и отдельных задач, основанных на методах искусственного интеллекта.

К одной из информационных систем можно отнести криминалистическую (уголовную) регистрацию. Методы регистрации в целях борьбы с преступностью использовались еще в глубокой древности. Для этого применялись обычно два способа: клеймение и калечение, одновременно осуществлявшие функции наказания и опознания (второй век до н.э. древнеиндийские законы Ману; законы Хаммурапи, древнего Вавилона). Физические увечья указывали не только на характер содеянного преступления, но и на то, сколько преступлений

было совершено данным лицом. В России, например, ворам накладывали на лицо особое клеймо. При Петре I вместо наложения раскаленного клейма стали прикладывать пластинку, утыканную иглами, а затем в ранки втирали порох, чтобы можно было разобрать преступников. Иглы располагались либо в форме орла, либо в виде букв или целых слов (например: вор, убийца и т.д.[192]). В Англии проводились так называемые «идентификационные парады», заключавшиеся в том, что преступников, находящихся в заключении, осматривали полицейские, стараясь опознать ранее виденных.

Начало формирования криминалистической регистрации на научной основе было положено в конце XIX века внедрением антропометрического (А. Бертильон в 1882 году предложил производить 11 измерений тела: рост, высота в сидячем положении, длина и ширина головы, правого уха, левой ступни и т.п.) и дактилоскопического (В. Гершель, Г. Фулдс, Г. Гальтов в 1887–1891 гг.) способов регистрации преступников. В России дактилоскопическая регистрация была введена в 1905 году[193]. Первоначально система получила название «уголовная регистрация», ибо ее основу составлял учет лиц, привлеченных к уголовной ответственности, и совершенных ими преступлений. Последовательно расширился круг учитываемых объектов (сейчас регистрируются без вести пропавшие лица, трупы, предметы преступного посягательства, средства и способы совершения преступлений, предметы со следами преступлений, следы преступлений и т.д.). Разработанные криминалистами средства и методы получения указанной информации стали более совершенными. Все это позволило уточнить название регистрационной системы и считать ее именно криминалистической регистрацией.

Таким образом, криминалистическая регистрация имеет давнюю историю. С момента появления криминалистическая регистрация прошла в своем развитии четыре основных этапа:

первый характеризуется появлением первых примитивных форм регистрации, одновременно выполнявших роль и регистрации, и наказания;

второй – письменная форма регистрации;

третий – появление первых научно обоснованных учетных систем в связи с развитием антропометрии и дактилоскопии;

четвертый – автоматизация учетно-регистрационных систем в связи с появлением электронно-вычислительной техники.

---

[192] *Молчанов Н.Н.* Дипломатия Петра Великого. М., 1991. С. 199.

[193] *Рассейкин Д.П.* Очерки истории уголовной регистрации. Саратов, 1976. С. 60.

В настоящее время наметился переход от отдельных учетов к интегрированным и автоматизированным банкам данных, позволяющий сосредоточить в едином массиве сведения о различных объемах учета, освобождая специалиста от необходимости обращения к нескольким видам учета. Широкое распространение получили автоматизированные банки данных (АБД). Продолжается процесс создания и внедрения в практическую деятельность новых видов учета.

В информационно-регистрационных массивах можно выделить две группы учетов: специально созданные для нужд правоохранительных органов и созданные для информационного обслуживания государственных, общественных, частных структур и граждан. К криминалистической регистрации относится лишь та информация, которая обеспечивает криминалистическую деятельность (оперативно-розыскную, следственную и экспертную).

Криминалистическая регистрация интегрирует научные положения криминалистической трасологии, габитоскопии, почерковедения, других разделов криминалистики.

По определению Р.С. Белкина, **криминалистическая регистрация** в ее предметном выражении – это определенная система материальных объектов (картотеки, коллекции и иные хранилища регистрационных данных), как институт практической деятельности она основана на единстве системы вещественных средств регистрации и системы действий, оперирования этими средствами в борьбе с преступностью[194].

Целями криминалистической регистрации являются:

1) накопление данных, которые могут быть использованы для раскрытия, расследования и предупреждения преступлений;

2) обеспечение уголовной идентификации объектов с помощью учета данных;

3) содействие поиску объектов, данные о которых содержатся в криминалистических учетах;

4) предоставление в распоряжение оперативно-разыскных, следственных и судебных органов справочной и ориентирующей информации.

Система средств регистрации складывается из подсистем, называемых криминалистическими учетами, которые отличаются друг от друга учитываемыми данными, а также способами и формами их сосредоточения и систематизации.

Криминалистические учеты обычно именуются по видам учитываемых (регистрируемых) объектов, например: учет похищенного, утерянного, изъятого, добровольно сданного огнестрельного оружия, поддельных денежных знаков, дактилоскопический учет неопознанных трупов.

---

[194] *Белкин Р.С.* Курс криминалистики. М., 1977. Т. 2. С. 181.

От вида криминалистического учета следует отличать форму учета, то есть способ накопления регистрируемой информации: картотеки, коллекции, списки, альбомы, магнито- и видеозаписи, цифровизации учетов. Накопление информации производится, как и в любой другой информационной системе, с использованием информационно-поискового языка – искусственного языка, предназначенного для формализованного описания содержания данных и (или) отработки запросов, поступающих в систему. Перевод информации с естественного языка на информационно-поисковый осуществляется по определенным правилам в соответствии со словарем поисковых признаков (тезаурусом системы).

Разнообразны способы фиксации криминалистической информации: описательный (алфавитный, по признакам внешности, по способу совершения и т.п.); изобразительный, то есть изготовление вещественных изображений (фотоснимков, микрокарт, микрофишей, дактилоскопических карт, слепков и т.п.); графический (схемы, чертежи, хроматограммы, профилограммы, спектрограммы и т.п.); коллекционный (сбор натурных коллекций объектов-оригиналов и сравнительных образцов).

Информационное обеспечение процесса расследования понимается как процесс отыскания, опенки и использования криминалистической информации.

В процессе расследования возможно возникновение различных ситуаций, которые принято именовать следственными. Они могут быть простыми и сложными. В зависимости от складывающейся по уголовному делу ситуации лицо, производящее расследование, нуждается в получении информации, которая способствовала бы решению стоящих перед ним задач. С целью накопления, обработки, хранения и выдачи криминалистической информации созданы специализированные учеты. В своей деятельности лица, осуществляющие следствие, обращаются также к различным вспомогательным учетам, ведомственным массивам, регистрационно-справочной документации.

Занесение в базу данных того или иного криминалистического учета осуществляется посредством регистрации индивидуализирующих признаков, которые можно рассматривать как сигналы, несущие криминалистическую информацию.

Одна часть криминалистических учетов содержит краткое описание объектов учета, и основным их назначением является помощь в раскрытии, расследовании и предупреждении преступлений путем проверки наличия сведений об объекте и его местонахождении на момент запроса (оперативно-справочные учеты). Другая – содержит подробные сведения об объекте учета и выполняет наряду с оперативно-справочной функцией и функцию сравнения не только установленных данных об объекте учета, но и сходных внешних описаний.

Эффективность информационного обеспечения деятельности правоохранительных органов зависит от полноты сбора, качества обработки, надежности хранения и поиска, оперативности выдачи ориентирующей криминалистической информации, необходимой при расследовании преступлений. Хранение и поиск информации занимают в информационном процессе центральное место. Их сущность заключается в обеспечении сохранности сведений, содержащихся в информационных массивах, и выдаче на запрос необходимой для заинтересованного лица информации. В качестве средства хранения и поиска информации выступают информационно-поисковые системы, автоматизированные и интегрированные банки данных. Последние обрабатывают сейчас разнородные массивы данных, и процедура обработки их охватывает информацию по всем видам данных.

Новые технические возможности обработки информации постепенно изменяют форму учетов. Идет переход от механизированного к автоматизированному способу обработки информации. Создаются автоматизированные информационно-поисковые системы (АИПС), широко применяемые в настоящее время в деятельности правоохранительных органов. Такие системы осуществляют многоаспектный поиск необходимых сведений, хранящихся в электронной памяти (информация).

Первая АИПС появилась в штате Иллинойс США в 1953 г. Она позволяла ускорить розыск угнанных автомашин.

Эффективность использования криминалистических учетов существенно повысилась в связи с применением для обработки криминалистической информации средств автоматизации и вычислительной техники, позволяющих не только во много раз сократить время обработки запросов, но и устанавливать корреляционные зависимости между объектами регистрации. Совершенствование технической и информационной базы криминалистических учетов в целом и отдельных видов в частности продолжается постоянно.

Практика расследования преступлений во всем мире свидетельствует о том, что в подавляющем большинстве случаев на месте происшествия остаются следы рук правонарушителя.

Следы рук по своему криминалистическому значению занимают первое место в группе следов. Такая возможность обусловлена строением кожного покрова ладонной поверхности и особыми свойствами папиллярных узоров ногтевых фаланг пальцев рук человека. Поэтому для раскрытия и расследования преступлений используется дактилоскопия (от двух древнегреческих слов: «дактилос» – палец и «скопео» – смотрю, изучаю), т.е. изучающий следы пальцев.

Для этого следы рук живого человека или трупа фиксируются на специальных бланках, т.е. формируются дактилоскопические карты с отпечатками

поверхностей всех пальцев и ладоней рук человека. Такой способ дактилоскопирования носит название десятипальцевого. На лицевой стороне карты указываются также демографические данные, а на оборотной – сведения о судимостях, задержаниях и особых приметах этого лица. На местах происшествия при обнаружении следов пальцев рук проводится фиксация этих следов, а затем и изъятие с помощью криминалистических средств.

Однако десятипальцевая дактилоскопическая картотека практически не используется для проверки следов рук с мест преступлений, которые обычно являются одиночными. Имеются также сложности при установлении личности трупов, когда по каким-то причинам (например вследствие гнилостных изменений) не удаётся получить отпечатки нескольких пальцев рук.

Описанные проблемы стали решать с созданием монодактилоскопической картотеки – АДИС (Автоматизированная дактилоскопическая информационная система), в которой отпечаток каждого отдельного пальца является отдельным объектом картотеки. Создание такой картотеки возможно с использованием средств вычислительной техники и при условии, что папиллярный узор каждого пальца будет описан с очень высокой степенью информативности, поскольку нужный узор должен быть с высокой степенью надёжности найден в массивах в сотни миллионов объектов (современные объёмы баз данных). Система также должна по возможности обеспечивать поиск не только полного папиллярного узора, но и его фрагмента (при идентификации по следам рук, изъятым с мест преступлений, или трупов со значительными гнилостными изменениями).

Для непосредственного ввода дактилоскопической информации в АДИС используется бескрасковое дактилоскопирование пальцев и ладоней («живой» сканер), а также высокоскоростные сканеры, специальные фото- и телекамеры для считывания папиллярных узоров с дактилоскопических карт и иных носителей.

25 июля 1998 года Президентом РФ был подписан Закон «О государственной дактилоскопической регистрации в Российской Федерации». В соответствии с этим законом дактилоскопической регистрации подлежат как лица, привлекавшиеся к уголовной ответственности, так и другие категории граждан, в том числе занимающиеся опасными для жизни видами деятельности: военнослужащие, сотрудники правоохранительных органов, противопожарных и аварийно-спасательных служб, экипажи воздушных судов и т.д. Также возможно добровольное прохождение регистрации.

В 2002 году было начато выполнение федеральной программы автоматизации дактилоскопических учётов. Для этого стали использовать разработанную систему АДИС «ПАПИЛОН». Системы «ПАПИЛОН» – это вертикально интегрированный провайдер различных биометрических решений типа АДИС

с высокими поисковыми характеристиками, способная обеспечить максимальную автоматизацию всех технологических процессов ввода, обработки, сравнения, хранения и передачи дактилоскопической информации. Весь массив дактилокарт Главного информационно-аналитического центра МВД России (более 20-ти миллионов дактилокарт) переведён на автоматизированный режим работы. В настоящее время проверка одного следа по этому массиву занимает всего несколько десятков минут, что экономит тысячи человеко-часов рабочего времени.

Так, 16.01.2002 было возбуждено уголовное дело по признакам преступления, предусмотренного п. «а» ч. 2 ст. 105 УК РФ, по факту обнаружения в подвале дома № 10 по ул. Восточная г. Ижевска трупов трех неустановленных мужчин с признаками насильственной смерти.

16.05.2002 предварительное следствие по уголовному делу приостановлено в соответствии с п. 3 ч. 1 ст. 195 УПК РФ, в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

В октябре 2015 года было принято решение провести повторные исследования изъятых с места происшествия отпечатков пальцев рук, в том числе ограничено пригодных, на более совершенном оборудовании с использованием обновленных программ ЭКЦ МВД по УР – АДИС «ПАПИЛОН».

В конце ноября 2015 года была получена информация о совпадении одного из следов с дактокартой гр. И., уроженца Удмуртской АССР.

В результате чего расследование уголовного дела возобновлено и установлено, что в один из дней начала января 2002 года в вечернее время гр-не В. и И., находясь в подвале дома № 10 по ул. Восточная г. Ижевска, в ходе употребления спиртных напитков, на почве внезапно возникших личных неприязненных отношений нанесли многочисленные побои руками и ногами по различным частям тела трем неустановленным мужчинам, которые от полученных телесных повреждений скончались на месте[195].

Мультибиометрический потенциал системы представлен возможностью хранения в записи дактилокарты дополнительных характеристик личности – двухмерных фронтальных изображений внешности, изображений радужных оболочек глаз, а также – трёхмерных изображений лица, образцов почерка, описания ДНК и/или других биометрических признаков.

АДИС «ПАПИЛОН» решает задачи:

– Установление личности граждан по отпечаткам и следам пальцев рук и ладоней, в том числе путём проведения оперативных проверок личности по оттиску пальца в режиме реального времени.

[195] Отчет отдела криминалистики СУ СК РФ по Удмуртской Республике 2016 г.

– Идентификация неопознанных трупов.

– Установление причастности лиц к ранее совершённым преступлениям.

– Объединение преступлений, совершённых одним и тем же лицом.

– Широкое применение в криминалистической практике получили автоматизированные информационные поисковые системы генетических данных – *системы геномной регистрации.*

Для постановки на учет дактилоскопической следотеки Следственного комитета Российской Федерации за 2022 год отделом криминалистики СУ СК РФ по УР направлено 1117 электронных копий следов рук по 1156 уголовным делам, находившимся в производстве следователей следственного управления Удмуртии[196].

Системы геномной регистрации (системы ДНК-регистрации, генетические учеты) являются новым видом криминалистических учетов. Порядок работы таких систем в разных странах имеет особенности, определяемые правилами внесения и хранения генетической информации в базе данных, а также образцов ДНК – в банке ДНК; требованиями к соблюдению конфиденциальности; порядком исключения информации из базы данных и др.[197].

В России постановка ДНК-профилей на криминалистический учет проводится относительно недавно. В соответствии с приказом МВД РФ от 10.02.2006 № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел РФ» учет ДНК-профилей биологических объектов определен для нахождения лиц, оставивших биологические следы на месте происшествия; фактов принадлежности биологических следов, изъятых по нескольким преступлениям, одному и тому же неустановленному лицу, а также для установления личности неопознанных трупов.

Контингенты лиц, подлежащих генетической регистрации, также определяются законодательством конкретной страны. Все они включают лиц, осужденных за определенные виды преступлений, а в некоторых странах – также лиц, которые отбыли наказание, подозреваемых, задержанных. Критерии включения данных контингентов в базу данных обычно определяются видом преступления либо максимальным наказанием за него.

В базу данных могут также помещаться на добровольной основе генотипы потерпевших и иных лиц. Для идентификации неопознанных трупов в базу данных вносятся генотипы, полученные при исследовании останков неопознанных лиц, а также лиц, пропавших без вести, и их родственников.

---

[196] Докладная отдела криминалистики СУ СК РФ по Удмуртской Республике Руководителю Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации по итогам работы за 2022 год.

[197] Организация и тактика раскрытия отдельных видов преступлений : учебное пособие / *М.К. Каминский, А.М. Каминский, Н.В. Матушкина* [и др.]. 2-е изд. С. 67.

1 января 2009 года вступил в действие Федеральный закон «О государственной геномной регистрации в Российской Федерации», который ввел два вида государственной геномной регистрации: добровольная и обязательная. Обязательной государственной геномной регистрации подлежат:

1) лица, осужденные и отбывающие наказание в виде лишения свободы за совершение преступлений;

2) неустановленные лица, биологический материал которых изъят в ходе производства следственных действий;

3) лица, подозреваемые в совершении преступлений, обвиняемые в совершении преступлений;

4) близкие родственники лица, пропавшего без вести.

Целью геномной регистрации является идентификация личности. Для этого действующая генетическая регистрационная система состоит их двух баз данных. В одной базе содержатся генотипы лиц, подлежащих криминалистическому учету, во второй – генетические профили, изъятые с мест происшествий. При получении генетического профиля производится сопоставление с генотипами, содержащимися в той и другой базе. При совпадении генотипа с данными, содержащимися в первой базе, устанавливается его принадлежность конкретному лицу, что говорит о его возможной причастности к преступлению. При совпадении с генотипным профилем, содержащимся во второй базе, можно говорить о возможности совершения преступлений одним лицом и связанности этих преступлений между собой.

Характерным примером раскрытия преступлений «прошлых лет» с использованием геномной регистрации может служить опыт работы по делу, возбужденному по факту совершения изнасилования, насильственных действий сексуального характера и разбойного нападения на С-ву и по факту совершения изнасилования, насильственных действий сексуального характера в отношении В-й.

Следствием установлено, что в 2008 году преступник в ночное время на территории г. Сарапула неоднократно, угрожая убийством, с применением ножа нападал на женщин с целью совершения в отношении них изнасилований и насильственных действий сексуального характера, а также хищения имущества. С учетом того, что нападения носили внезапный характер, и в 2008 году отсутствовали современные экспертные методы, установить виновное лицо длительное время не представлялось возможным.

Следователи-криминалисты отдела криминалистики СУ СК РФ по УР, проанализировав аналогичные деяния, совершенные в период с 2008 года по настоящее время, решили провести повторные проверки с использованием генетических учетов ЭКЦ МВД по УР на причастность к совершению преступлений лиц, склонных к подобным действиям. В результате этого в следах, обнаруженных на местах происшествия, установлено наличие генотипа гр-на С., судимого за аналогичные преступления.

Проведенным комплексом следственных действий причастность обвиняемого С. к совершению преступлений доказана в полном объеме. Под тяжестью неопровержимых доказательств он признал вину, дал показания по обстоятельствам совершенных преступлений[198].

При несовпадении профиля ДНК с данными той и другой базы вновь полученный генетический профиль остается на хранение во второй базе.

Учет ведется в виде картотеки, развиваемой из информационных карт установленного образца, а также электронной базы данных.

В России была разработана специально для целей розыска система «КРИМНЕТ», т.е. интеллектуальная система автоматизированного поиска по признакам внешности человека. Она реализована на основе новой методики криминалистического описания внешности человека, искусственных нейронных сетей (искусственного интеллекта) и интернет-технологии и предназначена для криминалистической регистрации по признакам внешности подучетных лиц и автоматизированного поиска.

Информационная система предназначена для автоматизированной идентификации внешнего облика человека по различным видам изображений (фотографии, фотороботы и т.п.), когда речь идет о больших базах данных, содержащих несколько тысяч или сотен тысяч изображений прототипов. Система «КРИМНЕТ» значительно ускоряет процедуру поиска подозреваемого в совершении преступления и идентификации личности по словесным описаниям, субъективным портретам и фотографиям. Система обладает очень высокой производительностью на обычных персональных компьютерах.

В новой методике использован оригинальный подход, учитывающий психологию восприятия внешности человека человеком, а также решения задач поиска лица среди множества других. Это связано с тем, что мысленный образ является базовым отображением внешности в оперативно-разыскной работе, лимитирующий по сравнению с другими отображениями: описания с натуры, фото-, видео-, электронные – степень полноты и качества передачи информации о признаках. В соответствии с особенностями психических процессов, происходящих в мозгу человека, мысленный образ формируется в соответствии с общими закономерностями восприятия признаков внешности человека: фрагментарно, обобщенно, имеет неустойчивость и сильно зависит от влияния субъективных и объективных факторов. Вот поэтому была разработана такая структура системы признаков внешности, которая не только полно учитывает свойства мысленного образа, но и максимально способствует получение информации.

---

[198] Докладная отдела криминалистики СУ СК РФ по Удмуртской Республике от 15.01.2023.

В целях повышения эффективности раскрытия и расследования преступлений с использованием криминалистических учетов приказом МВД по УР от 14 февраля 2008 года № 100 «Об использовании габитоскопических учетов, на базе системы «КРИМНЕТ» была организована криминалистическая регистрация подучетных лиц по признакам внешности человека, накопление полученных данных и их использование при поиске в базе данных интеллектуальной системы автоматизированного поиска по признакам внешности человека в системе «КРИМНЕТ».

В системе КРИМНЕТ имеется возможность регистрировать внешность и производить перекрестный поиск следующих категорий лиц:

- лицо (представляющее оперативный интерес);
- лицо, без вести пропавшее;
- неопознанный труп;
- лицо, находящееся в розыске (федеральном, местном);
- неустановленный преступник (фотороботы);
- неизвестный больной, ребенок;
- неизвестное лицо (очевидец, потерпевший).

Основные достоинства данной методики заключаются в том, что она позволяет описывать внешность и производить автоматизированный поиск по фотографиям, фотороботам среди всех категорий живых лиц, неизвестных трупов, стоящих на учетах в ОВД. Простая, легко запоминается, может применяться сыщиками, розыскниками, специалистами по изготовлению субъективных портретов, а также не требует специального образования от оператора по вводу информации.

В настоящее время в России введена общероссийская комплексная система информирования и оповещения населения в местах массового пребывания людей (ОКСИОН), представляющая собой организационно-техническую систему, объединяющую аппаратно-программные средства обработки, передачи и отображения аудио- и видеоинформации в целях подготовки населения в области гражданской обороны, защиты от чрезвычайных ситуаций, обеспечения пожарной безопасности, безопасности на водных объектах и охраны общественного порядка, своевременного оповещения и оперативного информирования граждан о ЧС и угрозе террористических акций, мониторинга обстановки и состояния правопорядка в местах массового пребывания людей на основе использования современных технических средств и технологий.

В случае введения на какой-либо из территорий – в зоне ответственности ОКСИОН – режима повышенной готовности или режима чрезвычайной ситуации, информационные центры ОКСИОН соответствующего уровня

переходят в оперативное управление территориального органа МЧС России по вопросу вывода оперативных информационных материалов на территориях, на которых введен данный режим.

Технические средства информирования и оповещения населения, при установке в местах массового пребывания людей, функционально объединяются со средствами видеонаблюдения, образуя различные типы терминальных комплексов.

Терминальный комплекс представляет собой автоматизированную систему, содержащую выделенный сервер, управляющий работой точек трансляции, а именно:

- видеокамер;
- датчиков уровня радиации и химического контроля;
- светодиодных экранов;
- плазменных экранов;
- бегущих строк;
- аудиосистем оповещения.

Для использования возможностей системы «ОКСИОН» отделом криминалистики СУ СК РФ по УР в 2022 году было размещено 8 сообщений о безвестном исчезновении несовершеннолетних, которые впоследствии были найдены[199].

Успешность раскрытия и расследования преступлений во многом зависит от степени обеспечения правоохранительных органов накопленной и систематизированной криминалистически значимой информацией о преступлениях, совершенных в прошлом, причастных к ним лицах, средствах и способах их совершения, различных следах преступлений и объектах, связанных с криминальными событиями, а также от возможности и умения следователя пользоваться подобной информацией в своей деятельности.

Совершенствование информационного обеспечения оперативных подразделений становится одним из главных направлений повышения эффективности правоохранительной деятельности.

[199] Докладная отдела криминалистики СУ СК РФ по Удмуртской Республике Руководителю Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации по итогам работы за 2022 год.

АВТОРСКИЙ КОЛЛЕКТИВ

Ровнейко Вера Владимировна,
кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии ФГБОУ ВО «Удмуртский государственный университет»

Абашева Флюра Ахунзяновна,
кандидат юридических наук, доцент, доцент кафедры уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

Татьянина Лариса Геннадьевна,
доктор юридических наук, профессор, заведующая кафедрой уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

Решетнева Татьяна Васильевна,
кандидат юридических наук, доцент, заведующая кафедрой теории и истории государства и права ФГБОУ ВО «Удмуртский государственный университет»

Решетникова Гульнара Аликовна,
кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии ФГБОУ ВО «Удмуртский государственный университет»

Татьянин Дмитрий Владимирович,
кандидат юридических наук, доцент, доцент кафедры уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

Тенсина Елена Фанавиевна,
кандидат юридических наук, доцент, доцент кафедры уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

Хуснутдинов Рашид Марсович,
старший преподаватель кафедры уголовного права и процесса Ижевского института (филиал) Всероссийского государственного университета юстиции (РПА Минюста России)

Шамсеева Алина Маратовна,
ассистент кафедры уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

Каминский Александр Маратович,
доктор юридических наук, профессор, профессор кафедры уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

Хомяков Эдуард Геннадьевич,
кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

Соболев Сергей Владимирович,
старший преподаватель кафедры уголовного процесса и криминалистики ФГБОУ ВО «Удмуртский государственный университет»

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе : монография. – М. : Юрлитинформ, 2012. – 89 с.

2. Аксаментова О.П. О понятии информации в уголовном судопроизводстве // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 1. – С. 27–34.

3. Анисимова А.С., Спиридонова М.П. К вопросу о возможностях использования технологий искусственного интеллекта в правосудии // Юридический вестник ДГУ. – 2021. – Т. 39, № 3. – С. 161–165.

4. Балакшин В.С. Доказательства в российском уголовном процессе: понятие, сущность, классификация : монография. – Екатеринбург : УрГЮА, 2002. – 278 с.

5. Балашова А.А., Жмурова А.И. К вопросу об электронных доказательствах в уголовном процессе России // Глава 2. Цифровизация как основа конвергенции частного и публичного права // Частноправовые и публично-правовые проблемы современной юриспруденции : коллективная монография / отв. ред. С.Ю. Морозов, О.А. Зайцев. – М. : Проспект, 2022. – С. 96–99.

6. Бахтеев Д.В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений» : дисс. … д-ра юрид. наук. Уральский государственный юридический университет имени В.Ф. Яковлева. – Екатеринбург, 2022. – 504 с.

7. Белкин Р.С. Курс криминалистики : в 3 т. Т. 1: Общая теория криминалистики. – М. : Юристь, 1997. – 408 с.

8. Бессонов А.А. Географическое профилирование как метод установления серийных преступников: фантом или реальность? // Эксперт-криминалист. – Москва, 2021. – № 4. – С. 3–6.

9. Бессонов А.А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности : сборник научных трудов Межведомственной научно-практической конференции, Москва, 16 сентября 2022 года. Москва : Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. С. 40–45.

10. Бирюков П.Н. Искусственный интеллект и «предсказанное правосудие: зарубежный опыт // Lexrussica. – 2019. – № 11 (156). – С. 79–87.

11. Бутусова Л.И. К вопросу о киберпреступности в международном праве // Вестник экономической безопасности. – 2016. – № 2. – С. 48–52.

12. Вехов В.Б. Преступления в сфере цифровой экономики: совершенствование расследования на основе положений электронной криминалистики // Пермский юридический альманах. Ежегодный научный журнал. – 2019.

13. Волчецкая Т.С. Современная криминалистическая наука: реалии и перспективы развития // Казанские уголовно-процессуальные и криминалистические чтения : в 2 ч. Ч. 1 : материалы Междунар. науч.-практ. конф., Казань, 28 апр. 2022 г. – Казань : ЮрЭксПрактик, 2022.

14. Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex Russica. – 2019. – № 7 (152). – С. 74–84. – URL: https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-v-upk-byt-ili-ne-byt (дата обращения: 22.10.2024).

15. Габеев С.В. Проблемы реализации уголовной политики в отношении преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – Москва : Издательство Проспект, 2023. – 272 с. – С. 28–38.

16. Гамбарова Е.А. Социальные сети как источник цифровых доказательств // Криминалистическое обеспечение расследования преступлений: проблемы, перспективы и инновации : материалы Междунар. науч.-практ. конф. – Минск : БГУ, 2017. – С. 187–189.

17. Глимейда В.В. Применение технических средств и цифровых технологий при производстве следственных действий : дисс. ... канд. юрид. наук. – Краснодар, 2024. – 241 с.

18. Говердовская Т.В., Крайнюкова Л.М. Анализ правовых механизмов противодействия мошенничеству в сфере электронной торговли: европейский и российский опыт // Правопорядок: история, теория, практика. – 2021. – № 3 (30). С. 134. – URL: https://cyberleninka.ru/article/n/analiz-pravovyh-mehanizmov-protivodeystviya-moshennichestvu-v-sfere-elektronnoy-torgovli-evropeyskiy-i-rossiyskiy-opyt (дата обращения: 04.11.2024).

19. Головин А.Ю. К вопросу собирания криминалистически значимой информации по открытым цифровым данным // Актуальные проблемы криминалистики и судебной экспертизы : сборник материалов Международной научно-практической конференции, Иркутск, 16–17 марта 2023 года. – Иркутск : Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2023. – С. 29–32.

20. Григорьев В.Н., Максимов О.А. Некоторые вопросы использования электронных носителей информации при расследовании уголовных дел // Полицейская деятельность. – 2018. – № 1. – С. 1–8.

21. Григорьев О.Г. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства : дисс. … канд. юрид. наук. – Тюмень, 2003. – 221 с.

22. Денисов Е.А. Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Скиф. – 2017. – № 15. – С. 35–39. – URL: https://cyberleninka.ru/article/n/skrinshoty-v-sisteme-ugolovno-protsessualnyh-dokazatelstv-voprosy-teorii-i-praktiki (дата обращения: 07.10.2024).

23. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие : в 2 ч. Ч. 1 / под ред. А.В. Аносова. – М. : Академия управления МВД России, 2019. – 208 с.

24. Дубко М.А. О понятии компьютерного преступления // Центр исследования компьютерной преступности : [Электронный ресурс]. – URL: http://www.crime-research.ru/analitics/computercrime06

25. Ефремова О.М. Реализация полномочий следователя, направленных на получение и использование компьютерной информации при производстве следственных действий : дисс. ... канд. юрид. наук. – Орел, 2021. – 225 с.

26. Зазулин А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу : автореф. дисс. ... канд. юрид. наук. – Екатеринбург, 2018.

27. Закиров Р.Ф. Цит. по: Макутчев А.В. Современные возможности и пределы внедрения искусственного интеллекта в систему правосудия // Актуальные проблемы российского права. – 2022. – Т. 17, № 8 (141). – С. 47–58.

28. Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России : дисс. … канд. юрид. наук. – Челябинск, 2010. – 234 с.

29. Иванов В.В., Цой В.А. Понятие, виды и правила применения технических средств в уголовном процессе // Технологи в инфосфере. – 2021. – № 2 (4). – С. 109–124.

30. Ионова О.А., Калитин С.В. Понятие доказательств, имеющих электронную форму и цифровое содержание: проблемы и перспективы // Вестник Хабаровской государственной академии экономики и права. – 2013. – № 1. – С. 49–61.

31. Каминский А.М. О системе следов преступной деятельности в сфере компьютерной информации // Казанские уголовно-процессуальные и криминалистические чтения : в 2 ч. : материалы Междунар. науч.-практ. конф., Казань, 22 апр. 2022 г.

32. Каминский А.М., Овчинникова Д.А. Использование электронных криминалистически неупорядоченных банков данных в раскрытии преступлений // Вестник Удмуртского университета. Серия «Экономика и право». – 2020. – Т. 30, № 1. – С. 91–98.

33. Каминский А.М., Русских Ж.А. Некоторые аспекты использования компьютерного сленга для решения задач расследования преступлений в сфере

компьютерной информации // Пермский юридический альманах. – 2019. – № 2. – С. 665–672.

34. Карташов И.И., Лесников О.А. Цифровая информация в уголовно-процессуальном доказывании: понятие и свойства // Электронный научный журнал «Наука. Общество. Государство». – 2020. – Т. 8, № 4. – С. 73–82. – URL: http://esj.pnzgu.ru/

35. Катрин Е.В. Цифровизация: научные подходы к определению термина // Вестник Забайкальского государственного университета. – 2022. – Т. 28, № 5. – С. 49–54.

36. Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий (ГАС «Доступ к правосудию») : монография / отв. ред. Л.Н. Масленникова. – М. : Норма, Инфра-М, 2022.

37. Краснова Л.Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Экономические и юридические науки. – 2013. – № 4-2. – С. 254–260.

38. Криминалистика : учебник / П.Н. Аленичев, Р.С. Белкин, Е.М. Лившиц, И.М. Лузгин [и др.] ; под ред. Р.С. Белкина. – М. : Юрид. лит., 1974. – 672 с.

39. Криминалистика. Т. 1. История, общая и частные теории / под ред. Р.С. Белкина, В.Г. Коломацкого, И.М. Лузгина. – М., 1995. – 280 с.

40. Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде : дисс. ... канд. юрид. наук. – Нижний Новгород, 2016. – 273 с.

41. Липинский А.П. Обеспечение недопустимости разглашения данных досудебного производства : автореф. дисс. … канд. юрид. наук. – Ижевск, 2023. – 32 с.

42. Лобач Д.В. Развитие российского уголовного законодательства в сфере противодействия преступлениям, совершаемым в сети «Интернет» // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – Москва : Издательство «Проспект», 2023. – 272 с. – С. 21–27.

43. Луценко Е.П. Применение искусственного интеллекта при осуществлении правосудия в России и за рубежом // Образование и право. – 2022. – № 6. – С. 220–222.

44. Макутчев А.В. Современные возможности и пределы внедрения искусственного интеллекта в систему правосудия // Актуальные проблемы российского права. – 2022. – Т. 17, № 8 (141). – С. 47–58.

45. Маринкин Д.Н., Костарева В.А. Цифровые доказательства в уголовном судопроизводстве // Вестник Пермского института ФСИН России. – 2019. – № 1(32). – С. 33–36.

46. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дисс. … д-ра. юрид. наук. – Воронеж, 2001. – 39 с.

47. Миролюбова С.Ю. Перспективы использования искусственного интеллекта в правосудии и вопросы правового регулирования в Российской Федерации // Конституционное правосудие. – 2019. – № 5. – URL: https://zakon.ru/publication/perspektivy_ispolzovaniya_iskusstvennogo_intellekta_v_pravosudii_perspektivy_pravovogo_regulirovani

48. Молчанов Н.Н. Дипломатия Петра Великого. – М., 1991. – 446 с.

49. Момотов В.В. Доклад на пленарном заседании участников Глобальной сети обеспечения честности и неподкупности судебных органов (GlobalJudicialIntegrityNetwork) под эгидой Управления ООН по наркотикам и преступности на тему: «Перспективы использования искусственного интеллекта в судебной системе Российской Федерации» ; Катар, 26 февраля 2020 г. – URL: http://www.ssrf.ru/news/lienta-novostiei/36912

50. Момотов В.В. Искусственный интеллект в судопроизводстве: состояние, перспективы использования // Вестник университета имени О.Е. Кутафина (МГЮА). – 2021. – № 5. – С. 188–191.

51. Новикова К.С. Искусственный интеллект как элемент электронного правосудия: смарт – решение и электронные весы правосудия // Образование и право. – 2020. – № 3. – С. 240–244.

52. Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации : дисс. … канд. юрид. наук. – М., 2016. – 158 с.

53. Организация и тактика раскрытия отдельных видов преступлений : учебное пособие / М.К. Каминский, А.М. Каминский, Н.В. Матушкина [и др.]. – 2-е изд., испр. и доп. – Ижевск : Jus est, 2017. – 402 с.

54. Основы теории электронных доказательств : монография / под ред. д-ра юрид. наук С.В. Зуева. – М. : Юрлитинформ, 2019.

55. Пастухов П.С. Электронное вещественное доказательство в уголовном судопроизводстве // Вестник Томского государственного университета. – 2015. – № 396. – С. 149–153.

56. Пережогина Г.В. Проблемы определения понятия «преступления, совершаемые с использованием информационных технологий» в современных условиях // Уголовное право: стратегия развития в XXI веке : материалы XVIII Международной научно-практической конференции. – Москва : РГ-Пресс, 2021. – С. 97–103.

57. Рассейкин Д.П. Очерки истории уголовной регистрации. – Саратов, 1976. – 60 с.

58. Рахманова Е.Н., Пономарева Е.В. Киберпреступность, цифровая преступность и кибербезопасность: проблемы определения и взаимосвязи // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – Москва : Издательство «Проспект», 2023. – 272 с. – С. 202–209.

59. Репецкая А.Л. Российская организованная преступность: характеристика современного развития // Вестник Восточно-Сибирского института МВД России. – 2015. – № 4.

60. Решетникова Г.А. Факторы, препятствующие оправлению правосудия системой искусственного интеллекта // Процессуальные гарантии современного правосудия: к 100-летию Судебной системы в Удмуртской Республике : сб. ст. – Ижевск : Удмуртский университет, 2023. – С. 249 – 257.

61. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия ТулГУ. Экономические и юридические науки. Вып. 3, ч. 2: Юридические науки. – Тула : Изд-во Тульского гос. ун-та, 2016.

62. Россинская Е.Р. Проблемы исследования цифровых следов в судебной экспертизе // Цифровой след как объект судебной экспертизы : материалы Междунар. науч.-практ. конф. – М., 17 января 2020 г.

63. Рудых А.А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : автореф. дисс. … канд. юрид. наук. – Ростов-на-Дону, 2020. – 25 с.

64. Рыбин А.В. Электронный документ как вещественное доказательство по делам о преступлениях в сфере компьютерной информации: процессуальные и криминалистические аспекты : дисс. ... канд. юрид. наук. – Краснодар, 2005. – 192 с.

65. Семушкин А.Б. Экосистема предварительного расследования // Актуальные проблемы российского права. – 2023. – № 7. – С. 143–158.

66. Советский энциклопедический словарь / науч.-ред. совет: А.М. Прохоров (пред.), М.С. Гиляров, Е.М. Жуков, Н.Н. Иноземцев, И.Л. Кнунянц, П.Н. Федосеев, М.Б. Храпченко. – М. : Изд-во «Советская Энциклопедия», 1981. – 1600 с.

67. Степанов О.А., Басангов Д.А. О перспективах влияния искусственного интеллекта на судопроизводство // Вестник Томского государственного университета. – 2022. – № 475. – С. 229 – 237.

68. Строгович М.С. Курс советского уголовного процесса. Т. 1. Основные положения науки советского уголовного процесса. – М. : Издательство «Наука», 1968. – 468 с.

69. Таболина К.А., Таболин В.П. Надзор прокурора в уголовном судопроизводстве в условиях развития цифровых отношений // Актуальные проблемы российского права. – 2023. – № 4. – С. 115–123.

70. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дисс. … канд. юрид. наук. – Владивосток, 2005. – 26 с. : [Электронный ресурс]. – URL: https://www.dissercat.com/content/kiberprestupnost-ponyatie-sostoyanie-ugolovno-pravovye-mery-borby

71. Урсул А.Д. Природа информации : философский очерк. – 2-е изд. – Челябинск : Челяб. гос. акад. культуры и искусств, 2010. – 231 с.

72. Федюкина А.Ю. О месте электронных носителей информации в системе доказательств по уголовным делам // Вестник Московского университета МВД России. – 2020. – № 3. – С. 81–83.

73. Цепелев В.Ф. Перспективы адекватного уголовно-правового реагирования на новые виды преступлений, совершаемых с использованием электронных информационно-телекоммуникационных и иных цифровых технологий // Уголовное право: стратегия развития в XXI веке : материалы XVIII Международной научно-практической конференции. – Москва : РГ-Пресс, 2021. – С. 103–106.

74. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. – 2012. – № 2.

75. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и криминологическая квалификация киберпреступлений // Право и кибербезопасность. – 2012.

76. Черкасов В.С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса : дисс. ... канд. юрид. наук. – Хабаровск, 2022. – 210 с.

77. Чистилина Д.О. Использование возможностей искусственного интеллекта в уголовном процессе // Вестник Удмуртского университета. Серия «Экономика и право». – 2021. – Т. 31, вып. 4. – С. 705–710.

78. Шаповалова Г.М. Возможность использования информационных следов в криминалистике (вопросы теории и практики) : автореф. дисс. …канд. юрид. наук. – Владивосток., 2006. – 24 с.

79. Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования : монография. – 2-е изд., испр. и доп. – М. : Норма : ИНФРА-М, 2024. – 240 с.

80. Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение : монография. – Самара, 2008. – 168 с.

81. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом // Информатизация и информационная безопасность правоохранительных органов : материалы XI Межд. конф. – М., 2002. – С. 17, 57.

82. Ponce del Castillo, Aida, A Law on Robotics and Artificial Intelligence in the EU? (October 3, 2017). ETUI Research Paper – Foresight Brief #02-September 2017, Available at SSRN: https://ssrn.com/abstract=3180004 or http://dx.doi.org/10.2139/ssrn.3180004

83. Legg, Michael and Bell, Felicity, Artificial Intelligence and the Legal Profession: Becoming The AI-Enhanced Lawyer (2019). University of Tasmania Law Review, 38(2), 34-59 (2019), UNSW Law Research Paper No. 20-63, Available at SSRN: https://ssrn.com/abstract=3725949

84. Leenes, Ronald E. and Leenes, Ronald E. and Lucivero, Federica, Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design (November 28, 2014). Law, Innovation and Technology (2014) 6(2) LIT 194–222, Available at SSRN: https://ssrn.com/abstract=2546759

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ 2
Ровнейко В.В. Понятие и виды преступлений в сфере информационных технологий 4
Абашева Ф.А. К вопросу об определении понятия «определяемое физическое лицо» и гарантии его прав 20
Татьянина Л.Г., Решетнева Т.В., Решетникова Г.А. Принципы правосудия как правовые барьеры ограничения деятельности систем искусственного интеллекта 32
Татьянин Д.В. Обеспечение информационной безопасности по уголовному делу в досудебном производстве 48
Тенсина Е.Ф. Уголовно-процессуальное регулирование цифровизации досудебного производства по уголовному делу 53
Хуснутдинов Р.М. Использование в доказывании электронной информации о бездокументарных ценных бумагах 59
Шамсеева А.М. О возможности введения нового «электронного доказательства» в УПК РФ 65
Каминский А.М. О некоторых тенденциях и перспективах развития криминалистических исследований в области IT-технологий 71
Хомяков Э.Г. Применение современных технологий при расследовании дистанционных мошенничеств в интернет-магазинах (на маркетплейсах) 85
Соболев С.В. Информационные системы для обеспечения деятельности правоохранительных органов по борьбе с преступностью 98
БИБЛИОГРАФИЧЕСКИЙ СПИСОК 112
СОДЕРЖАНИЕ 120

ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ ИЗДАНИЯ:

Интерфейс электронного издания (в формате pdf) можно условно разделить на 2 части.

Левая навигационная часть (закладки) включает в себя содержание книги с возможностью перехода к тексту соответствующей главы по левому щелчку компьютерной мыши.

Центральная часть отображает содержание текущего раздела. В тексте могут использоваться ссылки, позволяющие более подробно раскрыть содержание некоторых понятий.

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ:

Минимальные системные требования: Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше; 8x CDROM; разрешение экрана 1024×768 или выше; программа для просмотра pdf.

СВЕДЕНИЯ О ЛИЦАХ, ОСУЩЕСТВЛЯВШИХ ТЕХНИЧЕСКУЮ ОБРАБОТКУ И ПОДГОТОВКУ МАТЕРИАЛОВ:

Оформление электронного издания : Издательский центр «Удмуртский университет».

Редактор: И.А. Бусоргина

Подписано к использованию 13.12.2024
Объем электронного издания 1,4 Мб
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru