ТАДЖИКСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ

На правах рукописи

УДК: 343.9 (575.3)

ББК: 67.99(2) 8 (2 тадж.)

С – 16

САЛИМОВ БАХРОМДЖОН АЗИЗОВИЧ

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ОБНАРУЖЕНИЯ И ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ

ДИССЕРТАЦИЯ

на соискание ученой степени кандидата юридических наук по специальности: 12.00.12 – Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность

НАУЧНЫЙ РУКОВОДИТЕЛЬ:

доктор юридических наук, профессор

НАЗАРОВ А.К.

Душанбе – 2024

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И (ИЛИ) УСЛОВНЫХ ОБОЗНАЧЕНИЙ

г. – год

гг. – годы

ГКНБ – Государственный комитет национальной безопасности

др. – другие

и т.д. – и так далее

и т.п. – и тому подобное

МВД – Министерство внутренних дел

ОЗУ – Оперативное запоминающее устройство

ООН – Организация Объединенных Наций

п. – пункт

п.п. – пункты

ПЗУ – Постоянное запоминающее устройство

ПК – Персональный компьютер

ПО – Программное обеспечение

РТ – Республика Таджикистан

са – Канада

СКТЭ – Судебная компьютерно-техническая экспертиза

СНГ – Содружество Независимых Государств

ст. – статья

США – Соединённые Штаты Америки

т.е. – то есть

т.к. – так как

УК – Уголовный кодекс

УПК – Уголовно-процессуальный кодекс

ч. – часть

ШОС – Шанхайская организация сотрудничества

ЭВМ – Электронно-вычислительная машина

CD-R – диски для разовой записи, хранения и считывания информации

CD-ROM – диски, предназначенные для хранения и считывания предварительно записанной на него цифровой информации

CD-RW – диски для записи, перезаписи и хранения сведений

DNS – Domain Name System (Доменная Система Имен)

DVD – диски для хранения видеоизображений и больших объёмов разных видов цифровой информации - текст, звук, изображение

E-mail – Электронная почта

EMS – Enhanced Messaging Service (улучшенная служба сообщений)

Fr – Франция

FTP – File Transfer Protocol (протокол передачи файлов); Служба передачи файлов

HTTP – Hyper Text Transfer Protocol (протокол передачи гипертекста)

ID – Персональный идентификатор страницы

IP – Internet Protocol (адресный протокол)

IRC – Internet Relay Chat (служба непосредственного общения нескольких пользователей в режиме реального времени)

IT – Информационные технологии

MMS – Multimedia Messaging Service (система передачи мультимедийных сообщений (изображений, мелодий, видео)

POP – Post Office Protocol (протокол обработки входящей почты)

ru – Россия

SMS – Short Message Service (служба коротких сообщений)

SMTP – Simple Mail Transfer Protocol (протокол подтверждения о приёме, либо об ошибке, либо запроса дополнительных сведений)

TCP – Transmission Control Protocol (протокол транспортного назначения)

Tj – Таджикистан

us – США

WWW (Web) – World Wide Web (Всемирная паутина)

ВВЕДЕНИЕ

Актуальность темы исследования. Стремительное технологическое развитие общества внесло определённые коррективы в жизнь современного человека. Особенно информационные технологии, динамично развивающиеся в последние десятилетия, проникли в различные сферы жизнедеятельности общества и активно применяются в таких областях, как связь, финансы, торговля, промышленность, транспорт, медицина, управление жизнеобеспечением городов, населённых пунктов, критически важных и иных объектов. Самым важным достижением человечества в данном направлении является создание глобальной сети Интернет.

Согласно отчёту Digital 2023, выполненному организациями We Are Social и Hootsuite, количество интернет-пользователей по всему миру на начало 2023 года составило 5,15 млрд человек. Это 64,4% от общей численности населения планеты. Социальными сетями же пользуются 4,76 млрд человек или 60% от населения. Пользователей мобильных телефонов больше – 5,44 млрд или 68%[1].

Интернет превратился в глобальный источник хранения и распространения информации, в том числе, и криминалистически значимой. Безопасная, стабильная и доступная электронно-цифровая среда необходима всему обществу и требует от правоохранительных и других надзорных органов эффективной работы в целях снижения рисков её использования в преступной деятельности.

Несмотря на высокую эффективность и необходимость внедрения новых информационных технологий во все сферы жизнедеятельности общества, нельзя забывать, что они также выступают в качестве источника угроз общественной безопасности.

Анализ состояния преступности в Республике Таджикистан показывает, что с каждым годом увеличивается количество преступлений, совершаемых с использованием информационных технологий. Помимо преступлений против

[1] См.: Интернет и соцсети в начале 2023 года – главные цифры Global Digital 2023 [Электронный ресурс]. – Режим доступа: URL: https://vc.ru/marketing/596126-internet-i-socseti-v-nachale-2023-goda-glavnye-cifry-global-digital-2023 (дата обращения: 20.08.2023).

информационной безопасности, эти технологии применяются при планировании и совершении других общественно-опасных правонарушений, объектами которых являются иные правоотношения уголовно-правовой охраны. Происходит так называемая компьютеризация классических преступлений[2] (распространение экстремистских материалов, хищение, кража, незаконный оборот наркотиков и пр.), в механизме совершения которых важную роль играют компьютерные технологии.

Особую тревогу вызывает тот факт, что в последние годы террористические и экстремистские организации все чаще используют информационные технологии для распространения радикальной пропаганды, рассылки запрещённых материалов, сбора денежных средств, привлечения новых членов, обучения и подстрекательства других лиц к совершению актов терроризма и экстремизма. По этому поводу Основатель мира и национального единства - Лидер нации, Президент Республики Таджикистан уважаемый Эмомали Рахмон в своём Послании Маджлиси Оли Республики Таджикистан, выражая обеспокоенность, отметил, что «сегодня террористические и экстремистские группировки для привлечения и вербовки граждан в свои ряды используют современные информационные технологии, направляют малоопытных и заблудших молодых людей на путь радикализма»[3].

Генеральная Ассамблея Организации Объединенных Наций (ООН) отметила возрастающую степень использования информационно-коммуникационных технологий террористами и их сторонниками[4]. Принимая во внимание важность цифровых доказательств при расследовании преступлений террористического характера, Совет Безопасности ООН в своих резолюциях (2322 (2016 г.)[5], 2331

---

[2] См.: Голик Ю.В. Меняется мир – меняется преступность / Ю.В. Голик // Криминология: вчера, сегодня, завтра. – 2015. – №3 (38). – С. 35.

[3] Послание Президента Республики Таджикистан, уважаемого Эмомали Рахмона «Об основных направлениях внутренней и внешней политики республики» (г. Душанбе, 23.12.2022, 28.12.2023) [Электронный ресурс]. – Режим доступа: https://president.tj (дата обращения: 04.02.2023, 30.12.2023).

[4] См.: Обзор Глобальной контртеррористической стратегии ООН (A/RES/70/291), пункт 42, 19 июля 2016 [Электронный ресурс]. – Режим доступа: https://www.isdglobal.org/wp-content/uploads/2019/12/Policy-Toolkit-on-Z-L-Recommendations-RUS.pdf (дата обращения: 09.03.2023).

[5] См.: Резолюция Совета Безопасности ООН 2322 (2016). Угрозы международному миру и безопасности, создаваемые террористическими актами [Электронный ресурс]. – Режим доступа: URL: https://capve.org/components/com_jshopping/files/demo_products/2322.pdf (дата обращения: 04.07.2023).

(2016 г.)[6], 2341 (2017 г.)[7] и 2396 (2017 г.)[8]) призвал государства собирать и сохранять доказательства, чтобы обеспечить возможность проведения расследований и судебного преследования для привлечения к ответу лиц, ответственных за террористические атаки. В резолюции 2322 (2016 г.) отмечается значительный рост запросов о сотрудничестве в части сбора доказательств в форме цифровых данных из Интернета.

Нередко сведения, хранящиеся в сети Интернет и других электронных носителях, выступают основанием для возбуждения уголовного дела и в дальнейшем становятся доказательствами по делу. Проведённое анкетирование следователей центрального аппарата и территориальных подразделений ГКНБ Республики Таджикистан показало, что подавляющему большинству опрошенных (92,3%) приходилось в ходе расследования общественно-опасных правонарушений, совершённых с применением информационных технологий, получать доказательства с электронных носителей информации, и всего лишь 7,7% респондентов ответили, что им не доводилось получать электронные доказательства.

Вместе с тем, органы следствия и дознания испытывают трудности в процессе расследования преступлений данной категории. Это обусловлено, прежде всего, особым характером электронно-цифровой информации и сложной технической структурой информационных технологий. Также, недостаточный уровень знаний сотрудников в области компьютерных технологий, постоянное развитие и совершенствование информационно-телекоммуникационных средств, специфичность механизма следообразования электронно-цифровых данных, техническая сложность выявления источников информации и отсутствие процессуальных средств фиксации электронных доказательств, несомненно, приводят к возникновению новых проблем в правоприменительной деятельности.

---

[6] См.: Резолюция Совета Безопасности ООН 2331 (2016) [Электронный ресурс]. – Режим доступа: URL: https://www.hrnk.org/uploads/pdfs/N1640753.pdf (дата обращения: 04.07.2023).

[7] См.: Резолюция Совета Безопасности ООН 2341 (2017) [Электронный ресурс]. – Режим доступа: URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf? OpenElement (дата обращения: 04.07.2023).

[8] См.: Резолюция Совета Безопасности ООН 2396 (2017) [Электронный ресурс]. – Режим доступа: URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/27/PDF/N1746027.pdf? OpenElement (дата обращения: 04.07.2023).

Таким образом, актуальность исследования проблем обнаружения и фиксации доказательственной электронно-цифровой информации в значительной мере определяется указанными обстоятельствами, практической и научной значимостью эффективного расследования преступлений, в механизме совершения которых используются информационные технологии, а также необходимостью проработки научно обоснованных рекомендаций по совершенствованию законодательства и правоприменительной деятельности в данной области.

Степень изученности научной темы: Изучение проблем «обнаружения и фиксации доказательственной электронно-цифровой информации» не было предметом самостоятельного научно-монографического исследования отечественных правоведов. Отдельные аспекты темы исследованы в работах К.Д. Давлатзода[9], Дж.М. Зоира[10], У.А. Меликова[11], А.К. Назарова[12] и Р.Х. Рахимзода[13].

В российских научных кругах вопросам фиксации и использования доказательственной информации, выраженных в цифровой форме, применения электронных носителей информации в уголовном судопроизводстве, производства отдельных следственных действий по преступлениям, совершаемым с использованием информационных технологий, исследования компьютерной информации и средств её обработки посвящены работы В.Ю. Агибалова[14], А.А. Балашовой[15], Д.В. Бахтеева[16], В.В. Борисова[17], А.С. Бутенко[18], В.Ю. Васюкова[19],

[9] См.: Давлатзода К.Д. Угрозы виртуальной среды: практика и теория киберпреступлений: монография. – Душанбе, 2023. – 248 с.; Давлатзода К.Д. Основания расследования киберпреступлений. – Душанбе, 2023. – 150 с.; Давлатзода К.Д. Классификация киберпреступлений / К.Д. Давлатзода // Вестник Таджикского национального университета. – 2022. – №8. – С. 279-284.

[10] См.: Зоиров Дж.М. Оперативно-розыскное мероприятие получение компьютерной информации и права человека / Дж.М. Зоиров // Труды Академии МВД Республики Таджикистан. – 2018. – №1 (37). – С. 26-37.

[11] См.: Меликов У.А. Правовой режим объектов гражданских прав в интернете: монография. – Душанбе, 2017. – 244 с.

[12] См.: Назаров А.К., Салимов Б.А. Криминалистическая тактика осмотра устройства мобильной связи (мобильного телефона) как источника доказательственной информации / А.К. Назаров, Б.А. Салимов // Наука и безопасность. – 2023. – №3 (5). – С. 104-109.

[13] См.: Рахимзода Р.Х. Оперативно-розыскная политика по обеспечению экономической безопасности Республики Таджикистан: проблемы теории, методологии и практики (историко-правовой и общетеоретический анализ): дис. … д-ра юрид. наук. – Душанбе, 2018. – 581 с.

[14] См.: Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: дис. ... канд. юрид. наук. – Воронеж, 2010. – 198 с.

[15] См.: Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. … канд. юрид. наук. – М., 2020. – 214 с.

В.Б. Вехова[20], А.Г. Волеводза[21], С.П. Ворожбит[22], Ю.В. Гаврилина[23], Б.Я. Гаврилова[24], В.Н. Григорьева[25], С.В. Зуева[26], А.Н. Иванова[27], Д.А. Илюшина[28], И.И. Карташева[29], А.Н. Колычевой[30], Л.Б. Красновой[31], Т.Э. Кукарниковой[32], Н.Н. Лыткина[33], В.А. Мещерякова[34], Р.И. Оконенко[35], А.Л. Осипенко[36], М.А. Простосердова[37], Е.Р. Россинской[38], А.Г. Себякина[39], М.В. Старичкова[40] и других.

---

[16] См.: Бахтеев Д.В. Основы теории электронных доказательств: монография / Под ред. д-ра юрид. наук С.В. Зуева. – М, 2019. – 284 с.

[17] См.: Борисов В.В. Об особенностях фиксации информационных следов в практике защиты информации / В.В. Борисов // Известия Южного федерального университета. Технические науки. – 2009. – Т. 94. – №5. – С. 164-168.

[18] См.: Бутенко А.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/ (дата обращения: 25.07.2022).

[19] См.: Васюков В.Ф., Колычева А.Л. Осмотр и фиксация страниц интернет-сайта в сети Интернет / В.Ф. Васюков, А.Л. Колычева // Вестник экономической безопасности. – 2019. – №1. – С. 115-118.

[20] См.: Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. – М., 1996. – 182 с.; Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. – 2016. – №2 (46). – С. 10-19.

[21] См.: Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М., 2001. – 496 с.

[22] См.: Ворожбит С.П. Электронные средства доказывания в гражданском и арбитражном процессе: автореф. дис. … канд. юрид. наук. – Санкт-Петербург, 2011. – 25 с.

[23] См.: Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: автореф. дис. ... д-ра юрид. наук. – М., 2010. – 56 с.

[24] См.: Гаврилов Б.Я. Получение доказательств и информации с электронных носителей: вопросы законодательного регулирования и правоприменения / Уголовное судопроизводство: проблемы теории и практики. – 2018. – Т. 3. – 216 с.

[25] См.: Григорьев В.Н. Понятие электронных носителей информации в уголовном судопроизводстве / В.Н. Григорьев // Вестник Уфимского юридического института МВД России. – 2019. – №2 (84). – С. 33-44.

[26] См.: Зуев С.В. Основы теории электронных доказательств: монография / Под ред. д-ра юрид. наук С.В. Зуева. – М., 2019. – 304 с.

[27] См.: Иванов А.Н. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы / А.Н. Иванов // Известия Саратовского университета. – 2009. – Т. 9. – Вып. 2. – С. 74-77.

[28] См.: Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дис. ... канд. юрид. наук. – Волгоград, 2008. – 233 с.

[29] См.: Карташев И.И. Цифровые доказательства» в уголовном процессе / И.И. Карташев // Центральный научный вестник. – 2016. – №155. – С. 23-25.

[30] См.: Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. … канд. юрид. наук. – М., 2018. – 199 с.

[31] См.: Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. – Воронеж, 2005. – 24 с.

[32] См.: Кукарникова Т.Э. Компьютерная информация как следообразующая система / Т.Э. Кукарникова // Криминалистика в системе правоприменения: материалы конф. (27-28 октября 2008 г.). – М., 2008. – С. 147-150.

[33] См.: Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: дис. ... канд. юрид. наук. – М., 2007. – 201 с.

[34] См.: Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. – Воронеж, 2001. – 39 с.

[35] См.: Оконенко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р.И. Оконенко // Актуальные проблемы российского права. – 2015. – №3. – С. 120-124.

[36] См.: Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. – М., 2004. – 432 с.

[37] См.: Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. – М., 2016. – 232 с.

Вместе с тем, несмотря на значимость научных трудов указанных авторов, вопросы обнаружения и фиксации доказательственной электронно-цифровой информации согласно законодательству Республики Таджикистан и относительно правоприменительной деятельности её компетентных органов не являлись предметом комплексных научных исследований. Также, анализ научных работ показал, что многие вопросы, касающиеся криминалистического исследования намеченной темы, требуют дополнительной научной проработки.

Связь исследования с программами либо научной тематикой. Диссертационная работа выполнена в рамках исследовательского проекта кафедры криминалистики и судебно-экспертной деятельности юридического факультета Таджикского национального университета «Методика расследования преступлений». Тема диссертации является актуальной и соответствует Концепции правовой политики Республики Таджикистан на 2018-2028 гг. от 6 февраля 2018 г.

ОБЩАЯ ХАРАКТЕРИСТИКА ИССЛЕДОВАНИЯ

Цель исследования состоит в комплексном анализе действующего законодательства Республики Таджикистан и международных нормативно-правовых актов, регламентирующих вопросы обнаружения и фиксации доказательственной электронно-цифровой информации, а также, изучении теоретических положений и правоприменительной деятельности компетентных органов республики в данной области и на этой основе разработать научно обоснованные рекомендации, направленные на совершенствование правовых механизмов и тактических приёмов собирания доказательственной информации на локальных и сетевых носителях.

Задачи исследования. Достижению сформулированной цели способствовало решение следующих задач:

---

[38] См.: Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. – М., 2018. – 576 с.

[39] См.: Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. ... канд. юрид. наук. – М., 2021. – 271с.

[40] См.: Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве / М.В. Старичков // Вестник Восточно-Сибирского института МВД России. – 2014. – №1. – С. 16-20.

– определение криминалистического понятия электронно-цифровой информации и её правового положения в системе доказательств по уголовным делам;

– анализ вопросов использования информационных технологий в механизме совершения общественно-опасных деяний;

– исследование сущности, содержания и классификации электронно-цифровых следов;

– научный анализ механизма следообразования доказательственной электронно-цифровой информации на локальных и сетевых носителях;

– выработка научно обоснованных тактических приёмов обнаружения и фиксации электронно-цифровых следов с учётом функционирования электронно-вычислительных средств и сетей;

– исследование особенностей производства отдельных процессуальных действий, направленных на обнаружение и фиксацию электронно-цифровых доказательств;

– раскрытие тактики осмотра электронно-цифровой информации и исследования отдельных объектов, содержащих криминалистически значимую информацию;

– исследование проблем процессуального использования специальных познаний по делам о преступлениях, совершаемых с применением информационных технологий.

Объектом исследования является деятельность, складывающаяся в процессе выявления, фиксации и исследования криминалистически значимой информации на электронных носителях.

Предметом исследования выступают закономерности образования электронно-цифровых следов преступлений, совершаемых с использованием компьютерных и информационно-телекоммуникационных технологий, а также состояние нормативного регулирования процесса доказывания по уголовным делам данной категории.

Этап, место и период исследования (исторические рамки исследования).

Диссертационное исследование включает периоды утверждения и подготовки работы, а также его обсуждения на кафедре криминалистики и судебно-экспертной деятельности юридического факультета Таджикского национального университета. Временной интервал исследования охватывает 2011-2023 годы и местом его реализации является Республика Таджикистан.

Теоретическую основу исследования составили труды учёных в области криминалистики, судебной экспертизы, уголовного права и уголовного процесса В.Ю. Агибалова, А.А. Балашовой, Д.В. Бахтеева, Р.С. Белкина, В.В. Борисова, А.С. Бутенко, В.Ф. Васюкова, В.Б. Вехова, А.Г. Волеводза, С.П. Ворожбит, Ю.В. Гаврилина, Б.Я. Гаврилова, В.Н. Григорьева, С.В. Зуева, А.Н. Иванова, Д.А. Илюшина, И.И. Карташева, А.Л. Колычевой, Л.Б. Красновой, Т.Э. Кукарниковой, Н.Н. Лыткина, В.А. Мещерякова, Р.И. Оконенко, А.Л. Осипенко, М.А. Простосердова, Е.Р. Россинской, А.Г. Себякина, М.В. Старичкова и ряда других. Также, в ходе исследования были использованы работы отечественных правоведов К.Д. Давлатзода, Дж.М. Зоира, У.А. Меликова, А.К. Назарова и Р.Х. Рахимзода, в которых рассмотрены отдельные вопросы фиксации доказательственной информации.

Методологические основы исследования. Для объективного, всестороннего, полного изучения предмета исследования, достижения намеченной цели и решения сформулированных задач автором был использован всеобщий универсальный диалектический метод познания, а также комплекс общенаучных и специальных методов.

С использованием историко-правового метода удалось проследить возникновение и развитие понятия электронно-цифровой информации. Применение формально-логического метода состояло в анализе правовой природы доказательственной информации, хранящейся на локальных и сетевых носителях, с использованием законов мышления человека. Для формирования и обработки эмпирической базы исследования использовался социологический метод, заключающейся в опросе следователей органов национальной безопасности об использовании электронно-цифровой информации в процессе

доказывания и применяемых процессуальных средствах собирания доказательств на электронных носителях. Статистический метод применялся в ходе сбора и анализа сведений о преступлениях, совершаемых с использованием информационных технологий. При разработке и формулировании научно обоснованных предложений по совершенствованию норм уголовного и уголовно-процессуального законодательства использовался метод юридико-технического анализа. Применение системно-функционального и системно-структурного методов позволило исследовать механизм следообразования на электронных носителях, сформулировать тактические приёмы обнаружения и фиксации доказательственной информации.

Эмпирические предпосылки исследования составляют:

– статистическая информация Главного информационно-аналитического центра МВД Республики Таджикистан о преступлениях, совершённых с использованием информационных технологий, за период с 2018 по 2022 год;

– материалы 155 уголовных дел, расследованных следственными подразделениями ГКНБ Республики Таджикистан и в рамках которых осуществлялось собирание доказательственной информации на электронных носителях;

– анкетирование следователей органов национальной безопасности Республики Таджикистан, расследовавших уголовные дела, в рамках которых электронно-цифровая информация использовалась в процессе доказывания;

– информационно-аналитические материалы Антитеррористического центра Содружества Независимых Государств (СНГ) и Региональной антитеррористической структуры Шанхайской организации сотрудничества (ШОС) об использовании террористическими и экстремистскими организациями информационных технологий в преступных целях.

Научная новизна исследования состоит в том, что на монографическом уровне осуществлено комплексное исследование проблем обнаружения, фиксации и использования доказательственной электронно-цифровой информации в правоприменительной деятельности правоохранительных и

судебных органов Республики Таджикистан.

К основным положениям, отвечающим критерии научной новизны, может быть отнесено следующее:

– определение правового положения доказательственной электронно-цифровой информации в системе доказательств по уголовным делам;

– на основе структуры объектов охраны уголовного закона проведена авторская классификация общественно-опасных деяний, совершаемых с использованием информационных технологий, и тем самым определён весь спектр преступлений данной категории;

– формулирование автором определения преступлений, совершаемых с использованием информационных технологий;

– с учётом механизма следообразования и особенностей производства отдельных следственных действий, формирование тактических приёмов обнаружения и фиксации криминалистически значимой информации на электронных носителях;

– разработка научно обоснованных рекомендаций по совершенствованию законодательства, в части определения названия и понятия электронно-цифровой информации, включения её в систему доказательств и создания процессуальных средств собирания доказательств на сетевых носителях.

Положения, выносимые на защиту. Научная новизна исследования состоит также в следующих положениях, подлежащих вынесению на защиту:

I. Предложения теоретического характера:

1) Проанализировав различные научные и законодательные подходы к понятию «компьютерная информация» автор обосновывает концепцию о том, что в связи с развитием информационных технологий необходимо исключить слово «компьютер» из данного определения и взамен использовать термин «электронно-цифровая информация». Так как в современном обществе появилось много технических средств (смартфоны, цифровые фотоаппараты, цифровые диктофоны, смарт-часы и пр.), имеющих функции создания, обработки, хранения и передачи электронно-цифровой информации, но, вместе с тем, не являющиеся

компьютерным устройством.

Диссертант предлагает под термином «электронно-цифровая информация» понимать зафиксированные в устройствах памяти компьютерной или иной микропроцессорной техники данные, предназначенные для записи, хранения и обработки с помощью электронно-вычислительной либо цифровой техники, а также сведения, передаваемые посредством электромагнитных сигналов по каналам связи.

2) На основе исследования существующих в криминалистике взглядов и положений законодательства страны и международных нормативно-правовых актов, автором утверждается, что при определении преступлений, совершаемых с применением информационных технологий, не надо основываться только на тех действиях, которые направлены на неправомерный доступ к электронно-цифровой информации, её модификацию, уничтожение, блокирование, незаконное завладение и противозаконное вмешательство в эксплуатацию электронно-вычислительной техники, а оно должно базироваться и на иные противоправные общественно-опасные деяния, совершаемые посредством или с помощью компьютерной техники, компьютерных сетей и программ.

В связи с этим, предлагается авторское определение преступлений данной категории, под которыми следует понимать противоправные деяния, запрещённые уголовным законом, наносящие ущерб или создающие угрозу нанесения ущерба интересам личности, общества и государства, совершаемые посредством цифровой и (или) электронно-вычислительной техники, компьютерных сетей и программ.

3) В настоящее время в научных кругах существуют различные суждения о том, какой термин стоит применять к цифровым следам: «электронные», «бинарные», «цифровые», «электронно-цифровые», «компьютерные», «виртуальные» и т.п.

Автор утверждает, что для содержательного определения рассматриваемого вида следов необходимо использовать термин «электронно-цифровые следы» и под ним следует понимать всякую связанную с расследуемым событием

трансформацию в информационном поле, зафиксированную в форме электромагнитных сигналов на материальном носителе и отражающую события действительности.

Электронно-цифровые следы по своей сути схожи со многими невидимыми материальными следами и имеют материальную природу происхождения.

4) Диссертантом обосновано, что выявление электронного отображения изменений в памяти электронных носителей о событии преступления является основой при установлении механизма образования электронно-цифровых следов. В связи с тем, что следообразующие и следовоспринимающие объекты не имеют материальной формы в информационном пространстве, любое изменение происходит в результате взаимодействия дискретных сигналов и среды.

Для установления и фиксации следов названной категории надлежит выявить пересекающееся взаимосоединение между образовавшимися изменениями, вычислительной системой и оставившим свое отражение действием или событием.

5) При механизме следообразования рассматриваемой группы следов в качестве отражающего объекта выступает вычислительная система, а отражаемого – пользователь. Инструментами отражения могут быть команды и электромагнитные сигналы, активизированные пользователем или прикладным программным обеспечением. Следообразующим объектом считается системное программное обеспечение, а в качестве следовоспринимающего объекта выступает массив памяти соответствующего устройства. Механизм образования данных следов зависит от конструкции информационного пространства, в котором они запечатлены.

6) В связи с отсутствием уголовно-процессуальных средств собирания фактических данных в информационно-телекоммуникационных сетях, предлагается восполнить данный пробел в законодательстве путём введения новых следственных действий в Уголовно-процессуальный кодекс Республики Таджикистан, таких как «Дистанционный осмотр электронно-цифровых информационных ресурсов» и «Дистанционный обыск».

Эти действия будут направлены на собирание доказательств, хранящихся в информационных системах, доступ к которым происходит опосредованно, через компьютерные сети. Различие этих двух следственных действий заключается в том, что дистанционный обыск осуществляется в принудительном порядке, а дистанционный осмотр – без применения принудительных мер.

Фиксация и изъятие доказательственной информации, находящейся в открытом доступе без применения паролей или иной защиты, должны осуществляться в рамках дистанционного (удалённого) осмотра интернет-ресурсов, под которым следует понимать процессуальное (следственное) действие, выражающееся в визуальном исследовании информации, содержащейся в компьютерных сетях, доступ к которой предоставлен неограниченному количеству лиц.

Сущность дистанционного обыска заключается в принудительном исследовании информационных ресурсов, доступ к которым ограничен, в целях получения доказательственной электронно-цифровой информации.

Под дистанционным (удалённым) обыском следует понимать процессуальное (следственное) действие, выражающееся в принудительном обследовании информационной системы посредством компьютерных сетей, доступ к содержимому которой ограничен её обладателем.

II. Предложения, направленные на совершенствование уголовного и уголовно-процессуального законодательства:

1) Предложен авторский подход для разрешения вопроса об использовании единого криминалистического определения информации, создаваемой, обрабатываемой и передаваемой средствами электронно-вычислительной техники и информационно-телекоммуникационных систем. В частности, предлагается в статьях главы 28 Уголовного кодекса Республики Таджикистан (Преступления против информационной безопасности) слова «компьютерная информация» заменить на «электронно-цифровую информацию» и статью 298 данной главы дополнить примечанием, где дать определение понятию «электронно-цифровой информации» в следующей редакции: «Электронно-цифровая информация –

данные, записанные в памяти компьютерных или иных микропроцессорных устройств, предназначенные для обработки с помощью электронно-вычислительной либо цифровой техники, а также сведения, передаваемые по каналам связи посредством дискретных сигналов».

2) Существует необходимость в пересмотре отдельных норм уголовно-процессуального законодательства Республики Таджикистан, которые относят электронно-цифровую информацию как разновидность доказательств к иным документам.

Электронно-цифровая информация не является бумагой, не всегда может выступать в качестве письменного свидетельства и в отличие от документов не составляется человеком, а создаётся путём набора определённых команд или записи процессов, протекающих в окружающем мире, посредством технических устройств. Кроме того, электронно-цифровую информацию невозможно воспринимать без использования технических устройств, тогда как документ доступен для непосредственного восприятия человеком. В связи с чем, предлагается определить электронно-цифровую информацию как отдельный вид доказательств и с этой целью внести соответствующее дополнение и изменение в УПК Республики Таджикистан: а) ч. 2 ст. 72 (Доказательства) дополнить новым подпунктом – «электронно-цифровая информация»; б) из ч. 2 ст. 82 исключить слова «электронные источники информации».

3) В целях правового регулирования процесса собирания доказательственной информации из информационно-телекоммуникационных сетей, доступ к которой предоставлен неограниченному кругу лиц, необходимо дополнить действующий Уголовно-процессуальный кодекс Республики Таджикистан статьёй 183 (1) «Дистанционный осмотр электронно-цифровых информационных ресурсов» в следующей редакции:

«Статья 183 (1). Дистанционный осмотр электронно-цифровых информационных ресурсов

1. Дознаватель, следователь или прокурор в целях обнаружения следов преступных действий, выяснения иных обстоятельств, имеющих значение для

правильного разрешения дела, проводит дистанционный (удалённый) осмотр информации, размещенной на электронно-цифровых информационных ресурсах и доступ к которой не ограничен.

2. В порядке, предусмотренном настоящим Кодексом, при производстве дистанционного осмотра в качестве специалиста может быть привлечено лицо, обладающее необходимыми знаниями в области информационных технологий.

3. О результатах проведения дистанционного осмотра составляется протокол, где помимо требований статей 172-173 настоящего Кодекса, также отражается сетевой адрес обследуемого электронного ресурса, содержащаяся на нём доказательственная информация, использованные программные и технические средства, модель и характерные свойства носителя, на котором скопированы криминалистически значимые данные.

4. Носитель со скопированными данными упаковывается способом, исключающим возможность получения доступа к его содержимому посторонним лицам».

4) Для создания уголовно-процессуальных норм по фиксации доказательственной информации в информационно-телекоммуникационных сетях, доступ к которой ограничен, предлагается дополнить действующий Уголовно-процессуальный кодекс Республики Таджикистан статьёй 194 (1) «Дистанционный обыск» следующего содержания:

«Статья 194 (1). Дистанционный обыск

1. Дознаватель, следователь или прокурор в целях принудительного обследования данных, доступ к которым ограничен, проводит дистанционный (удалённый) обыск электронно-цифровых информационных ресурсов.

2. Основанием для производства дистанционного обыска является наличие достаточных данных о возможном наличии в информационных ресурсах сведений, относящихся к расследуемому событию.

3. Дистанционный обыск проводится на основании мотивированного постановления должностного лица, в производстве которого находится уголовное дело, согласия прокурора и разрешения суда.

4. Участие специалиста при производстве дистанционного обыска является обязательным. При его содействии преодолеваются возможные технические и программные средства защиты электронно-цифровой информации.

5. Перед началом дистанционного обыска присутствующим разъясняется порядок проведения следственного действия. В случае присутствия владельца обследуемых информационных ресурсов, должностное лицо, осуществляющее следственное действие, ознакомит его с санкцией суда и предлагает добровольно предоставить доступ к интересующим следствие данным.

6. О результатах проведения дистанционного обыска информационных ресурсов составляется протокол с соблюдением требований статьи 194 настоящего Кодекса. Также, в протоколе указываются сетевой адрес обследуемого информационного ресурса, содержащаяся в нём доказательственная информация, использованные программные и технические средства, модель и характерные свойства носителя, на котором скопированы криминалистически значимые данные.

7. Электронный носитель со скопированной информацией упаковывается и опечатывается на месте производства следственного действия, что удостоверяется подписями лиц, участвующих в нём».

III. Предложения практического характера:

В зависимости от конкретной следственной ситуации автором обоснованно рекомендуются две группы тактических комплексов по обнаружению и фиксации электронно-цифровых следов:

1) В следственной ситуации, характеризующейся наличием данных о нахождении в компьютерной или иной цифровой технике участника уголовного судопроизводства электронно-цифровых следов, необходимо осуществить следующие процессуальные действия: а) произвести осмотр электронных носителей при участии специалиста соответствующего профиля; б) исследование полученной информации и её сопоставление с данными, имеющимися в распоряжении органов следствия; в) допрос участника уголовного судопроизводства (свидетеля, потерпевшего, подозреваемого, обвиняемого) с

предъявлением изъятых с электронных носителей данных.

В том случае, когда в результате следственного осмотра не получены искомые данные, необходимым считается: а) изъятие электронного носителя; б) назначение судебной компьютерно-технической экспертизы; в) допрос участника уголовного судопроизводства с предъявлением результатов экспертизы.

При благоприятном развитии ситуации, когда со стороны участников уголовного судопроизводства не оказывается противодействие следствию, перед вышеотмеченным комплексом можно произвести допрос владельца электронного носителя и осмотр места происшествия при участии специалиста.

2) В следственной ситуации, когда в распоряжении органов предварительного следствия имеются сведения о конкретном месте совершения общественно-опасного деяния, о лице либо лицах, совершивших преступление, и при этом предварительному следствию оказывается противодействие, результативным является применение следующего тактического комплекса: а) осмотр места происшествия в целях поиска и обнаружения электронных носителей информации; б) обыск в местах жительства и работы подозреваемых лиц в указанных целях; в) при участии специалиста в области информационных технологий осуществить оценку радиоэлектронной обстановки местности; г) установить номера сотовых аппаратов конкретных участников уголовного судопроизводства и запросить у операторов мобильной связи сведений о детализациях их телефонных переговоров с указанием месторасположения абонентов (геолокацией) на момент осуществления звонков, а также информацию о зонах обслуживания конкретных сервисных базовых станций; д) анализ или исследование полученных сведений; е) допрос участника уголовного судопроизводства с предъявлением детализации телефонных переговоров и результатов осмотра электронных носителей. Анализ может проводиться следователем самостоятельно либо с привлечением специалиста. При привлечении специалиста либо эксперта в исследовании, их выводы могут быть оформлены в форме заключения специалиста или эксперта.

Теоретическая и практическая значимость исследования. Теоретическая значимость состоит в том, что его результаты и сформулированные выводы послужат дальнейшему развитию криминалистической тактики и совершенствованию криминалистических рекомендаций по обнаружению и фиксации доказательственной электронно-цифровой информации на локальных и сетевых носителях. Также, в диссертации обозначено решение ряда проблем, связанных с правовым положением электронно-цифровых доказательств и упорядочением порядка собирания доказательственной информации в информационно-телекоммуникационных сетях.

Практическая значимость диссертационной работы определяется её прикладным характером и состоит в том, что представленные в диссертации заключения, выводы и предложения заслуживают внимания при разработке вопроса о совершенствовании уголовного и уголовно-процессуального законодательства в целях разрешения проблем, связанных с использованием электронно-цифровых доказательств в уголовном судопроизводстве, а также могут быть использованы в правоприменительной работе компетентных органов и педагогической деятельности образовательных учреждений юридической направленности.

Степень достоверности результатов. Достоверность диссертационного исследования обеспечена эмпирической базой исследования, широким использованием общенаучных и специально-научных методов, изучением общей и специальной литературы, диссертаций ряда учёных по избранной теме, в которых отражены современные научные подходы и взгляды об особенностях обнаружения и фиксации доказательственной информации на электронных носителях, а также практические рекомендации, направленные на совершенствование уголовного и уголовно-процессуального законодательства, а также правоприменительной деятельности по собиранию электронно-цифровых доказательств.

Соответствие диссертации паспорту научной специальности. Предмет и содержание исследования соответствует паспорту специальности: 12.00.12 –

Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность, утвержденному Высшей аттестационной комиссией при Президенте Республики Таджикистан.

Личный вклад соискателя учёной степени. Личный вклад соискателя учёной степени в исследование заключается в том, что основные идеи, имеющие теоретическую и практическую значимость, выносимые на защиту положения, выводы и обобщения, практические рекомендации могут иметь существенное значение для развития и совершенствования уголовного и уголовно-процессуального законодательства Республики Таджикистан, а также правоприменительной деятельности компетентных органов страны по собиранию электронно-цифровых доказательств. Научные публикации и выступления автора на различных научно-практических и научно-теоретических конференциях международного и республиканского уровня подтверждают его компетентность в исследуемых в диссертации вопросах.

Апробация и применение результатов диссертации. Диссертация выполнена на кафедре криминалистики и судебно-экспертной деятельности юридического факультета Таджикского национального университета.

Основные положения диссертационного исследования были представлены на международных и республиканских научно-практических и научно-теоретических конференциях:

– II Международной научно-практической конференции на тему «Юридическая наука и практика», посвященной Дню таджикской науки (г. Душанбе, 29 апреля 2023 г.);

– Республиканской научно-теоретической конференции на тему «Охрана границы - гарантия безопасности», посвященной 29-ой годовщине образования Пограничных войск ГКНБ Республики Таджикистан (г. Душанбе, 19 мая 2023 г.);

– Международной научно-практической конференции «Таджики в зеркале истории», посвященной 115-летию академика Бободжона Гафурова (г. Душанбе, 27 октября 2023 г.).

Рекомендации и предложения диссертационного исследования внедрены в

практическую деятельность следственных подразделений Государственного комитета национальной безопасности Республики Таджикистан, а также в учебный процесс Высшей школы ГКНБ Республики Таджикистан, что подтверждается соответствующими актами.

Публикации по теме диссертации. Основные выводы и рекомендации, разработанные и изложенные в диссертационной работе, освещались в 7 научных статьях, в том числе в 5 статьях, опубликованных в изданиях, рецензируемых Высшей аттестационной комиссией при Президенте Республики Таджикистан. А также по результатам работы издано 2 практических пособия.

Структура и объем диссертации. Диссертация состоит из перечня сокращений и (или) условных обозначений, введения, двух глав, включающие шесть параграфов, заключения, рекомендаций по практическому использованию результатов исследования, списка литературы (источников) и приложений. Наименование и последовательность глав и параграфов определены логикой исследования и порядком решения поставленных задач. Общий объём диссертации составляет 197 страниц.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ И МЕХАНИЗМ СЛЕДООБРАЗОВАНИЯ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ

1.1. Криминалистическое понятие электронно-цифровой информации и её место в системе доказательств по уголовным делам

Прежде всего, для определения сущности электронно-цифровой информации и её всестороннего анализа, необходимо определиться с базовыми понятиями «информация» и «криминалистически значимая информация».

Слово «информация» происходит от латинского слова «information» – разъяснение, изложение. В толковом словаре русского языка под редакцией С.И. Ожегова и Н.Ю. Шведовой даны следующие определения этого термина: «1. Информация – сведения об окружающем мире и протекающих в нем процессах, воспринимаемых человеком или специальным устройством. 2. Информация – сообщения, осведомляющие о положении дел, о состоянии чего-нибудь». Также, в словаре информация раскрывается через понятия «сведение», что означает «познания в какой-нибудь области, известия, сообщения, знания, представление о чем-нибудь»[41].

Закон Республики Таджикистан «Об информации» (№55, от 10.05.2002 г.) считается главным законодательным актом, регулирующим информационные отношения в Таджикистане. Он устанавливает общие правовые нормы получения, использования, распространения и хранения информации, закрепляет право субъекта информационных отношений на информацию во всех сферах общественной и государственной жизни Республики Таджикистан, а также систему информации, её источники, определяет статус участников информационных отношений, регулирует доступ к информации и обеспечивает её защиту, защищает личность и общество от ложной информации.

[41] Толковый словарь русского языка / Под ред. С.И. Ожегова, С.И. и Н.Ю. Шведовой. – М., 2010. – С. 250, 699.

В соответствии со ст. 1 настоящего Закона, «информация – сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их представления»[42]. Аналогичное понятие информации, также приводится в ст. 3 Закона Республики Таджикистан «Об информатизации» от 06.08.2001 г., №40[43]. Вместе с тем, в указанных нормативных актах формы представления информации не раскрываются. Обычно, по форме представления различают текстовую, числовую, графическую, звуковую и видеоинформацию. К текстовой информации относится все, что написано или напечатано на любом из существующих или существовавших языков. Она передаётся в виде символов, предназначенных обозначить лексемы языка. Числовая информация – сведения в виде цифр и знаков, обозначающие количественные характеристики объектов окружающего мира. Графические данные могут быть в виде рисунков, фотографий, схем, карт, чертежей и др. Человеческая речь, пение птиц, музыка, звук машин и другие различные сигналы, воспринимаемые органами слуха человека, относятся к звуковой информации. Видеоинформация – передаваемые в виде видеозаписи данные: фильмы, мультфильмы, выступления и т.п.

Впервые с юридической точки зрения определение информации было сформулировано А.И. Трусовым. Согласно его мнению, «информация охватывает отражение предметов и явлений в человеческом сознании, явлений и процессов друг в друге, вне связи с сознанием»[44]. То есть, он в данной формулировке брал за основу теорию отражения как свойство материи.

А.А. Фатьянов, отрицая материальную природу происхождения информации, предлагает понимать под этим термином воспринимаемую органами чувств человека окружающую действительность в виде распределения материи и энергии во времени и пространстве, а также процессы их перераспределения.

---

[42] Закон Республики Таджикистан «Об информации» от 10.05.2002 г. / В редакции закона от 03.07.2012 г., №848 [Электронный ресурс]. – Режим доступа: URL: http://www.adlia.tj/show_doc.fwx?rgn=3251&conttype=2 (дата обращения: 21.06.2022).

[43] Закон Республики Таджикистан «Об информатизации» // Ахбор Маджлиси Оли Республики Таджикистан, 2001 год. – №7, ст.502.

44 Савельева М.В., Степанов В.В. О понятии криминалистической информации / М.В. Савельева, В.В. Степанов // Вестник криминалистики. – 2009. – №4 (32). – С. 16.

Вместе с тем, он считает, что носителем информации является материя[45].

Все перечисленные определения информации в той или иной степени охватывают её свойства и раскрывают сущность данного термина. Вместе с тем, наиболее удачно и всесторонне, на наш взгляд, изложил понятие информации И.И. Салихов, по мнению которого «информация – нематериальные по своей сути, неразрывно связанные с конкретным материальным носителем, обладающие количественными и качественными характеристиками сведения о социальной форме движения материи и обо всех других её формах в той мере, в какой они используются участниками общественных отношений, вовлечены в орбиту общественной жизни»[46].

Вышеуказанные авторы предлагали только общее понятие информации, которое не охватывает её криминалистические параметры. Криминалистическая информация является частью информационного поля общества, и именно она имеет значение для установления истины и послужит правильному разрешению дела.

Большинство ученых-правоведов утверждает, что криминалистически значимая информация – это всякие сведения, имеющие отношение к раскрытию и расследованию общественно-опасных деяний. Она подразделяется на доказательственную и ориентирующую информацию. Под доказательственной информацией следует понимать сведения, связанные с событием преступления, и о сопряжённых с ним обстоятельствах, которые могут быть использованы в ходе предварительного следствия и судебного рассмотрения уголовных дел в качестве средства доказывания.

Ориентирующая информация – это не имеющие доказательственного значения данные, полученные из не процессуальных источников, которые могут быть использованы для раскрытия и расследования преступлений. Это сведения о возможных носителях доказательственной информации, местах их нахождения,

---

[45] См.: Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: учебное пособие. – М.: Издательская группа «Юрист», 2001. – С. 10.

[46] Салихов И.И. Информация с ограниченным доступом как объект гражданско-правовых правоотношений: автореф. дис. … канд. юрид. наук. – Казань, 2004. – С. 17.

обстоятельствах, позволяющих решить вопрос о выборе наиболее эффективных средств доказывания и т.п. Она необходима для выдвижения версий, планирования и подготовки оперативно-следственных мероприятий, определения направлений расследования и решения других задач, стоящих перед органами предварительного следствия.

По определению Е.Н. Паршина, «криминалистически значимая информация – информация, имеющая значение для установления обстоятельств, подлежащих доказыванию при производстве по уголовному делу, или способствующая получению таковой, также любая информация, имеющая значение для достижения целей уголовного судопроизводства»[47].

А.В. Григорьев считает, что: «Вся информация, используемая в ходе расследования преступлений, может быть определена как криминалистически значимая»[48]. Пожалуй, следует согласиться с данным утверждением, ибо, как выше было указано, криминалистически значимая информация может быть доказательственной и ориентирующей.

Кроме того, некоторые учёные криминалистически значимую информацию в зависимости от формы её получения разделяют на внутреннюю и внешнюю. Так, Р.С. Белкин утверждает, что «следователь получает два потока информации, один из которых является внешним, возникающим при изучении обстановки и обстоятельств расследуемого преступления. Второй поток – внутренний, содержится в памяти следователя в виде знаний, понятий, полученных как в процессе профессиональной подготовки, так и в ходе практической работы»[49].

На наш взгляд, внутренняя информация является основой профессиональных знаний участника уголовного судопроизводства, осуществляющего уголовное преследование. Она выступает в качестве первоисточника формирования информационного поля по расследуемому уголовному делу. Так как субъект расследования через призму своих профессиональных знаний и качеств

---

[47] Паршина Е.Н. Проблемы информационного обеспечения и защиты информации в предварительном расследовании: автореф. дис. ... канд. юрид. наук. – Ижевск, 2004. – С. 11.

[48] Григорьев А.Н. Теоретические аспекты информации и ее защиты в предварительном расследовании преступлений: автореф. дис. … канд. юрид. наук. – Калининград, 2002. – С. 7.

[49] Белкин Р.С. Курс криминалистики: в 3 т. Т. 1: Общая теория криминалистики. – М.: Юристъ, 1997. – С. 118.

анализирует внешнюю информацию и познает фактические обстоятельства дела.

В Уголовно-процессуальном кодексе Республики Таджикистан термины «криминалистически значимая информация» или «доказательственная информация» не встречаются, однако, они охватываются такими понятиями как «фактические сведения» и «фактические данные», которые, в свою очередь, сопряжены с доказательствами по уголовному делу.

Так, в ч. 1 ст. 72 УПК РТ говорится, что «доказательствами по уголовному делу считаются *фактические сведения*, на основе которых в порядке, определенном настоящим Кодексом, суд, прокурор, следователь, дознаватель устанавливают наличие или отсутствие общественно опасного деяния, доказанности или недоказанности совершения этого деяния и иные обстоятельства, имеющие значение для правильного разрешения дела».

Согласно ч. 2 ст. 88 указанного Кодекса, доказательство признается относящимся к делу, если оно представляет собой *фактические данные*, которые подтверждают, опровергают или ставят под сомнение выводы о существовании обстоятельств, имеющих значение для данного дела[50].

На наш взгляд, в данном положении уголовно-процессуального закона слова «ставят под сомнение» являются излишними, так как они не соответствуют общему определению понятия доказательства, которое, как выше отметили, дано в ч. 1 ст. 72 УПК РТ. Доказательство устанавливает наличие или отсутствие определённого юридического факта, доказанность либо недоказанность вины физического лица в совершении конкретного преступления, а также иные обстоятельства, имеющие значение для уголовного судопроизводства. Действительно, при осуществлении уголовного судопроизводства могут быть получены доказательства, достоверность которых вызывает сомнение, но утверждение о том, что доказательством также могут считаться фактические данные, которые ставят под сомнение выводы о чём-либо, является не корректным.

[50] Уголовно-процессуальный кодекс Республики Таджикистан от 03.12.2009 // Ахбор Маджлиси Оли Республики Таджикистан. – 2016. – №3. – ст. 128.

Следует отметить, что передача информации происходит посредством сигналов. Сигналы - это информационные коды, предназначенные для передачи сообщений. При этом, сообщением считается тот сигнал, который был принят получателем. Одними из первых методов передачи сообщений были сигнальные костры. К примеру, при возникновении угрозы нападения военные последовательно разжигали костры от одного поста к другому.

Сигналы бывают аналоговыми и дискретными. Человеческие органы чувств воспринимают всю информацию в аналоговом виде. Например, если мы видим проезжающий мимо поезд, то мы видим его непрерывно. Практически вся информация, возникающая в природе, являются аналоговыми, они непрерывистые и передавать их проще всего аналоговыми сигналами.

Примером аналогового сигнала в криминалистике могут быть устные показания очевидца преступления, которые в последующем преобразуются в дискретные сигналы в виде протокола допроса. Дискретный сигнал является прерывистым, представлен последовательностью цифровых значений и имеет два значения «1» и «0».

Информация в дискретном виде хранится, обрабатывается и передаётся посредством компьютерных устройств и информационно-телекоммуникационных систем. В криминалистике подобного рода информация получила название машинной, компьютерной, электронной или цифровой. Получение этих названий связано, прежде всего, с развитием информационных технологий. Нет единой терминологии применительно к информации данной категории. Первоначально такая информация получила название «машинной», так как она обрабатывалась посредством электронно-вычислительных машин (ЭВМ). После, данное название трансформировалась на «компьютерную», поскольку на смену названия ЭВМ пришёл термин «компьютер», а в последующем на «электронно-цифровую».

В Уголовном кодексе Республики Таджикистан целая глава посвящена защите «компьютерной информации» от преступных посягательств. Вместе с тем, в Кодексе отсутствует законодательное определение «компьютерной информации» как предмета преступного посягательства. Однако, анализ

отдельных статей главы 28 УК Республики Таджикистан (ст.ст. 298, 299, 301) позволяет сделать вывод о том, что в уголовном законе под этим термином понимается любая информация, содержащаяся в компьютерной системе, компьютерной сети или на машинных носителях[51].

В связи с отсутствием точного уголовно-правового определения понятия «компьютерной информации», в настоящее время в научных кругах нет единой позиции относительно данного вопроса. Так, В.Ю. Агибалов и В.А. Мещеряков утверждают, что для отнесения информации к классу «компьютерной» необходимо присутствие двух основных признаков: наличие материального носителя и представление информации в специальном виде, то есть, в виде, пригодном для обработки с использованием технических средств. По их мнению, «компьютерная информация – это информация, представленная в специальном (машинном) виде, предназначенном и/или пригодном для ее автоматической обработки, хранения и передачи с использованием технических средств и находящаяся на каком-либо материальном носителе, в том числе в электромагнитном поле»[52]. По сути, близка к данному понятию и точка зрения М.В. Старичкова, который при определении «компьютерной информации», также делает упор на местонахождение информации и форму её представления[53].

Применительно к процессу доказывания сформулировал определение информации рассматриваемого вида К.Д. Давлатзода, который считает, что компьютерная информация, применяемая в процессе доказывания, это фактические данные, обработанные в компьютерной системе и (или) переданные через телекоммуникационные каналы, доступные для восприятия человеком, на основе которых устанавливается обстоятельства, связанные с расследованием уголовного дела[54]. В данной формулировке вызывает возражение утверждение о

---

[51] Уголовный кодекс Республики Таджикистан от 21.05.1998 // Ахбор Маджлиси Оли Республики Таджикистан. – 2020. – №1. – ст.8, ст.9.

[52] См.: Агибалов В.Ю., Мещеряков В.А. Природа и сущность виртуальных следов / В.Ю. Агибалов, В.А. Мещеряков // Воронежские криминалистические чтения: сб. науч. трудов. – 2010. – Вып. 12. – С. 11; Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж: Изд-во Воронеж. гос. ун-та, 2002. – С. 46.

[53] См.: Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве / М.В. Старичков // Вестник Восточно-Сибирского института МВД России. – 2014. – №1. – С. 20.

[54] См.: Давлатзода К.Д. Основания расследования киберпреступлений. – Душанбе, 2023. – С. 57.

том, что компьютерные данные доступны для восприятия человеком. Ибо человеческие органы чувств не в состоянии воспринимать информацию в дискретном виде.

Между тем, некоторые научные круги считают необходимым исключить слово «компьютер» из определения «компьютерная информация» и взамен предлагают использовать понятие «электронно-цифровая информация». Одним из сторонников данной концепции является П.Г. Смагин, который считает, что в связи с появлением огромного количества цифровых устройств, создаваемую, записываемую и обрабатываемую в них информацию нельзя называть компьютерной. К примеру, если информация была создана на цифровом фотоаппарате, она никак не может быть компьютерной. Ему видится, понятие «компьютерная информация» уже не может охватывать все сферы использования информации в электронно-цифровом виде[55]. Пожалуй, следует соглашаться с данной точкой зрения. Действительно, в современном обществе динамично развиваются информационные технологии, разрабатывается и производится множество технических средств, которые имеют функции создания, обработки, хранения и передачи данных, но, вместе с тем, не являются компьютерным устройством. В связи с этим, необходимо для определения этих данных вместо дефиниции «компьютерная информация» использовать термин «электронно-цифровая информация».

В уголовно-процессуальном законе понятие «электронно-цифровая информация» законодательно не закреплено и этот термин упоминается лишь в одной норме, а именно в ч. 5 ст. 199 (Общие правила производства допроса) УПК РТ, где говорится, что «если показания связаны с *цифровыми данными* или иными сведениями, которые трудно удержать в памяти, допрашиваемый вправе пользоваться документами и записями…». В то же время, анализ нормативно-правовых актов Республики Таджикистан, регулирующих информационные правоотношения, позволяет сформулировать законодательное определение

[55] См.: Смагин П.Г. О понятии «компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД / П.Г. Смагин // Вестник Воронежского института МВД России. – 2008. – №1. – С. 80.

данного понятия следующим образом: электронно-цифровая информация – это зафиксированные на машинном носителе данные, предназначенные для обработки, записи и хранения с помощью электронно-вычислительной техники[56]. При этом, под машинным носителем понимается магнитная лента, магнитный диск, лазерный диск и иные материальные носители.

Наиболее точное и ёмкое по смыслу определение названной дефиниции предложено Н.А. Ивановым, который считает, что «электронно-цифровая информация – это информация, вводимая, обрабатываемая и хранящаяся в устройствах памяти средств компьютерной и иной микропроцессорной техники или передаваемая по каким-либо каналам связи, имеет вид или зафиксирована (представлена) в виде дискретных сигналов, т.е. сигналов, имеющих конечное число значений»[57].

В уголовном процессе дискуссионным является вопрос отнесения электронно-цифровой информации к тем или иным видам доказательств и по этому поводу существует несколько точек зрения.

Первая из них заключается в том, что электронно-цифровая информация относится к распространённым видам доказательств, а именно к иным документам или вещественным доказательствам. Подобную позицию занимает С.П. Ворожбит, которая предлагает при определении данной категории информации к тем или иным видам доказательств принимать во внимание её доказательственное значение. Так, если для процесса доказывания значение имеют материальные свойства носителя информации, то её следует относить к вещественным доказательствам, а в случае, когда существенным является содержание носителя, то его и его содержимое следует определить как иной

[56] Закон Республики Таджикистан «Об электронном документе» от 10.05.2002г., №51 (в редакции Закона РТ от 26.12.2005 г. №122; от 28.12.2012 г., №908; от 22.07.2013 г., №995) [Электронный ресурс]. – Режим доступа: URL: http://www.adlia.tj/show_doc.fwx?rgn=123088 (дата обращения: 23.05.2022).

[57] См.: Иванов Н.А. О понятии «цифровые доказательства» и их месте в общей системе доказательств / Н.А. Иванов // Проблемы профилактики и противодействия компьютерным преступлениям: материалы межд. науч.-практ. конф. (г. Челябинск, 30 мая 2007 г.) и «круглого стола» (г. Челябинск, 18 мая 2007 г.) – Челябинск: Челябинский центр по исследованию проблем противодействия организованной преступности и коррупции. – 2008. – С. 96.

документ[58].

Сторонники другой точки зрения предлагают признать электронно-цифровую информацию новым видом доказательств. Свою позицию они аргументируют тем, что данному виду информации присущи специфические свойства, которые отличают её от иных документов и вещественных доказательств[59]. Полагаю, что данная точка зрения является состоятельным, так как электронно-цифровая информация в отличие от документов не составляется человеком, а создаётся путём набора определённых команд или записи процессов, протекающих в окружающем мире, посредством технических устройств. Электронно-цифровую информацию невозможно воспринимать без использования технических устройств, тогда как документ и вещественное доказательство доступны для непосредственного восприятия человеком.

Также, существует точка зрения, согласно которой признание электронно-цифровой информации в качестве доказательства в уголовном процессе категорически отрицается. Так, А.М. Баранов считает, концепция о существовании электронно-цифровых доказательств ничем не обоснована, она является иллюзией авторов. Так как только человек может быть источником и носителем доказательственной информации. Электронная среда, устройства сохранения и передачи данных, протоколы процессуальных действий не считаются источниками (носителями) фактических данных, а являются их хранителями и в связи с чем, они не могут быть электронными доказательствами. А в качестве источника или носителя может выступать лицо, хранящее их на электронном устройстве или получившее их из электронного пространства либо прибора[60]. Пожалуй, не стоит соглашаться с мнением А.М. Баранова, ибо источником электронно-цифровой информации, кроме человека, могут выступать различные юридические лица, предприятия и учреждения.

---

[58] См.: Ворожбит С.П. Электронные средства доказывания в гражданском и арбитражном процессе: автореф. дис. … канд. юрид. наук. – Санкт-Петербург, 2011. – С. 8.

[59] См.: Карташов И. И. Проблемы формирования доказательств в уголовном судопроизводстве на основе цифровой информации / И.И. Карташов // Юридическая наука. – 2018. – №3. – С. 99-103.

[60] См.: Баранов А. М. Электронные доказательства: иллюзия уголовного процесса XXI в. / И.И. Карташов // Юридическая наука. – 2018. – №3. – С. 64-69.

Электронно-цифровую информацию, как правило, классифицируют по следующим трем критериям: по материальному носителю информации, по её функциональному назначению и по правовому статусу.

В соответствии с видом материального носителя выделяют электронно-цифровую информацию, находящуюся в жестком магнитном диске (винчестер, НЖМД, HDD, RAID), в оперативном запоминающем устройстве (ОЗУ-RAM) и постоянном запоминающем устройстве (ПЗУ-ROM), в микропроцессорах, в съемных носителях информации и в электронных средствах связи: проводных и беспроводных (линии электросвязи, компьютерные сети и другие), в которых она находится при передаче.

Согласно функциональному применению исследуемый вид информации делится на документы (текстовые и графические), сведения в форматах мультимедиа, данные в форматах баз данных и программное обеспечение (базовые программы, операционные системы, служебные (сервисные) программы, языки программирования, прикладные программы).

По правовому статусу различают две формы электронно-цифровой информации: документированную информацию (документ) и информацию, не имеющую документированной формы. Электронно-цифровые документы имеют определенные реквизиты и должны отвечать определённым требованиям.

В соответствии со ст. 6 Закона Республики Таджикистан «Об электронном документе» (№51, от 10 мая 2002 г.) к основным требованиям, предъявляемым к электронному документу относятся возможность его создания, обработки, приёма, передачи и хранения посредством программных и технических устройств, наличие у него определённой структуры и реквизитов для идентификации, а также, представление его в форме, понятной для восприятия человеком[61].

В недокументированной электронно-цифровой информации значение имеет содержание и её материальный носитель.

---

[61] Закон Республики Таджикистан «Об электронном документе» от 10.05.2002г., №51 (в редакции Закона РТ от 26.12.2005 г. №122; от 28.12.2012 г., №908; от 22.07.2013 г., №995) [Электронный ресурс]. – Режим доступа: URL: http://www.adlia.tj/show_doc.fwx?rgn=123088 (дата обращения: 23.05.2022).

И так, можно констатировать, что основной отличительной чертой электронно-цифровой информации является наличие у неё материального носителя, без которого её существование невозможно.

В действующем Уголовно-процессуальном кодексе Республики Таджикистан термин «электронные носители информации» не встречается. Вместо него используется выражение «электронные источники информации». В соответствии с ч. 2 ст. 82 Кодекса электронные источники информации отнесены как разновидность доказательств к иным документам. Также, положения данной статьи уголовно-процессуального закона не исключает признать их вещественными доказательствами. Так, согласно ч. 3 ст. 82 УПК РТ, если документы обладают признаками, предусмотренными в статье 78 настоящего Кодекса, они могут быть признаны вещественными доказательствами. В статье 78 речь идёт о вещественных доказательствах и обстоятельствах, при которых определённые предметы могут признаваться таковыми.

Следует отметить, что положения ст. 82 УПК Республики Таджикистан об отнесении электронно-цифровой информации (её носителей) как разновидность доказательств к иным документам не соответствуют этимологическому значению данной категории информации. Так, «документ – это облечённый в письменную форму носитель информации, удостоверяющий наличие фактов определённого значения»[62]. Слово «документ» в «Толковом словаре русского языка» приводится в двух значениях: «1. Документ – это деловая бумага, подтверждающая какой-либо факт или право на что-либо. 2. Письменное свидетельство каких-либо исторических событий»[63]. Вместе с тем электронно-цифровая информация не является бумагой, не всегда может выступать в качестве письменного свидетельства и в отличие от документов не составляется человеком, а создаётся путём набора определённых команд или записи процессов, протекающих в окружающем мире, посредством технических устройств. Кроме того, электронно-

[62] См.: Документ [Электронный ресурс]. – Режим доступа: https:// ru.wikipedia.org/wiki (дата обращения: 22.02.2023).

[63] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений. / С.И. Ожегов, Н.Ю. Шведова / Российская академия наук. Институт русского языка им. В.В. Виноградова. – 4-е изд., – Москва: ООО «А ТЕМП», 2013. – С. 168.

цифровую информацию невозможно воспринимать без использования технических устройств, тогда как документ доступен для непосредственного восприятия человеком. В связи с чем, необходимо определить электронно-цифровую информацию как отдельный вид доказательств и включить её в ст. 72 (Доказательства) УПК Республики Таджикистан.

В Законе Республики Таджикистан «Об электронном документе» (№51 от 10 мая 2002 г.) встречается термин «машинный носитель», который по определению означает «электронный носитель информации». В соответствии со ст. 1 Закона, «машинный носитель - магнитный диск, магнитная лента, лазерный диск и иные материальные носители, используемые для записи и хранения информации с помощью электронно-вычислительной техники»[64]. Следует согласиться, что на момент принятия Закона данное определение отвечало существующим требованиям к электронным источникам информации. Однако, с учётом стремительного развития информационно-телекоммуникационных технологий в последние два десятилетия, возникла необходимость в его усовершенствовании.

Ввиду того, что в законодательстве отсутствует определение понятия «электронного носителя (источника) информации», в юридической литературе имеются различные мнения на этот счёт. Так, А.А. Балашова в своей диссертационной работе сформулировала понятие электронного носителя информации как «техническое средство, конструктивно предназначенное для хранения информации в электронно-цифровой форме, доступной для обработки с использованием средств вычислительной техники»[65]. В целом данное определение раскрывает природу исследуемого предмета, но, вместе с тем, оно не охватывает всю совокупность его функций по записи, передаче и воспроизведению информации.

Также, обращает на себя внимание классификация электронных носителей информации, предложенная А.А. Балашовой. Она проводит её одновременно по

[64] Закон Республики Таджикистан «Об электронном документе» от 10.05.2002г., №51 (в редакции Закона РТ от 26.12.2005 г. №122; от 28.12.2012 г., №908; от 22.07.2013 г., №995) [Электронный ресурс]. – Режим доступа: URL: http://www.adlia.tj/show_doc.fwx?rgn=123088 (дата обращения: 23.05.2022).

[65] Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. … канд. юрид. наук. – Москва, 2020. – С. 28.

нескольким критериям:

– в зависимости от связи с расследуемым событием, она разделяет их на первичные и вторичные. К числу первичных предлагает относить электронные носители информации, непосредственно связанные с преступным событием, а к вторичным – носители, полученные в результате следственных и иных процессуальных действий;

– в зависимости от типа устройства отличает внутренние и внешние носители. Первая группа носителей конструктивно встроена в вычислительную технику и информационную систему и является их неотделимой частью. Внешние носители считаются добавочным компонентом, и их снятие не повлияет на полноценное функционирование вычислительной техники и информационной системы;

– по продолжительности хранения информации она выделяет три вида электронных носителей: носители оперативного хранения, носители временного хранения и носители постоянного хранения;

– по функциональности разделяет монофункциональные и полифункциональные электронные носители информации. Монофункциональные носители предназначены всего лишь для хранения данных, а вторые, помимо хранения, наделены и другими функциями;

– по возможности автономного функционирования на энергозависимые и энергонезависимые. Первая группа носителей может сохранить в себе информацию при условии внешнего энергопотребления, а вторая группа способна осуществить данную функцию без внешнего энергопотребления;

– в зависимости от способа получения доступа к данным различает локальные и сетевые носители. Для получения доступа к информации, хранящейся на локальном носителе, необходимо физическое подключение к компьютерной системе или носителю, а доступ к данным, содержащимся на сетевых носителях, осуществляется дистанционно по каналам связи[66].

Р.И. Оконенко, рассматривая электронных носителей информации как

[66] См.: Там же. – С. 12-13.

важнейший компонент информационной системы, в качестве их отличительных свойств выделяет такие элементы, как наличие большой информационной вместимости, лёгкость передачи и копирования данных, возможность дистанционно доступа к их содержимому, относительность и неочевидность содержания носителей[67].

Вместе с тем, В.Н. Григорьев и О.А. Максимов применительно к уголовному процессу рассматривают «электронный носитель информации» как «предмет, содержащий значимую для уголовного дела информацию, созданную не в процессе расследования уголовного дела, восприятие которой невозможно без использования электронно-вычислительных средств»[68]. По нашему мнению, здесь слова «созданные не в процессе расследования уголовного дела» являются излишними и сужающими понятия исследуемого устройства. Ибо не исключена возможность получения криминалистически значимой информации с технических устройств, образовавшейся в ходе расследования уголовного дела. Например, сведения, полученные при прослушивании и записи переговоров, произведенных в рамках расследования уголовных дел в порядке ст. 196 УПК Республики Таджикистан.

На наш взгляд, с точки зрения криминалистической науки удачно сформулировал определение «электронного носителя информации» Ю.В. Гаврилин, по мнению которого «это устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для её передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[69].

Таким образом, учитывая рассмотренные теоретические аспекты понятия электронно-цифровой информации можно подытожить следующее.

---

[67] См.: Оконенко Р. И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р.И. Оконенко // Актуальные проблемы российского права. – 2015. – №3. – С. 120-124.

[68] Григорьев В.Н. Понятие электронных носителей информации в уголовном судопроизводстве / В.Н. Григорьев // Вестник Уфимского юридического института МВД России. – 2019. – №2 (84). – С. 40.

[69] См.: Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве / Ю.В. Гаврилин // Труды Академии управления МВД России. – 2017. – №4 (44). – С. 48.

В современном обществе электронно-цифровая информация играет значимую роль в процессе доказывания по уголовным делам и существует потребность в активном использовании цифровых следов в работе по раскрытию и расследованию преступлений. С развитием информационных технологий расследование преступлений практически невозможно представить без информации с электронных носителей, на которых могут содержаться криминалистически значимые сведения, необходимые для правильного разрешения дела. Электронные носители достаточно информативны и содержащиеся на них данные необходимо правильно фиксировать, извлекать и приобщать к уголовным делам.

Термины «цифровая информация», «электронно-цифровая информация», «машинная информация» и «компьютерная информация» являются тождественными понятиями и имеют одинаковое значение в криминалистической науке. Поскольку, всем им присуще наличие материальных носителей, представлены они в форме электрических сигналов, воспроизводятся и обрабатываются посредством технических устройств.

При совершении преступлений с использованием информационных технологий, их следы отражаются в виртуальной среде в виде электронно-цифровой информации, а не на конкретных предметах материального мира. От своевременного обнаружения и грамотной фиксации криминалистически значимой цифровой информации зависит раскрываемость преступлений.

Вместе с тем, работа с электронно-цифровой информацией вызывает определённые сложности у органов предварительного следствия. Это связано, прежде всего, с особенностью образования цифровых следов, отсутствием специальных технических знаний у сотрудников, а также недостаточным правовым регулированием данного вопроса.

В связи с изложенным, полагаем, что в условиях постоянного развития информационных технологий и их широким использованием в преступной деятельности, сотрудникам органов дознания и следствия необходимо совершенствовать свои знания в области информационно-

телекоммуникационных технологий, изучить опыт зарубежных коллег по выявлению, изъятию и хранению электронно-цифровой информации, проводить процессуальные действия по осмотру и фиксации доказательственной электронно-цифровой информации, с обязательным участием специалиста, так как последний знаком с техническими особенностями компьютерных систем и сетевого пространства, и не допустить утери доказательств.

Также, считаем, что назрела объективная необходимость в проработке вопроса о внесении соответствующих изменений и дополнений в законодательство Республики Таджикистан в целях правового регулирования рассматриваемого вопроса, а именно: а) определить электронно-цифровую информацию как отдельный вид доказательств и включить её в ст. 72 УПК РТ; б) в статьях главы 28 УК РТ (Преступления против информационной безопасности) слова «компьютерная информация» заменить на «электронно-цифровую информацию» и статью 298 данной главы дополнить примечанием, где определить понятие «электронно-цифровой информации» в следующей редакции: «Электронно-цифровая информация – данные, записанные в памяти компьютерных или иных микропроцессорных устройств, предназначенные для обработки с помощью электронно-вычислительной либо цифровой техники, а также сведения, передаваемые по каналам связи посредством дискретных сигналов».

1.2. Криминалистические аспекты понятия и классификации преступлений, совершаемых с применением информационных технологий

Техническая вооружённость является новым качеством преступности в современном информационном обществе. Информационное общество - это «общество, в котором социально-экономическое развитие зависит, прежде всего, от производства, переработки, хранения, распространения информации среди его членов»[70]. Стремительный переход общества в цифровую среду и внедрение

[70] Павловец В.И. России нужны не биороботы, а креативный средний класс: о направлениях эффективного реформирования экономики и образования / В.И. Павловец // Альманах современной науки и образования. – 2013. – №1 (68). – С. 104.

инновационных технологий в управление общественными и производственными процессами порождают новые способы совершения общественно-опасных деяний, связанных с применением информационных технологий.

Преступники, используя широкую распространённость и доступность информационных технологий, умело применяют их как при совершении преступлений, так и при сокрытии следов преступной деятельности.

В современном обществе информационные технологии используются в механизме совершения большого количества общественно-опасных деяний. Особенно часто отмечается данная проблема при расследовании преступлений в сфере экономики, информационной безопасности, против общественной безопасности и конституционного строя.

В законодательстве и юридической литературе употребляются различные термины для определения преступлений, совершаемых с использованием информационных технологий.

Так, глава 28 Уголовного кодекса Республики Таджикистан носит название «Преступления против информационной безопасности», которая включает семь статей (ст.ст. 298-304). Однако в них определение данной категории преступлений не даётся. Из анализа положений уголовного закона можно приходить к выводу, что преступлениями против информационной безопасности являются деяния (действия или бездействия), совершаемые в области информационных процессов, посягающие на общественные отношения в сфере информационной безопасности, предметом которых являются электронно-вычислительная техника и цифровая информация.

В Конвенции Совета Европы о преступности в сфере компьютерной информации (ETS №185, от 23 ноября 2001 г.), рассматриваемая категория преступлений называется преступлениями в сфере компьютерной информации. Хотя в данном международном нормативно-правовом акте определение преступлений в сфере компьютерной информации напрямую не приводится, однако положения его преамбулы позволяют включить под данное определение общественно-опасные действия, направленные против конфиденциальности,

целостности и доступности компьютерных систем и сетей и компьютерных данных, а также на злоупотребление такими системами, сетями и данными[71].

Следует отметить, что эти два определения, вытекающие из положений уголовного закона и норм упомянутого международно-правового акта, не могут описать всю совокупность совершаемых с использованием информационных технологий преступлений. Так как, объекты посягательства этих преступлений намного шире, чем преступлений, предусмотренных главой 28 УК Республики Таджикистан и Конвенцией Совета Европы о преступности в сфере компьютерной информации.

В.В. Крылов именует их информационными преступлениями и в качестве объекта их преступного посягательства рассматривает наиболее узкую группу общественных правоотношений, то есть только те правоотношения, которые возникнут в процессе оборота электронно-цифровой информации и функционирования информационных систем. Он предлагает понимать под информационными преступлениями «общественно опасные деяния, совершенные в области информационных правоотношений и запрещенные уголовным законом под угрозой наказания»[72].

Близкое по смыслу с В.В. Крыловым определение компьютерным преступлениям даётся В.Б. Веховым. При этом, последний только компьютерную (машинную) информацию считает объектом преступлений данного вида, а вычислительную технику, компьютерную систему и сеть относит к предмету и средствам их совершения[73].

Наиболее широкое определение высказывает Т.Г. Смирнова, по мнению которой преступлениями в области компьютерной информации являются «запрещенные уголовным законом общественно-опасные виновные деяния, которые направлены на нарушение неприкосновенности охраняемой законом

[71] Конвенция Совета Европы о преступности в сфере компьютерной информации, ETS №185 (23 ноября 2001 г., г. Будапешт) [Электронный ресурс]. – Режим доступа: URL: https://rm.coe.int/1680081580 (дата обращения: 23.05.2022).
[72] Крылов В.В. Основы криминалистической теории расследования преступлений в сфере информации: дис. ... д-ра юрид. наук. – М., 1998. – С. 184.
[73] См.: Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. / Под общ. ред. Б.П. Смагоринского. – Москва, 1996. – С. 11.

компьютерной информации и её материальных носителей (в том силе, электронно-вычислительные машины (ЭВМ), систем ЭВМ или их сетей), причиняют либо создают угрозу причинения вреда жизни и здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности»[74].

Несколько иной точки зрения относительно определения компьютерных преступлений придерживается И.А. Клепицкий, согласно которой компьютерное преступление (преступление в сфере компьютерной информации) – «запрещённое уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности и конституционному строю)»[75].

Ряд авторов применяют к рассматриваемой группе преступлений слово «киберпреступления». Так, Алексеев С.В. рассматривает киберпреступления как «уголовно караемые действия, предполагающие незаконное попадание в службу компьютерных систем, с задачей модифицирования компьютерных данных». При этом он ошибочно полагает, что подобные преступления преследуют исключительно экономическую цель и наносят вред чьей-либо собственности или предпринимательской деятельности. И объектом преступления считает информационную безопасность, а предметом – компьютер[76].

М.А. Простосердов[77]. и О.С. Гузеева[78]. при формулировании определения киберпреступлений в качестве основного характеризующего элемента указывают

---

[74] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис. … канд. юрид. наук. – М., 1999. – С. 32.

[75] Уголовное право Российской Федерации. Особенная часть / Под ред. Здравомыслова Б.В. – М.: БЕК, 2000. – С. 353.

[76] Алексеев С.В. Особенности раннего становления групповых преступлений в киберпространстве / С.В. Алексеев // Вопросы российского и международного права. – 2020. – Том 10. – №10 А. – С. 183-191.

[77] См.: Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. – М., 2016. – С. 30.

[78] См.: Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы): автореф. дис. ... канд. юрид. наук. – М., 2008. – С. 12.

на возможность их совершения удалённым (дистанционным) способом. По нашему мнению, нельзя согласиться с утверждением названных авторов о том, что киберпреступления могут совершаться только посредством удалённого доступа к объекту посягательства, поскольку существует много способов совершения общественно-опасных деяний данной категории путём непосредственного воздействия на электронно-цифровую информацию и её материальных носителей.

Т.М. Хусяинов в своём исследовании предлагает понимать под киберпреступлениями весь спектр преступных действий в сфере информационных технологий[79]. Необходимо подчеркнуть, что данное определение намного сужает сущность данной категории преступлений, поскольку их объектом могут выступать не только сфера информационных технологий, как утверждает Т.М. Хусяинов, но могут быть и другие охраняемые уголовным законом общественные отношения.

По мнению А. Щетилова, понятие «киберпреступления» подразумевает не только противоправные действия в глобальной сети Интернет, а оно охватывает и другие преступления, совершаемые в области информации и телекоммуникаций и объектами которых могут выступать информация, информационные ресурсы и технологии[80].

Согласно позиции К.Д. Давлатзода, «киберпреступления» - это совокупность преступлений, совершаемых в виртуальной среде посредством сети Интернет, компьютерных систем и сетей, а также других средств доступа в виртуальное пространство[81].

---

[79] См.: Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве / Т.М. Хусяинов // Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования. Материалы всероссийского круглого стола. – 2015. – С. 120.

[80] См.: Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом / А. Щетилов // Информатизация и информационная безопасность правоохранительных органов: материалы XI междунар. конф. – М., 2002. – С.187.

[81] См.: Давлатзода К.Д. Угрозы виртуальной среды: практика и теория киберпреступлений: монография. – Душанбе, 2023. – С. 33.

Более широкое определение даётся М.Е. Батухтиным, по мнению которого «киберпреступление - это любое преступление в электронной сфере, совершенное при помощи компьютерных средств или виртуальной сети, или против них»[82].

Принимая во внимание приведенные выше позиции и отдельные положения Закона Республики Таджикистан «Об информатизации»[83], можно сформулировать понятие преступлений, совершаемых с использованием информационных технологий и определить их как противоправные деяния, запрещённые уголовным законом, наносящие ущерб или создающие угрозу нанесения ущерба интересам личности, общества и государства, совершаемые посредством цифровой и (или) электронно-вычислительной техники, компьютерных сетей и программ.

Таким образом, в связи с внедрением информационных технологий в большинство сфер деятельности личности, общества и государства понятие «преступления, совершаемые с применением информационных технологий» необходимо трактовать широко, так как оно включает в себя большую часть преступлений, предусмотренных уголовным законом.

Большое значение в нашем исследовании имеют вопросы классификации преступлений исследуемого вида.

В Конвенции Совета Европы о преступности в сфере компьютерной информации исследуемая группа преступлений делится на четыре подгруппы:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем: незаконный доступ, незаконный перехват, воздействие на компьютерные данные или компьютерные системы, а также противозаконное использование компьютерных устройств (ст.ст. 2-6);

2. Преступления, связанные с использованием компьютерных средств: подлог и мошенничество с использованием компьютерных технологий (ст.ст. 7-8);

---

[82] Батухтин М. Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе. Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов – 2018. – С. 25.

[83] См.: Закон Республики Таджикистан «Об информатизации. Ахбор Маджлиси Оли Республики Таджикистан. – 2001. – №7. – ст. 502.

3. Преступления, связанные с незаконным производством, распространением и приобретением порнографических материалов. незаконные действия, направленные на производство, предложение, приобретение и владение детской порнографической продукции с использованием компьютерных технологий (ст. 9);

4. Преступления, связанные с нарушением авторского права и смежных прав (ст. 10). Данная подгруппа охватывает действия, связанные с незаконным использованием объектов авторского права и смежных прав, в том числе, противоправное приобретение, хранение и пересылка незаконных копий произведений, совершённые с помощью компьютерной системы.

Согласно принятому в 2002 году Протока к настоящей Конвенции в данный перечень включён новый состав, заключающийся в незаконном распространении данных расистского и другого характера, направленного на насильственные действия, ненависть или дискриминацию отдельного лица или группы лиц на основе расовой, национальной, религиозной или этнической принадлежности[84].

Необходимо заметить, что положения Конвенции не охватывает весь масштаб уголовно наказуемых деяний, совершаемых посредством информационных технологий. К примеру, в ней не указаны составы преступлений против личности, здоровья населения, государственной власти, общественной безопасности и т.п., при совершении которых используются информационные технологии.

Намного шире, чем в указанной Конвенции, приводится классификация исследуемой категории преступлений в Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий (28 сентября 2018 г., г. Душанбе)[85].

[84] Конвенция Совета Европы о преступности в сфере компьютерной информации, ETS №185 (23 ноября 2001 г., г. Будапешт) [Электронный ресурс]. – Режим доступа: URL: https://rm.coe.int/1680081580 (дата обращения: 23.05.2022).

[85] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (28 сентября 2018 г., г. Душанбе) [Электронный ресурс]. – Режим доступа: URL: https://www.cisatc.org/1289/9115/135/9126/9128/9034 (дата обращения: 23.05.2022).

В соответствии со ст. 3 Соглашения все уголовно наказуемые деяния в сфере информационных технологий разделены на 8 групп:

а) уничтожение, блокирование, модификация либо копирование информации и нарушение работы информационной (компьютерной) системы;

б) действия, направленные на создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы;

г) хищение имущества путем изменения компьютерной информации;

д) использование информационных сетей для распространения порнографии;

е) изготовление специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) неправомерное использование компьютерных программ для нарушения авторских прав;

з) распространение с использованием компьютерных сетей материалов экстремистской и террористической направленности.

Спецификой приведенной классификации заключается в том, что в настоящем Соглашении указывается использование «информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи» и она охватывает более широкий круг уголовно наказуемых деяний.

В научной литературе в качестве одного из оснований для классификации преступлений, совершаемых с использованием информационных технологий, предлагается принять функции информационных технологий.

Так, А.А. Рудых выделяет шесть функций информационных технологий в механизме совершения преступлений рассматриваемой категории: информационную, коммуникативно-координирующую, операционную, функцию сокрытия преступления, объективизации и функция обеспечения[86].

[86] См.: Рудых А.А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: автореф. дис. ... канд. юрид. наук. – Ростов н/Д., 2020. – С. 11-12.

На этой основе эти преступления можно разделить на две группы:

а) преступления, совершаемые с использованием информационных технологий;

б) общественно-опасные деяния, объектом посягательства которых является информационная безопасность.

В первую группу включены те преступления, при совершении которых машинная (компьютерная) информация и информационные технологии применяются для достижения преступных целей: кражи, мошенничества, вымогательства, преступления террористической и экстремистской направленности, незаконный оборот наркотических средств, ядовитых веществ и оружия и т.п.

Вторую группу составляют преступления, в механизме совершения которых происходят процессы, связанные с преобразованием электронно-цифровой информации, нарушением функционирования компьютерной техники и компьютерной системы, незаконным оборотом специальных средств для получения доступа к компьютерной системе.

А.В. Федоров, основываясь на объекты преступного посягательства, классифицирует киберпреступления на три группы:

– экономические;

– против личных прав и частной неприкосновенности;

– против интересов общества и государства[87].

Если за основу классификации брать структуру объектов уголовно-правовой охраны, то рассматриваемую категорию преступлений можно разделить на следующие группы:

1. Преступления, совершаемые с применением информационных технологий против личности (доведение до самоубийства (ст. 109), угроза убийством или причинением тяжкого вреда здоровью (ст. 120), вербовка людей для эксплуатации

[87] См.: Федоров А.В. Информационная безопасность в мировом политическом процессе: учеб. пособие / А.В. Федоров. – М., 2006. – С. 111.

(ст. 132), публичное оскорбление Президента Республики Таджикистан или клевета в его адрес (ст. 137) и др.).

2. Преступления, совершаемые с применением информационных технологий против общественной безопасности и здоровья населения (терроризм (ст. 179), вовлечение в совершение преступлений террористического характера или иное содействие их совершению (ст. 179 (1)), финансирование преступлений террористического характера (ст. 179 (2)) и др).

3. Преступления, совершаемые с применением информационных технологий против общественного порядка и нравственности (вовлечение в занятие проституцией (ст. 238), незаконное изготовление и оборот порнографических материалов или предметов (ст. 241) и др.).

4. Преступления, совершаемые с применением информационных технологий в сфере экономики (кража (ст. 244), присвоение или растрата (ст. 245), хищение средств, выданных в качестве кредита (ст. 246), мошенничество (ст. 247) и др.).

4. Преступления, совершаемые с применением информационных технологий против информационной безопасности (неправомерный доступ к компьютерной информации (ст. 298), модификация компьютерной информации (ст. 298), компьютерный саботаж (ст. 300) и др.).

5. Преступления, совершаемые с применением информационных технологий против государственной власти (измена государству (ст. 305), публичные призывы к насильственному изменению конституционного строя Республики Таджикистан (ст. 307), публичные призывы к осуществлению экстремистской деятельности и публичное оправдание экстремизма (ст.307 (1)) и др.).

6. Преступления, совершаемые с применением информационных технологий против военной службы (оскорбление военнослужащего (ст. 372).

7. Преступления, совершаемые с применением информационных технологий против мира и безопасности человечества (публичные призывы к развязыванию агрессивной войны (ст. 396), наёмничество (ст. 401), незаконное

вовлечение и участие граждан Республики Таджикистан и лиц без гражданства в вооруженных подразделениях, вооруженном конфликте или военных действиях на территории других государств (ст. 401 (1)).

Следует отметить, что, несмотря на повсеместное использование информационных технологий в преступных целях, в Республике Таджикистан статистический учёт данной категории преступности не ведётся. В ходе исследования нам удалось получить в Главном информационно-аналитическом центре МВД Республики Таджикистан ограниченный объём информации о рассматриваемом виде преступности. То есть, только о тех преступлениях, в диспозиции которых использование электронно-цифровых данных и информационных технологий указано как элемент объективной стороны или как квалифицирующий признак соответствующего состава. А именно, о преступлениях, предусмотренных ч. 2 ст. 137, ч. 2 ст. 137(1), п. «г» ч. 2 ст. 179 (1), ч. 2 ст. 179 (3), ст. 189, п. «б» ч. 3 ст. 241, п. «д» ч. 2 ст. 241 (1), п. «г» ч. 2 ст. 241 (2), ст.ст. 298, 299, 300, 301, 302, 303, 304, п. «г» ч. 2 ст. 307, ч. 2 ст. 307 (1), ч. 2 ст. 307 (3), ч. 2 ст.330 и ч. 2 ст. 396 УК Республики Таджикистан.

Таким образом, количественная динамика преступлений, совершённых с применением информационных технологий, в Республике Таджикистан по вышеуказанным составам за 2018-2022 гг. выглядит следующим образом:

– за 2018 год – 785 преступлений;

– за 2019 год – 898 преступлений;

– за 2020 год – 1067 преступлений;

– за 2021 год – 1000 преступлений;

– за 10 месяцев 2022 года – 1041 преступление[88].

Количество рассматриваемого вида преступлений имеет тенденцию к росту. При этом, самый высокий показатель по использованию информационных технологий отмечается в механизме совершения преступлений террористической и экстремистской направленности (предусмотренных п. «г» ч. 2 ст. 179 (1), ч. 2 ст. 179 (3), ст. 189,п. «г» ч. 2 ст. 307, ч. 2 ст. 307 (1) и ч. 2 ст. 307 (3) УК РТ):

[88] См.: Письмо МВД Республики Таджикистан, №14/3-1251 от 23.11.2022 г.

– за 2018 год – 701 преступление;

– за 2019 год – 831 преступление;

– за 2020 год – 988 преступлений;

– за 2021 год – 966 преступлений;

– за 10 месяцев 2022 года – 980 преступлений[89].

Особую тревогу вызывает использование сети Интернет в террористических и экстремистских целях. С начала 90-х годов прошлого столетия Интернет неуклонно расширяет свою аудиторию по всему миру как средство коммуникации. Современные интернет-технологии способствуют безграничному общению людей в условиях анонимности и быстро преодолевая государственные границы. Вместе с тем, те же технологии активно используются террористическими и экстремистскими организациями. И в этой связи, Дж.М. Зоир совершенно справедливо отмечает, что «особенности преступности в сфере высоких технологий, полем которой является единое информационное пространство, создают угрозу международной безопасности во всех странах мира, независимо от их географического положения, в том числе и это касается Республики Таджикистан»[90].

Использование Интернета в пропаганде является одним из основных направлений деятельности террористов. В большинстве своём пропагандистские материалы имеют мультимедийную форму, содержащие идеологические наставления, разъяснения, оправдания либо рекламу террористической деятельности. Они состоят из виртуальных сообщений, презентаций, журналов, аудио и видеофайлов, различных электронных игр, побуждающих молодёжь участвовать в роли виртуального террориста. Подобные материалы, прежде всего, ориентированы на потенциальных сторонников террористических и экстремистских организаций и направлены на их вербовку, радикализацию и подстрекательство к совершению террористических преступлений. Они также могут быть использованы для отчета об успешном проведении террористических

[89] С динамикой преступности по каждому составу по отдельности можно ознакомиться в приложении №1.

[90] Зоир Дж.М. Оперативно-розыскное мероприятие получение компьютерной информации и права человека / Дж.М. Зоир // Труды Академии МВД Республики Таджикистан. – 2018. – №1 (37). – С. 26-37.

актов перед теми, кто обеспечивает их финансирование. Также, пропаганда может преследовать цель устрашения населения путём распространения чувств повышенной тревоги, страха или паники[91].

Интернет-технологии являются эффективным средством для поиска и установления отношений с потенциальными новобранцами в террористические организации. Для конфиденциальности своей деятельности по вербовке новых членов террористы используют защищённые веб-сайты и чат-группы ограниченного доступа[92]. В процессе привлечения к сотрудничеству они часто играют на чувства вербуемого, на его ощущениях о несправедливости, унижении и изоляции[93]. При этом, учитывается такие демографические факторы, как возраст, пол, религия, а также социальные или экономические обстоятельства.

В террористической деятельности вербовка тесно связана с радикализацией. Радикализация как процесс идеологической обработки способствует превращению завербованных рекрутов в людей, пронизанных экстремистской идеологией.

Наглядным примером радикализации, вербовки и привлечения к террористической деятельности являются материалы уголовного дела №19630 по обвинению гражданина Республики Таджикистан Р.Т. в совершении преступлений, предусмотренных ч.2 ст. 307 (2) (Участие в экстремистском сообществе) и ст. 401 (1) (Незаконное участие в вооруженном конфликте на территории других государств) Уголовного кодекса Республики Таджикистан. В ходе расследования было установлено, что гражданин Р.Т., находясь в трудовой миграции в городе Подольск Российской Федерации, в социальной сети «Фейсбук» познакомился с неким Муслимом, находящимся в Сирийской Арабской Республике. После неоднократных бесед на различные религиозные темы и по поводу якобы притеснения мусульман со стороны западных

[91] См.: Габриэль Вейманн. Террор в Интернете: новая арена, новые вызовы [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/? doc_id=31577354 (дата обращения: 25.07.2022).
[92] См.: Скотт Гервер и Сара Дейли, «Аль-Каида: отбор и вербовка террористов», в Справочнике по национальной безопасности McGraw-Hill, Дэвид Камьен, изд. (Нью-Йорк, McGraw-Hill, 2006) [Электронный ресурс]. – Режим доступа: https: www.clingendael.nl/publications (дата обращения: 09.03.2023).
[93] См.: Европейская комиссия, Экспертная группа по насильственной радикализации, «Процессы радикализации, ведущие к террористическим актам» (2008): [Электронный ресурс]. – Режим доступа: https: www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf (дата обращения: 09.03.2023).

государств, а также ознакомления с пропагандистскими материалами о священной войне «джихад», Муслим предложил ему приехать в Сирию и вступить в ряды международной террористической организации (МТО) «Исламское государство». Р.Т. согласился и по указанию Муслима 11 ноября 2019 года из г. Москвы вылетел в г. Стамбул Турецкой Республики, где его встретили, и он в сопровождении других членов названной МТО незаконно пересёк Турецко-сирийскую государственную границу и прибыл в Сирию. С приграничной территории Р.Т. и его попутчиков отвезли в г. Идлиб, где он, после прохождения военно-диверсионной подготовки, стал регулярно участвовать в террористических акциях МТО «Исламское государство» против легитимных Вооружённых сил Сирийской Арабской Республики[94].

Другим направлением использования Интернета является финансирование террористической деятельности путём прямых прошений о пожертвованиях, электронной коммерции и посредничества в благотворительных акциях.

Для прямых обращений используются веб-сайты, чат-группы и массовые рассылки в целях получения пожертвования от сторонников. Интернет-магазины, размещенные в веб-сайтах, могут быть использованы для сбора финансовых средств от продажи сторонникам книг, аудио- и видеозаписей и других товаров. Перевод полученных средств в основном осуществляется с помощью таких служб Интернета, как PayPal и Skype.

Также, нередко террористы под видом благотворительных целей осуществляют сбор финансов посредством Интернета, которых впоследствии используют в своей преступной деятельности[95].

Немалую пользу извлекают террористические организации от возможностей Интернета в таком компоненте, как подготовка террористов. В последние годы террористы используют Интернет в качестве виртуальной площадки для подготовки своих сторонников. С этой целью на отдельных платформах распространяют практические руководства в форме учебных пособий, аудио- и

[94] См.: Уголовное дело №19630 // Архив ГКНБ РТ.
[95] См.: Маура Конвей. Использование Интернета террористами и борьба с ними [Электронный ресурс]. – Режим доступа: https://www.academia.edu/ 34098438/International_Terrorism_Assignment (дата обращения: 09.03.2023).

видеоматериалов, различных информационных сообщений и рекомендаций. В частности, эти руководства содержат инструкции о том, как, например, присоединяться к террористам, как кустарным способом изготовить взрывные устройства, огнестрельное оружие или иные опасные для жизни и здоровья людей материалы, как подготовить и реализовать террористические акты.

В современном обществе Интернет превратился в действенный инструмент планирования и совершения террористических актов. С его помощью определяются потенциальная мишень и наиболее эффективные средства достижения террористических целей. В целях сокрытия следов своих преступных действий террористы при передаче информации часто используют анонимные сообщения. Для доставки анонимных сообщений используются обычные учётные записи абонентов электронной почты. То есть, создаётся черновик сообщения, который никуда не отправляется, но вместе с тем, другое лицо, владеющее паролем соответствующей электронной почты, оставив минимум электронных следов, может ознакомиться с содержанием черновика в любой точке мира. Также, существуют множество других технологий, затрудняющих установление содержания интернет-сообщений, а также их отправителей и получателей.

Необходимо признать, что ввиду отсутствия полноценного учёта, приведённые выше цифры, не раскрывают всю картину состояния преступности в данной области. Существует много других преступлений, при подготовке и совершении которых применяются возможности электронно-вычислительной техники, однако их учёт производится на общих основаниях и разделить необходимую информацию по ним от общей массы данных, не представляется возможным. Например, в последние годы информационно-телекоммуникационные технологии активно используются при совершении кражи, хищения, мошенничества, незаконного оборота наркотических средств, порнографических материалов и других преступлений.

Проведённое исследование позволяет сделать следующие выводы:

1. В современном обществе информационные технологии используются в механизме совершения большой части общественно-опасных деяний,

предусмотренных уголовным законом. Динамика развития данного вида преступности неразрывно связана с развитием информационных технологий. Сложившаяся обстановка осложняется тем, что внедрение современных технологий в преступную среду происходит быстрее, чем в деятельность правоохранительных органов и данное обстоятельство создаёт трудности для выявления и фиксации фактических данных по уголовным делам.

Понятие преступлений, совершаемых с применением информационных технологий, не ограничивается только противоправным вмешательством в работу ЭВМ, компьютерных программ, информационно-телекоммуникационных сетей и несанкционированной модификацией цифровых данных, а оно охватывает и иные противозаконные общественно-опасные деяния, совершённые посредством или с помощью компьютерной техники, компьютерных сетей и программ. В связи с этим, под преступлениями данной категории следует понимать противоправные деяния, запрещённые уголовным законом, наносящие ущерб или создающие угрозу нанесения ущерба интересам личности, общества и государства, совершаемые посредством цифровой и (или) электронно-вычислительной техники, компьютерных сетей и программ.

2. Учитывая масштабы распространения и общественную опасность преступлений рассматриваемого вида, для организации эффективного противодействия им, считаем целесообразным вводить централизованный статистический учёт преступлений данной категории и возложить данную функцию на Единый информационный центр, о создании которого высказался Основатель мира и национального единства – Лидер нации, Президент Республики Таджикистан уважаемый Эмомали Рахмон в своём Послании Маджлиси Оли Республики Таджикистан от 23 декабря 2022 года[96].

Также, существует необходимость в совершенствовании законодательства для упрощения процессуального оформления и фиксации следов преступлений, совершаемых с применением информационных технологий, о чём подробнее

[96] См.: Послание Президента Республики Таджикистан уважаемого Эмомали Рахмона «Об основных направлениях внутренней и внешней политики республики» (г. Душанбе, 23.12.2022 г.) [Электронный ресурс] – Режим доступа: https://president.tj (дата обращения: 04.02.2023).

расскажем ниже, в следующих параграфах.

1.3. Электронно-цифровые следы: сущность и механизм их образования на локальных и сетевых носителях

В криминалистической науке электронно-цифровые следы ещё мало разработаны и требуют глубокого изучения. Они появились, как качественно новые следы преступления, в связи с развитием информационных технологий и их внедрением в современное общество. Сущность данных следов сводится к отражению действительности в виде электронно-цифровой информации. В настоящее время количество электронно-цифровых следов становится больше, чем традиционных. Тенденция их роста отмечается не только при совершении общественно-опасных деяний против информационной безопасности, но подъём фиксируется и в процессе совершения других видов преступлений. В связи с этим, в современной криминалистической литературе определению электронно-цифровых следов, их именованию и механизму образования уделяется большое внимание.

В.А. Мещеряков для обозначения исследуемых следов использует термин «виртуальные следы» и полагает, что «это любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации на материальном носителе, в том числе в электромагнитном поле»[97]. В то же время, он отмечает, что электронно-цифровые (виртуальные) следы возникают в искусственно созданном пространстве, при их образовании фиксируются свойства математической модели наблюдаемого явления или процесса, связанного с расследуемым событием, они имеют дискретный цифровой вид отражения и представляют собой сложную структуру[98].

А.Б. Смушкин рассматривает виртуальные следы, как следы совершения любых действий по включению, созданию, открыванию, модификации и

[97] Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж: Изд-во Воронеж. гос. ун-та, 2002. – С. 104.

[98] См.: Агибалов В.Ю., Мещеряков В.А. Природа и сущность виртуальных следов / В.Ю. Агибалов, В.А. Мещеряков // Воронежские криминалистические чтения: сб. науч. трудов. – 2010. – Вып. 12. – С. 18 - 19;

удалению компьютерных данных.[99] Близкое по смыслу определение этим следам изложил Н.Н. Лыткин. Вместе с тем, он применяет выражение «компьютерно-технологические следы», под которыми предлагает понимать любую трансформацию связанной с преступлением компьютерной информации, возникающую в результате её уничтожения, копирования, блокирования и модификации[100]. На наш взгляд, данное определение не полностью охватывает сущность рассматриваемых следов и сужает их содержание, привязав только к общественно-опасным деяниям в сфере компьютерной информации. Поскольку эти следы могут образоваться при совершении преступлений любой направленности. К примеру, при осмотре мобильного телефона лица, подозреваемого в совершении преступления экстремистского характера, могут быть обнаружены электронно-цифровые следы в виде видеороликов с публичными призывами к осуществлению «джихада». В связи с этим, не совсем корректно говорить о следах данной категории, как о следах, образующихся при совершении преступлений против информационной безопасности.

С.Ю. Скобелином даётся абстрактное определение электронно-цифровым следам и в предложенном им понятии не усматриваются отличительные признаки названных следов, например, таких как наличие физического носителя, электронная форма отображения и возможность их передачи по каналам связи. С его точки зрения, электронно-цифровые следы – данные, содержащиеся в электронных устройствах, являющихся носителями цифровой информации[101]. Вместе с тем, в сформулированном В.Б. Веховым понятии этой группы следов вышеуказанные признаки присутствуют. Так, последний считает, что электронно-цифровой след «это любая криминалистически значимая компьютерная информация, находящаяся в электронно-цифровой форме, зафиксированная на

[99] См.: Смушкин А.Б. Виртуальные следы в криминалистике / А.Б. Смушкин // Законность. – 2012. – №8 (934). – С. 43.
[100] См.: Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: дис. … канд. юрид. наук. – Москва, 2007. – С. 57.
[101] См.: Скобелин С.Ю. Использование специальных знаний при работе с электронными следами / С.Ю. Скобелин // Российский следователь. – 2014. – №20. – С. 32.

материальном носителе с помощью электромагнитных взаимодействий либо передающаяся по каналам связи посредством электромагнитных сигналов»[102].

А.Н. Колычева предлагает под электронно-цифровыми следами понимать «криминалистически значимую информацию, выраженную посредством электромагнитных взаимодействий или сигналов в форме, пригодной для обработки с использованием компьютерной техники, в результате создания определенного набора двоичного машинного кода либо его преобразования, выразившегося в модификации, копировании, удалении или блокировании, зафиксированную на материальном носителе, без которого не может существовать»[103]. Несомненно, сформулированное А.Н. Колычевой определение весьма объемное по содержанию, привязано к криминалистической науке и тем самым вызывает интерес. Но, вместе с тем, следует знать, что эти следы могут найти свое отражение на материальных носителях не только путём набора двоичного машинного кода или его преобразования, но и могут возникнуть в результате записи протекающих в окружающем мире процессов посредством программных и технических средств без участия человека. Например, при фиксации сцены ограбления банка системой видеонаблюдения электронно-цифровые следы возникают не в процессе набора двоичного машинного кода или его модификации, а в результате записи происходящего события технической системой охраны.

В.А. Милашев указывает на термин «бинарные следы» и определяет их как «результат логических и математических операций с двоичным кодом»[104]. Е.Р. Россинская, обусловив формирование и преобразование данных следов спецификой функционирования информационных технологий, предлагает именовать такие следы информационно-технологическими[105]. В.В. Борисов

---

[102] См.: Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. – Волгоград: ВА МВД России, 2008. – С. 83.

[103] Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. … канд. юрид. наук. – Москва, 2018. – С.11.

[104] Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юр. наук. – М., 2004. – С. 18.

[105] См.: Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – №3-2. – С. 112.

сторонник использования термина «информационный след» для определения рассматриваемого вида следов, под которым понимает «информационную запись, сделанную на компьютерной технике подозреваемых в преступлении лиц с помощью специального программного средства и произведенную субъектом уголовно-процессуальной системы (например, следователем)»[106]. По нашему мнению, предложенное определение не раскрывает всю совокупность возможных источников криминалистически значимой информации и тем самым намного ограничивает сущность электронно-цифровых следов, так как «информационную запись», имеющую доказательственное значение, можно обнаружить, помимо компьютерной техники подозреваемых, и на электронно-вычислительных устройствах других участников уголовного судопроизводства (свидетелей, потерпевших, экспертов), а также различных юридических лиц, предприятий и учреждений, не заинтересованных в исходе уголовного дела.

Таким образом, можно констатировать, что на данный момент в научной литературе и научных кругах нет единого мнения относительно того, какой термин стоит применять к электронно-цифровым следам: «электронные», «бинарные», «цифровые», «электронно-цифровые», «компьютерные», «виртуальные» и т.п. По нашему мнению, главным вопросом здесь является определение сущности и содержания этих следов, а использование того или иного выражения не имеет существенного значения в процессе доказывания по уголовным делам. Вместе с тем, полагаем, что именовать их, как «электронно-цифровые следы» является более удачным.

Учитывая вышеизложенные мнения и позиции относительно понятия исследуемых следов, можно утверждать, что электронно-цифровые следы – это всякая связанная с расследуемым событием трансформация в информационном поле, зафиксированная в форме электромагнитных сигналов на материальном носителе и отражающая события действительности.

[106] Борисов В.В. Об особенностях фиксации информационных следов в практике защиты информации / В.В. Борисов // Известия Южного федерального университета. Технические науки. – 2009. – Т. 94. – №5. – С. 164

В криминалистической науке также вызывает большой интерес классификация электронно-цифровых следов. В научных источниках существует ряд оснований для классификации названной группы следов. Так, А.Г. Волеводз классифицирует их на основе материального носителя и выделяет следы на различных дисках, в запоминающих и периферийных устройствах, средствах связи и сетевых устройствах[107].

А.Ю. Семенов проводит классификацию электронно-цифровых следов на основании их местонахождения и различает следы на компьютере преступника и на компьютере жертвы[108].

Ряд авторов, в том числе Л.Б. Краснова и Ю.В. Гаврилин, при классификации берут за основу механизм следообразования и роль человека в возникновении электронно-цифровых следов и на этом основании выделяют первичные и вторичные следы. Те следы, которые образуются в результате воздействия пользователя в информационную среду, относят к первичным, а к числу вторичных определяют следы, инициированные компьютерной программой, без участия человека[109]. По похожему основанию, то есть по степени опосредованности пользователя в образовании следов, проводит классификацию также А.Г. Себякин. При этом, он первую группу следов называет непосредственными, а вторую – опосредованными[110].

Как известно из общей теории криминалистики, одним из распространенных критериев классификации следов является их разделение на материальные и идеальные. Материальные следы представляют собой материальные отображения события преступления и его механизма как результат воздействия на объекты живой и неживой природы. Идеальные следы – отображение события преступления в сознании человека как результат восприятия его органами чувств

---

[107] См.: Волеводз А.Г. Противодействие компьютерным преступлениям. – М., 2002. – С. 159-160.

[108] См.: Семенов А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации / А.Ю. Семенов // Сибирский юридический вестник. – 2004. – №1. – С. 53-55.

[109] См.: Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. – Воронеж, 2005. – С. 17; Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: автореф. дис. ... д-ра юрид. наук. – М., 2010. – С. 39.

[110] См.: Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. ... канд. юрид. наук. – Москва, 2021. – С. 42-43.

(зрением, слухом, обонянием и др.)[111]. В данном контексте дискуссионным остается вопрос отнесения электронно-цифровых следов к первому или второму виду следов. Некоторые авторы признают их материальными невидимыми следами[112]. Другие, основываясь на том, что данные следы не доступны для непосредственного восприятия человеком, то есть, воспринимать их можно опосредованно, относят их к идеальным следам[113].

На наш взгляд, опосредованность восприятия этих следов не может служить основанием для признания их идеальными следами. Поскольку отображение идеального следа имеет субъективный характер и обусловлено рядом влияющих на память человека факторов (возраст, физическое состояние, страх, тревога, стресс и т.п.), а воспроизведение следа, содержащегося на электронных носителях осуществляется путём реализации алгоритмов программ и выполнения определённых команд компьютерных устройств.

Вместе с тем, встречаются сторонники идеи отнесения электронно-цифровых следов в самостоятельную группу следов. Одним из авторов данной инициативы является В.В. Мещеряков, который определяя их как виртуальные следы, предлагает поставить данную категорию следов на промежуточную позицию между материальными и идеальными следами[114]. Данная позиция аргументируется тем, что в информационной среде при образовании виртуальных следов фиксируются не сами черты материального явления или процесса, а лишь

---

[111] См.: Криминалистика: учебник / Отв. ред. В.П. Лавров, Р.Х. Рахимзода, А.Ф. Волынский. – Душанбе, 2022. – С.52-53.

[112] См.: Россинская Е.Р., Шамаев Г.П. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники. Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства / Е.Р. Россинская, Г.П. Шамаев // Материалы междунар. науч.-практ. конф. – Иркутск, – 2014. – С. 320.; Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза / А.Б. Нехорошев. – Саратов, 2004. – С. 61., Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. – Волгоград: ВА МВД России, 2008. – С. 81-95.

[113] См.: Волеводз А.Г. Следы преступлений, совершённых в компьютерных сетях / А.Г. Волеводз // Российский следователь. – 2002. – № 1. – С. 10; Старикова М.Р. Значение электронных следов в расследовании преступлений. Обеспечение прав и свобод человека в уголовном судопроизводстве: организационные, процессуальные и криминалистические аспекты / М.Р. Старикова // Сб. статей по мат. междунар. студ. науч.-практ. конф. – 2017. – С. 233.

[114] См.: Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронежского государственного ун-та. – 2002. – С. 94-119.

свойства их математической модели[115].

В.Ю. Агибалов отмечает, что «фактически следа в традиционном криминалистическом его понимании нет, имеется только цифровой образ, на основании которого можно сформировать сигнал или некий физический процесс (звук, изображение, набор компьютерных данных), подобный (с определённой степенью схожести) исходному следообразующему объекту»[116].

Пожалуй, не стоит согласиться с утверждением В.Ю. Агибалова и необходимо заметить, что в соответствии с криминалистическим учением о следообразовании, полное отражение следообразующего объекта в следовоспринимающем невыполнимо. Всякая трансформация, происходящая в следовоспринимающем объекте, отражает лишь отдельные стороны следообразующего объекта. В этом смысле след отражает какую-либо сторону отражаемого объекта и электронно-цифровой след не считается в данном понимании особенным. К тому же, согласно учению о диалектическим тождестве, след вовсе не может быть полностью идентичен отражаемому объекту, любой предмет может быть тождественен только себе[117].

Неоднозначно выглядит позиция В.Б. Вехова относительно природы происхождения электронно-цифровых следов. С одной стороны, он считает, что «электронные следы являются материальными невидимыми следами», с другой - предлагает относить их в самостоятельную группу: «С определённой долей научной абстракции в системе криминалистической классификации электронные следы целесообразно выделить в самостоятельную группу и условно расположить между материальными и идеальными следами[118]».

Принимая во внимание вышеизложенное, и тот факт, что при образовании электронно-цифровых следов массив памяти электронного носителя, выступая в качестве следовоспринимающего объекта, отражает в себе изменения, связанные

---

[115] См.: Агибалов В.Ю., Мещеряков В.А. Природа и сущность виртуальных следов / В.Ю. Агибалов, В.А. Мещеряков // Воронежские криминалистические чтения: сб. науч. трудов. – 2010. – Вып. 12. – С. 18.

[116] Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: дис. ... канд. юрид. наук. – Воронеж, 2010. – С. 74.

[117] См.: Белкин Р.С. Курс криминалистики. В 3 т. Т. 2. Частные криминалистические теории. – М.: Юристъ, 1997. – С. 257

[118] Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. – 2016. – №2 (46).– С. 17.

с событием преступления, необходимо рассматривать их как материальные следы.

Доступ к данным, содержащимся на локальных носителях, происходит на месте их нахождения. К числу локальных электронных носителей можно отнести флэш-карты (универсальные перезаписываемые носители информации), CD-диски (CD-ROM – предназначен для хранения и считывания предварительно записанной на него цифровой информации, CD-R – используется для разовой записи, хранения и считывания информации, CD-RW приспособлен для записи, перезаписи и хранения сведений), DVD-диски (применяется для хранения видеоизображений и больших объёмов разных видов цифровой информации - текст, звук, изображение), съёмные жесткие диски, жесткие диски компьютеров, встроенная память ноутбуков, планшетов, сотовых телефонов, электронных книг и прочих устройств, дискеты и др.

Содержащуюся на локальных носителях информацию можно разделить на две группы: метаданные и искомые данные. К метаданным относятся идентифицирующие электронно-цифровую информацию сведения. Таковыми являются наименование файла, данные о времени создания, модификации, сеансах обращения к нему и т.п. Искомыми данными являются сведения, касающиеся расследуемого преступления, а также, не относящаяся в предмет доказывания информация. Какое бы событие или действие не произошло в информационной системе, сведение об этом фиксируется в автоматическом режиме на электронных носителях.

Доступ к информации, содержащейся на сетевых носителях, происходит дистанционно. Сетевые носители состоят из серверов, соединённых между собой посредством компьютерных сетей. Компьютерные сети бывают локальной, региональной, корпоративной и глобальной. Эти сети отличаются друг от друга в зависимости от зоны их охвата. Так, например, локальная сеть объединяет компьютеры, в основном, в пределах одного помещения, здания либо учреждения. А глобальная сеть, то есть Интернет, объединяет множество локальных сетей и ЭВМ, которые далеко расположены друг от друга.

В современной юридической литературе встречается множество определений понятия Интернет. Так, по мнению Е.С. Андрющенко, «Интернет – это глобальная децентрализованная система информационно-телекоммуникационных сетей, соединяющих на основе единых протоколов различные типы компьютеров»[119].

Согласно позиции И.М. Рассолова, «глобальная сеть (Интернет) – это новое международное пространство человеческого самовыражения, пересекающее любые границы, децентрализованное пространство, которым никакой субъект, никакое государство полностью не владеет и не управляет»[120].

В словаре терминов Интернет даётся следующее его понятие: «Интернет – глобальная информационная сеть, части которой логически взаимосвязаны друг с другом посредством единого адресного пространства, основанного на протоколе TCP/IP»[121].

В Республике Таджикистан определение Интернет нашло свое законодательное закрепление в Правилах предоставления услуг Интернета на территории Республики Таджикистан (утверждены Постановлением Правительства, №389 от 08.08.2001 г.). Согласно п.5 настоящих Правил «Интернет – совокупность различных телематических служб и служб передачи данных, которая базируется на различных физически неоднородных коммуникационных сетях, объединенных между собой в единую логическую архитектуру, и построенной на основе международных протоколов передачи данных». Относительно данного нормативного определения мы солидарны с У.А. Меликовым, который считает, что здесь «Интернет рассматривается узко – как «служба передачи данных» и оно не имеет ни познавательного, ни регулятивного характера»[122].

---

[119] Андрющенко Е.С. Интернет-отношения: государственное регулирование и саморегулирование: автореф. дис. … канд. юрид. наук. – Саратов, 2010. – С.9.

[120] См.: Рассолов И.М. Право и Интернет. Теоретические проблемы. – М.: Изд-во НОРМА, 2003. – С. 92.

[121] Словарь терминов Интернет [Электронный ресурс].–Режим доступа: URS: http/your-hosting.ru/terms/i/internet/ (дата обращения: 25.04.2022).

[122] Меликов У.А. Правовой режим объектов гражданских прав в интернете: монография. – Душанбе, 2017 – С.17-18.

Следует отметить, что большинство авторов научных работ по исследованию проблем глобальной сети, при определении термина «Интернет» делают акцент на три основные его элемента: сеть, компьютеры и протоколы. Наличие каждого элемента считается непременным, ибо при отсутствии хотя бы одного из них, Интернет не может существовать.

Основу глобальной сети Интернет составляют мощные компьютерные серверы, к которым посредством телекоммуникационных сетей подключены миллионы компьютеров и цифровых устройств.

Для раскрытия механизма следообразования в глобальной сети Интернет, необходимо иметь представление о протоколах передачи данных, наличие которых является одним из обязательных условий её функционирования.

Протоколы представляют собой общие правила обмена информацией между пользователями. Они бывают базовыми и прикладными. Базовые протоколы предназначены для пересылки электронных данных и называются они TCP (Transmission Control Protocol) и IP (Internet Protocol).

Прикладные протоколы необходимы для работы различных служб сети Интернет. Например, протокол HTTP предназначен для передачи гипертекстов, FTP – для передачи файлов, POP и SMTP – отвечают за почтовые соединения, а TELNET – необходим для удаленного доступа.

В процессе функционирования сети Интернет протоколы TCP и IP служат объединяющим элементом компьютерных сетей. Каждой подключённой технике к сети Интернет присваивается адрес, который состоит из чисел. Присвоенный номер называется IP-адресом, он является уникальным для конкретного сервера или компьютера и не может быть присвоен другим компьютерным средствам.

Большинством учёных механизм возникновения электронно-цифровых следов рассматривается с точки зрения теории отражения. Отражение происходит вследствие воздействия следообразующего объекта на следовоспринимающий. В.Б. Вехов совершенно верно отмечает, что «Отражением преступных действий являются следы. Отражение присутствует всегда, когда происходит взаимодействие двух и более материальных объектов – объектов

следообразования»[123]. В данном понимании результатом отражения считается изменение в окружающей обстановке и в предмете преступного посягательства, являющимися отражающими объектами.

Механизм следообразования на электронных носителях информации отличается от следообразования объектов материального мира. В материальном мире участниками процесса следообразования выступают «следообразующий (отражаемый)» и «следовоспринимающий (отражающий)» объекты, в результате контакта которых рождается след[124]. Электронно-цифровая информация не имеет пространственной формы и применить к ним эти понятия в том классическом понимании, которое принято в криминалистической науке, не приемлемо. Эти следы отражаются на электронных носителях в виде дискретных сигналов, у них отсутствует внешнее строение, воспринимать их возможно только с использованием технических средств, к ним можно удаленно получить доступ и дистанционно модифицировать их.

Следы рассматриваемой категории представляют собой сложную структуру. Они могут найти своё отражение в результате взаимодействия следообразующих объектов как на одном, так и на двух и более электронных носителях, объединённых в единую информационную систему или сеть.

Электронно-цифровые следы в информационных сетях представляют собой данные о протекании информации по каналам связи между устройствами (компьютерами, смартфонами и т.д.), подключёнными к определённой сети. Информационные системы фиксируют эти данные в автоматическом режиме в так называемых log-файлах. Сведения обо всех действиях и событиях в системе регистрируются в этих файлах. Они могут содержать информацию о том, кто инициировал событие (действие), время, какие IP-адреса и телефонные номера были использованы, скорость передачи сообщения, какие протоколы использовались и др.

---

[123] Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. – 2016. – №2 (46). – С. 12.

[124] См.: Белкин Р.С. Курс криминалистики. В 3 т. Т. 2. Частные криминалистические теории. – М.: Юристъ, 1997. – С. 61.

В.Б. Вехов утверждает, что «следами-отображениями в электронной среде являются фиксируемые компьютерной системой изменения объектов в результате взаимодействия, и благодаря алгоритмам обработки информации возможно определение причин возникновения следа и инструментов, создавших наблюдаемые изменения»[125].

А.Г. Себянин справедливо замечает, что при механизме образования названных следов в качестве отражаемого объекта выступает пользователь, а отражающего объекта – электронно-вычислительная система. Взаимодействие этих объектов возникает посредством команд и сигналов, которые могут быть задействованы пользователем или инициированы программным обеспечением компьютерной системы. При этом данный автор считает, что системное программное обеспечение – следообразующий объект, а массив памяти компьютерного устройства – следовоспринимающий объект[126].

Ряд авторов при исследовании данной проблемы приходят к аналогичным выводам и, по нашему мнению, с их утверждениями в части, касающейся следовоспринимающего объекта, стоит согласиться. Так, В.Б. Вехов, Б.П. Смагоринский и С.А. Ковалев считают, что носитель отражённой вследствие взаимодействия информации и есть следовоспринимающий объект[127]. Ж.Ю. Кабанова полагает, что при механизме формирования исследуемых следов матрица или аналоговый цифровой преобразователь и есть следообразующий объект, а электронный носитель информации считается следовоспринимающим объектом[128]. Похожую позицию занимает и С.Д. Долгинов, который утверждает, что «любые действия с компьютерными или иными программными устройствами получают свое непосредственное отражение в их памяти»[129].

---

[125] См.: Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. – Волгоград: ВА МВД России, 2008. – С. 87.

[126] См.: Себянин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. … канд. юрид. наук. – Москва, 2021. – С.14, 15, 28.

[127] См.: Вехов В.Б., Смагоринский Б.П., Ковалев С.А. Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. – 2016. – №2 (46). – С. 12.

[128] Кабанова Ж.Ю. Электронный след в уголовно-исполнительной системе / Ж.Ю. Кабанова // В сборнике: Уголовно-исполнительная система сегодня: взаимодействие науки и практики. Мат. науч. - практ. конф. – 2016. – С. 123.

[129] Долгинов С.Д. Следы электронных устройств в криминалистике / С.Д. Долгинов // В сб.: Шестой пермский конгресс ученых-юристов: Российская национальная правовая система: современное состояние, тенденции и

Тем самым, мы полагаем, что в механизме образования цифровых следов основой считается их электронное отображение в памяти электронных носителей информации, информационных системах, серверах, компьютерных сетях, каналах передачи информации. От того, как была спроектирована данная среда, какие стандарты и формы обработки и взаимодействия были разработаны, зависит размер и величина изымаемой доказательственной информации. Вместе с тем электронно-цифровой след как сложная информационная структура может сохранить в себе как сведения об общественно-опасном событии, так и иную вспомогательную информацию, позволяющую определить его принадлежность к конкретной цифровой среде.

На следообразование в компьютерных сетях влияют такие факторы, как виды каналов передачи данных, типы технологического оборудования, используемые потерпевшим или преступником, операционные системы, программные средства, наличие устройств безопасности, уровень технических знаний участника уголовного судопроизводства по вопросам использования телекоммуникационных сетей и т.п.

Ввиду того что в информационном пространстве следообразующие объекты не имеют физическую форму, электронно-цифровые следы формируются в результате взаимодействия дискретных сигналов и среды в виде электромагнитных изменений, которые фиксируются на электронных носителях компьютерных или цифровых устройств. Данные изменения не доступны для непосредственного восприятия человеком и для их выявления и фиксации требуется использование технических и программных средств. В то же время, электронный носитель может иметь как физическую форму (например, флэш-карты, компакт-диски, жёсткие диски и др.), так и не иметь её (например, беспроводные каналы связи).

Обобщая рассмотренные выше основные вопросы, касающиеся сущности электронно-цифровых следов и механизма их формирования, можно прийти к следующим выводам:

перспективы развития. Мат. междунар. науч. - практ. конф. – 2015. – С. 266.

1. Для содержательного определения следов, образующихся на локальных и сетевых электронных носителях, необходимо использовать термин «электронно-цифровые следы» и под ним следует понимать всякую связанную с расследуемым событием трансформацию в информационном поле, зафиксированную в форме электромагнитных сигналов на материальном носителе и отражающую события действительности.

Электронно-цифровые следы по своей сути схожи со многими невидимыми материальными следами и имеют материальную природу происхождения. К ним можно отнести файлы, созданные пользователем или записанные программным обеспечением, электронная переписка, история интернет-запросов, журнал вызовов, файлы реестра операционной системы, метаданные пользовательских файлов и пр.

2. В механизме формирования рассматриваемой категории следов основой считается электронное отображение изменений, связанных с событием преступления. Ввиду того, что в информационном пространстве следообразующие объекты не имеют физическую форму, электронно-цифровые следы формируются в результате взаимодействия дискретных сигналов и среды в виде электромагнитных изменений, которые фиксируются на электронных носителях компьютерных или цифровых устройств.

Для установления и фиксации следов названной категории надлежит выявить пересекающееся взаимосоединение между образовавшимися изменениями, вычислительной системой и оставившим свое отражение действием или событием.

3. При механизме следообразования рассматриваемой группы следов в качестве отражающего объекта выступает вычислительная система, а отражаемого – пользователь. Инструментами отражения могут быть команды и электромагнитные сигналы, активизированные пользователем или прикладным программным обеспечением. Следообразующим объектом считается системное программное обеспечение, а в качестве следовоспринимающего объекта выступает массив памяти соответствующего устройства. Механизм образования

данных следов зависит от конструкции информационного пространства, в котором они запечатлены.

ГЛАВА 2. КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ЭЛЕКТРОННО-ЦИФРОВОЙ ИНФОРМАЦИИ С ЛОКАЛЬНЫХ И СЕТЕВЫХ НОСИТЕЛЕЙ

2.1. Тактические особенности обнаружения и фиксации доказательственной электронно-цифровой информации, хранящейся на локальных и сетевых носителях

В условиях цифровизации общества и повсеместного внедрения цифровых технологий в протекающие в нём процессы, роль и значение доказательственной электронно-цифровой информации при расследовании уголовных дел неуклонно растет, и данное обстоятельство обуславливает детальное изучение особенностей её обнаружения и фиксации.

Обнаружение и фиксация доказательственной информации являются стадиями процесса собирания доказательств. Собирание доказательств, в свою очередь, является элементом процесса доказывания, наряду с проверкой и оценкой доказательств.

По мнению Р.С. Белкина, поиск, обнаружение, фиксация и изъятие информации являются составными элементами процесса собирания доказательств. При этом, он подчёркивает, что эти действия должны быть осуществлены предусмотренными уголовно-процессуальным законодательством средствами[130]. Обнаружение доказательств заключается в деятельности органов предварительного следствия, направленной на отыскание и выявление фактических данных, связанных с событием преступления и имеющих криминалистическое значение[131]. А фиксация, как составляющая часть названного процесса, состоит в том, что выявленные фактические данные должны быть закреплены и запечатлены предусмотренными законом способами, то есть в протокольной форме[132]. Здесь нам предстоит раскрывать сущность указанной деятельности применительно к электронно-цифровым

[130] См.: Белкин Р.С. Криминалистическая энциклопедия. 2-е изд., доп. – М.: Мега-трон XXI, 2000. – С. 211.
[131] См.: Белкин Р.С. Собирание, исследование и оценка доказательств. Сущность и методы. – М.: Наука, 1966. – С. 29.
[132] См.: Винберг А.И. Криминалистика. Вып. 1: Введение в криминалистику. – М., 1950. – С. 8.

доказательствам.

Анализ Уголовно-процессуального кодекса Республики Таджикистан и правоприменительной практики показал, что в настоящее время процессуальные средства собирания электронно-цифровых доказательств, содержащихся на локальных и сетевых носителях, не разработаны и данный процесс осуществляется правоохранительными органами в рамках существующих отдельных следственных действий. Так, к примеру, в ходе анкетирования следователей органов национальной безопасности Республики Таджикистан удалось выяснить, что основными процессуальными действиями, в рамках которых осуществляется собирание электронных доказательств, являются осмотр места происшествия, осмотр предметов, обыск, личный обыск, выемка и наложение ареста на почтово-телеграфные отправления**.** При этом, респонденты ответили, нередко эти доказательства представляются органам следствия с результатами оперативно-розыскной деятельности.

В современных условиях расследование преступлений, в механизме совершения которых используются информационные технологии, основано на получении криминалистически значимых данных в виде сообщений, текстовых и мультимедийных файлов, переписки в социальных сетях, сведений о соединениях абонентов и т.п.

Практика показывает, что нередко подобные данные, становясь весомым и неопровержимым доказательством по уголовным делам, способствуют установлению истины и привлечению к уголовной ответственности лиц, совершивших общественно-опасные деяния.

Данный аргумент ярко иллюстрируется материалами уголовного дела №15185, возбужденного в отношении Н.С.Х. по признакам преступления, предусмотренного ч.2 ст. 307 (3) УК Республики Таджикистан. Так, следствием было установлено, что обвиняемый, участвуя в деятельности террористическо-экстремистской организации, в период с 2018 г. по 2021 г. посредством своей интернет-страницы в «Фейсбуке» под названием «Suraj Nazar» систематически распространял пропагандистские материалы данной организации. В ходе осмотра

названной интернет-страницы в его смартфоне марки «Samsung G 7 prime» были обнаружены и зафиксированы все распространённые обвинаемым видеоролики и текстовые файлы с публичными призывами к осуществлению экстремистской деятельности. Данная информация, зафиксированная в протоколе осмотра, послужила основанием для начала уголовного преследования и в дальнейшем стала основным доказательством установления вины Н.С.Х. в содеянном[133].

Тактические приёмы обнаружения и фиксации электронно-цифровых следов во многом обусловлены определённой следственной ситуации, сложившейся на конкретный момент расследования. Анализируя следственную практику, из общего многообразия можно выделить следующие типичные следственные ситуации:

1) Органы следствия владеют данными о месте совершения уголовно наказуемого деяния, где находится электронное устройство, содержащее доказательственную информацию.

2) Имеются сведения о наличии электронно-цифровых следов в личных (персональных) устройствах участников уголовного судопроизводства, в частности, свидетеля, потерпевшего, подозреваемого либо обвиняемого. Возникновение подобной следственной ситуации возможно как в случае применения электронного устройства в качестве средства реализации преступных замыслов (к примеру, в ходе расследования преступления об участии в экстремистской деятельности, в мобильном устройстве марки «Redmi 9» обвиняемого Д.Д. обнаружены дискредитирующие политику государства и Правительства Республики Таджикистан материалы, направленные им для использования в агитационной работе в адрес запрещенного экстремистского интернет-сайта[134]), так и в случае, когда устройство не имеет прямого отношения к совершённым преступным действиям (например, в ходе совершения вымогательства соучастником преступления осуществлялась видеозапись).

[133] См.: Уголовное дело №15185 // Архив ГКНБ РТ.
[134] См.: Уголовное дело №23139 // Архив ГКНБ РТ.

3) Следственные органы имеют в своем распоряжении информацию относительно лица, причастного к совершению криминального деяния, следы которого сохранились в памяти электронного носителя используемого им компьютерного или цифрового устройства. Например, человек совершает преступление, связанное с незаконным оборотом наркотических средств и при сбыте наркотиков использует мобильное устройство связи для определения условий и места совершения сделки с потенциальным покупателем. В результате исследования детализации телефонных звонков участников данной сделки можно установить передвижение и местонахождение каждого из них в определённый момент времени. Таким образом можно опровергнуть возможные доводы сбытчика наркотических средств о том, что он в момент совершения преступления не находился в районе совершения преступления и не имел контакта с лицом, задержанным с вещественными доказательствами.

4) Имеется информация о размещении запрещённых материалов на ресурсах сети Интернет, и при этом, отсутствуют данные о лице, распространившем эти материалы, и месте совершения данного деяния.

Отмеченные выше следственные ситуации могут сочетаться друг с другом или преобразоваться из одной в другую. Например, при наличии сведений о месте совершения общественно-опасного деяния, может быть получена информация о личности подозреваемого.

Следственные ситуации объединяют взаимосвязанные тактические цели собирания электронно-цифровых следов. Эти цели заключаются в установлении электронного носителя, обнаружении на нём электронно-цифровых следов, их фиксации и исследовании.

В техническом плане работа с электронными носителями состоит из извлечения данных, превращения их в вид, подходящий для обработки, и анализа изъятой информации в целях получения дополнительных сведений о совершённом преступлении[135].

---

[135] См.: Гончаров А.В. Использование возможностей современных инновационных технологий при исследовании цифровых устройств мобильной связи и компьютерных носителей информации при расследовании преступлений / А.В. Гончаров // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития. Мат.

Следует заметить, что процессуальные действия, направленные на извлечение и превращение (преобразование) следов рассматриваемой категории в подходящий для обработки вид, в большинстве случаев осуществляются в едином цикле, которые, в свою очередь, образуют тактическую цель по обнаружению и фиксации этих следов. Относительно анализа полученной информации важно помнить, что наличие некоторой категории информации является криминалистически важным фактом для органов следствия, например, копия финансового документа о хищении денежных средств. А некоторые категории информации, после их обнаружения и фиксации, необходимо будет анализировать, сопоставить с другими данными, имеющимися в распоряжении следствия. Отсюда, в зависимости от конкретной ситуации, получение дополнительных данных посредством анализа обнаруженных следов выступает в качестве самостоятельной цели тактического воздействия.

При реализации цели по установлению электронного носителя решаются задачи, направленные на обнаружение электронно-цифровых следов преступной деятельности и нахождения интересующего следствие индивида в определённом месте.

Для решения задачи по обнаружению следов преступлений исследованию подлежат персональные и служебные устройства, в том числе компьютеры, смартфоны, цифровые диктофоны, игровые автоматы и т.п., и серверы систем видеофиксации.

Детализация телефонных соединений, анализ метаданных файлов и данных специализированных приложений, а также просмотр записей систем видеофиксации позволяют установить следы нахождения определённого участника уголовного судопроизводства в конкретном месте.

Тактическая цель по обнаружению на электронном носителе следов преступления и их фиксации достигается посредством решения задач, направленных на выявление пользовательских файлов, обнаружение

Междунар. науч.-практ. конф. – М.: Московская академия Следственного комитета Российской Федерации, 2019. – С. 186-201.

специализированного программного обеспечения, установление активности абонента в сети сотовой связи или сети Интернет, а также получение детализаций мобильных телефонных соединений участников уголовного судопроизводства с указанием базовой станции, оказавшей сервис, от операторов мобильной связи.

К пользовательским файлам относятся текстовые, мультимедийные, в том числе графические, видео, аудио и другие файлы. В данном случае криминалистическую значимость может иметь как непосредственное содержимое (контент) файла, так и метаданные (даты создания, изменения, удаления файла, источник его получения и создания, координаты местности и пр.).

Заключительной типичной целью тактического воздействия является исследование выявленных электронно-цифровых следов. Здесь, в первую очередь, исследуется содержимое файлов на предмет относимости к совершенному преступлению, например, видео или текст, содержащие призывы к осуществлению экстремистской деятельности, изображение фиктивного коммерческого договора, электронная версия платёжного поручения о переводе денег согласно названному договору и пр.

Путём анализа сведений об активности абонента в сети сотовой связи или сети Интернет можно установить ранее неизвестных следствию соучастников совершенного общественно-опасного деяния, потерпевших, свидетелей, и тем самым, способствовать полноте и всесторонности расследования уголовного дела.

В следственной ситуации, когда участник уголовного судопроизводства установлен и органам предварительного следствия известен его абонентский номер (номера), следователь или другое должностное лицо, ведущее расследование, на основе анализа информации о соединениях абонента может установить перемещение интересующего следствие лица в определённом интервале времени, а также определить его возможное нахождение в установленное время в конкретном месте. Данная тактическая задача, которая именуется геолокацией, решается благодаря тому, что в соответствии с принципами построения сетей связи, каждая базовая станция обеспечивает сотовой связью определённую территорию и имеет уникальный идентификатор,

который при осуществлении соединения отражается в детализации абонентского номера. Вместе с тем, точность геолокации в большей степени зависит от географии местности. В городских густонаселённых районах зона обслуживания станций может составлять 200-400 метров, а в районах с меньшим количеством жителей, транспортных магистралях – несколько километров.

При развитии исходной следственной ситуации в бесконфликтном русле, то есть полном или частичном совпадении интересов участников уголовного судопроизводства[136], в случае наличия сведений о месте совершения криминального деяния, плодотворным считается реализация тактического комплекса, заключающегося в проведении следующих процессуальных действий.

1. Допрос участника уголовного судопроизводства. Главной задачей допроса является выявление электронных носителей следов расследуемого уголовно наказуемого деяния, а также логинов и паролей от информационных ресурсов. Данное следственное действие необходимо произвести при участии специалиста в области информационно-телекоммуникационных технологий. Его участие позволит эффективно проводить допрос, получить исчерпывающую информацию у допрашиваемого лица о совершённом преступлении и спланировать дальнейшие действия органов уголовного преследования. На этот счёт А.В. Платёнкин верно отмечает, что в связи со специфическим характером большой части информации, относящейся к предмету допроса, на его подготовительном этапе следователь, проконсультировавшись со специалистом, должен уточнить ряд сложных моментов относительно принципов образования следов работы пользователя на компьютерной технике и совместно с ним сформулировать вопросы в каждом конкретном случае[137].

2. Осмотр места происшествия. На данном этапе выявляются электронные носители цифровых следов, а также следы присутствия того или иного заподозренного лица на месте совершения преступления, то есть на месте

---

[136] См.: Ратинов А. Р. Судебная психология для следователей. – М.: Юрлитинформ, 2008. – С. 157.

[137] Платёнкин А.В. Особенности использования электронных доказательств при проведении допроса подозреваемого [Электронный ресурс]. – Режим доступа: https: //cyberleninka.ru/article/n/ osobennosti-ispolzovaniya-elektronnyh-dokazatelstv-pri-provedenii-doprosa-podozrevaemogo (дата обращения: 25.08.2023).

нахождения компьютерных или иных персональных устройств. Участие специалиста при этом является важным фактором успешного производства осмотра.

Впоследствии исходная следственная ситуация превращается в ситуацию, при которой имеются сведения о наличии электронно-цифровых следов в личных (персональных) устройствах конкретного участника уголовного судопроизводства. В таком случае эффективным является следующий комплекс следственных действий.

3. Осмотр электронных носителей в рамках осмотра места происшествия. Данное следственное действие может быть произведено как с участием специалиста, так и самостоятельно следователем, с использованием собственных знаний в области компьютерной техники. Вместе с тем, рекомендуется привлекать специалиста на данном этапе, так как это позволит оценить риски утраты следов и принять решение об изъятии электронных носителей. В ходе осмотра решаются задачи по обнаружению пользовательских файлов, интернет-активности пользователей и специализированного программного обеспечения.

При осмотре электронно-цифровых носителей для обнаружения следов в электронных документах традиционно используется метод контекстного поиска. Данный метод может быть применён как с привлечением специалиста, так и самим следователем самостоятельно. Контекстный поиск заключается в том, что в процессе осмотра на основе анализа документов устанавливаются ключевые слова и путём их ввода осуществляется выискивание интересующих следствие документов. Такими словами могут быть наименование организации, имена её должностных лиц, название документа, предмет преступного посягательства и пр.

На этой стадии, в случае обнаружения достаточных искомых данных и решения всех вопросов, связанных с осмотром, изъятие электронного носителя не производится.

4. В случае, если при осмотре электронного носителя не выявлены электронно-цифровые следы преступления, в ходе осмотра места происшествия принимается решение об изъятии данного носителя для последующего

исследования. В зависимости от следственной ситуации изъятие может быть произведено, также в рамках обыска или выемки. Последующий детальный осмотр осуществляется в рамках осмотра предметов. При этом для повышения вероятности выявления криминалистически значимой информации важным считается привлечение специалиста в области информационных технологий. Также, в зависимости от разновидности получаемой информации и специфики расследуемого дела, на этом и предыдущем этапах, помимо специалиста названной категории, в следственном действии не исключается привлечение специалистов других областей (например, экономиста, психолога, искусствоведа и др.).

5. Исследование выявленной электронно-цифровой информации. Оно проводится в основном для решения типичных задач по выявлению других возможных соучастников преступления, свидетелей, потерпевших, а также иных эпизодов преступной деятельности.

6. Назначение судебной компьютерно-технической экспертизы. Необходимость в этом возникает тогда, когда в рамках осмотра не получена исчерпывающая информация. Данное тактическое действие подробно рассмотрим ниже, в параграфе 2.3 настоящей главы.

7. Производство обыска. Данный элемент тактического комплекса осуществляется в основном в том случае, когда следственная ситуация развивается в конфликтном русле, то есть когда участник уголовного судопроизводства не сотрудничает со следствием, всячески скрывает следы преступных действий, уничтожает их или иным образом оказывает противодействие органам предварительного следствия. Участие специалиста соответствующего профиля в процессе производства обыска является важным фактором успешного достижения его целей.

Следственная ситуация не является неподвижной и в нашем случае, при наличии данных о месте совершения преступления, чаще всего переходит в ситуацию, когда возникает необходимость в выявлении виновных лиц, установлении их местонахождения, выяснении и анализе контактов

(информационных связей) участников уголовного судопроизводства.

В данном случае эффективным является осуществление следующего тактического комплекса, направленного на добывание данных о соединениях между абонентами и абонентскими устройствами[138].

8. Оценка радиоэлектронной обстановки. Она позволяет получить сведения о наземных станциях операторов сотовой связи, предоставляющих услуги связи в определённой местности, на основе которой представляется возможным определить местонахождение интересующего следствие абонента и его телефонные соединения. Данное действие следует произвести с участием соответствующего специалиста и оформлять протоколом осмотра места происшествия либо протоколом осмотра местности**.**

Следует отметить, что оценка радиоэлектронной обстановки в основном проводится в случаях, когда в распоряжении следствия не имеются сведения о лицах, совершивших преступления. Главной задачей здесь является установление круга абонентов, среди которых могут быть лица, причастные к расследуемому событию. Решение этой задачи достигается путём анализа данных всех соединений, совершённых посредством определённой базовой станции, то есть осуществляется биллинг сотовых соединений. Оценка радиоэлектронной обстановки проводится с учётом установления вероятных мест нахождения подозреваемых лиц в момент совершения преступления и по всем операторам сотовой связи, действующим в конкретной местности, представляющей интерес для следствия. В случае, если установлены несколько значимых для следствия мест (например, место вооружённого нападения на инкассаторов, место обнаружения инкассаторского автомобиля, банк, денежные средства которого были ограблены и т.п.), то необходимо произвести данный тактический комплекс в каждом из известных мест и запросить у операторов сотовой связи информацию обо всех соединениях, осуществлённых посредством установленных базовых станций. Затем, владея информацией о времени совершения преступления,

[138] См.: Антонов О.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами в России: сущность, этапы и пути совершенствования тактического обеспечения / О.Ю. Антонов // Вестник Томского государственного университета. – 2020. – №459. – С. 221-229.

сопоставляются полученные биллинговые данные и устанавливается нахождение абонентов в том или ином месте в определённое время. Органы следствия в результате сравнения получат список абонентов, возможно причастных к совершённому преступлению. Вместе с тем, в зависимости от ряда факторов (густонаселённости района, оживлённости трассы и т.п.) этот список может содержать 10-15 абонентов, а может и 100-200. При анализе, всесторонней проверке абонентов и сопоставлении полученных сведений с другими данными уголовного дела, данный список может сужаться и позволит выйти на конкретных лиц, причастных к расследуемому событию.

9. Запрос у операторов мобильной связи сведений о детализациях телефонных соединений установленных участников уголовного судопроизводства, а также информации о месторасположении сервисных базовых станций. Данный комплекс может дать органам предварительного следствия большой объём информации о совершенном преступлении и иных обстоятельствах, подлежащих установлению. В частности, это позволит выявить лиц, контактирующих с подозреваемым, среди которых могут быть другие соучастники преступления, а также иных лиц, осведомленных о совершенном общественно-опасном деянии.

10. Исследование сведений, полученных у операторов мобильной связи. Оно может проводиться как самим следователем, так и специалистом, это зависит от стоящих перед исследованием задач. Специалист свои рассуждения относительно исследованных сведений может представить в форме заключения.

При следственной ситуации, когда имеются сведения о наличии в персональных устройствах участника уголовного судопроизводства электронно-цифровых следов, считается целесообразным совершение действий, последовательность которых описана выше в пунктах 3-6.

В следственной ситуации, при которой в наличии имеется информация о лицах, причастных к криминальным действиям, и при этом она развивается в конфликтном русле, целесообразным считается реализация тактического комплекса, изложенного выше в пунктах 7-10.

Следует отметить, что при осуществлении вышеуказанных тактических комплексов необходимо соблюдать основные принципы криминалистического исследования электронных носителей информации. Так, Е.Р. Россинская предлагает соблюдать четыре базовых принципа при проведении процессуальных действий, связанных с исследованием электронных носителей:

– Принцип неизменности информации, то есть хранящаяся на изымаемых носителях электронно-цифровая информация не должна изменяться;

– Принцип обязательного изъятия носителя. Данный принцип означает, что исследование электронно-цифровой информации на месте обнаружения носителя допускается только тогда, когда нет возможности изъять его для производства судебно-компьютерной экспертизы;

– Принцип обязательного участия специалиста. Сущность этого принципа заключается в том, что участие специалиста является обязательным, если в ходе следственного действия происходит манипуляция с электронными носителями;

– Принцип протоколирования. Следование данному принципу необходимо для того, чтобы результаты процессуальных действий по исследованию электронных носителей могли быть использованы в процессе доказывания по уголовным делам[139].

На наш взгляд, соблюдение принципов, сформулированных Е.Р. Россинской, бесспорно, имеет большое значение при работе с электронными носителями. Однако, реализация второго принципа (обязательного изъятия носителя) не всегда может быть эффективна с точки зрения доказывания. Как показывает практика, доступ к информации и исследование её на месте нахождения носителя зачастую является достаточным способом закрепления электронно-цифровых следов. Иногда необоснованное изъятие электронных носителей информации может ущемлять права других лиц и принести к негативным последствиям, к примеру, в производственных предприятиях оно может послужить причиной временного приостановления их деятельности или иным образом негативно повлиять на

[139] См.: Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – №3-2. – С. 115.

полноценное функционирование этих предприятий. В связи с этим, прежде чем решить вопрос о целесообразности изъятия электронного носителя, необходимо совместно со специалистом оценить все возможные риски, которые может вызвать извлечение устройства памяти из компьютерного устройства. По данному вопросу мы солидарны с позицией Ю.В. Гаврилина и А.В. Победкина, которые, признав копирование приоритетным способом изъятия информации, считают, что электронный носитель должен изыматься только в тех случаях, когда дальнейшее использование хранящейся на нём информации может воспрепятствовать следствию или применено в преступной деятельности, если копирование может привести к утрате информации, её модификации и невозможности дальнейшего воспроизведения, процедура копирования может занять продолжительное время или в процессе проведения следственного действия нет возможности определить значимость информации, содержащейся на электронном носителе[140]. По нашему мнению, электронный носитель должен изыматься также в случае, если обнаружение электронно-цифровых следов на месте его нахождения невозможно и существует необходимость в назначении судебной компьютерно-технической экспертизы.

На основе анализа следственной практики выяснилось, что в рамках расследования уголовных дел о преступлениях, в механизме совершения которых использованы информационные технологии, в подавляющем большинстве случаев производится изъятие электронных носителей и изредка - копирование их содержимого.

В связи с этим, следует отметить, что предпочтение изъятию электронных носителей обусловлено такими факторами как экономия времени, невозможности привлечения специалиста, исследование носителей в рамках последующих процессуальных действий, избежание рисков модификации и удаления данных, а также возможного повреждения носителей со скопированными сведениями.

---

[140] См.: Гаврилин Ю.В., Победкин А.В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы / Ю.В. Гаврилин, А.В. Победкин // Труды Академии управления МВД России. – 2018. – №3 (47). – С. 110.

Вместе с тем, С.В. Зуев[141], на основе анализа положений законодательства и практики органов следствия и суда, определил ряд условий для копирования электронно-цифровых данных. В особенности, он утверждает, что важными условиями для копирования являются доступность информации на электронных носителях, наличие у лица, проводящего следствие, электронного носителя с большим объёмом памяти, участие специалиста и понятых, отсутствие препятствующих этому процессу обстоятельств и точное соблюдение правил фиксации производимых действий и протоколирование процесса копирования.

Таким образом, можно утверждать, что тактические приёмы обнаружения и фиксации электронно-цифровых следов, в зависимости от расследуемого преступления, определяются с учётом сложившейся следственной ситуации. Вместе с тем, цели собирания следов данной категории состоит, во-первых, в установлении электронного носителя, во-вторых, в обнаружении и фиксации на установленном носителе следов преступной деятельности, и в-третьих, в получении дополнительной информации посредством исследования электронно-цифровых следов.

Характерные особенности фиксации электронно-цифровых следов на ресурсах сети Интернет

Следует признать, что из общего числа преступлений, в механизме которых используются информационные технологии, большинство из них совершаются с применением возможностей глобальной сети Интернет. В связи с чем, огромный объём доказательственной информации может содержаться на информационных ресурсах, доступ к которым происходит посредством сети Интернет.

Проведенный анализ показал, что в уголовно-процессуальном законе Республики Таджикистан особые процессуальные средства, предназначенные для собирания доказательств о преступлениях, совершаемых с применением информационно-телекоммуникационной сети Интернет, не предусмотрены. Вместе с тем, в последние годы, принимая во внимание высокую общественную

[141] См.: Зуев С.В. Основы теории электронных доказательств: монография. – М.: Юрлитинформ, 2019. – С. 304.

опасность использования телекоммуникационных сетей в преступной деятельности, законодательным органом были введены в Уголовный кодекс Республики Таджикистан несколько квалифицирующих составов преступлений, связанных с использованием сети Интернет. Эти нововведения касались ч. 2 ст. 137 (Публичное оскорбление Президента Республики Таджикистан или клевета в его адрес, совершенные с использованием сети Интернет), ч. 2 ст. 137 (1) (Публичное оскорбление Основателя мира и национального единства – Лидера нации или клевета в его адрес, совершенные с использованием сети Интернет), ч. 1 ст. 144 (Незаконное собирание и распространение информации о частной жизни в сети Интернет), п. «г» ч. 2 ст. 179 (1) (Вовлечение в совершение преступлений террористического характера или иное содействие их совершению с использованием сети Интернет), ч. 2 ст. 179 (3) (Публичные призывы к совершению преступлений террористического характера и (или) публичное оправдание террористической деятельности, совершённые с использованием сети Интернет), ч. 1 ст. 189 (Разжигание социальной, расовой, национальной, региональной, религиозной (конфессиональной) вражды или розни, совершённые с использованием сетей электрической связи, в том числе сети Интернет) и др.

В нынешних условиях расследование большинства преступлений данной категории основано на получении доказательственной электронно-цифровой информации в виде сообщений, текстовых и мультимедийных файлов, переписки в социальных сетях и т.п. Получаемая информация способствует выяснению обстоятельств расследуемого события и доказыванию вины лиц, причастных к совершению преступления.

В процессе обращения в компьютерных сетях информация оставляет электронно-цифровые следы на соответствующих носителях. Ю.В. Гаврилин, раскрывая особенности данной категории следов, отмечает, что электронно-цифровые следы отражают событие преступления в информационном пространстве, являются результатом модификации электронной информации, они не могут отражать материальную форму следообразующего объекта, им присущи свойства компьютерной информации и при копировании их свойства не

претерпят существенные изменения[142].

Несмотря на особенности доказательственной электронно-цифровой информации, её собирание осуществляется предусмотренными УПК Республики Таджикистан процессуальными средствами. К числу основных следственных действий, в рамках которых электронно-цифровые следы обнаруживаются, фиксируются и закрепляются в протокольной форме, относятся осмотр, обыск, выемка и экспертиза. Особых следственных действий, предназначенных для собирания фактических данных в компьютерных сетях, уголовно-процессуальное законодательство на данный момент не содержит.

По мнению Д.В. Бахтеева, при собирании и проверке доказательственной электронно-цифровой информации необходимо обратить внимание на следующие особенности следственных и иных процессуальных действий[143].

1. В протоколе следственного действия обязательному описанию подлежат содержимое и реквизиты электронно-цифровой информации. В случае её копирования, к протоколу прилагается электронный носитель.

2. Все действия лица, проводящего следственные мероприятия, и привлечённого специалиста по обнаружению и фиксации доказательств, а также использованные технические средства должны быть описаны в протоколе.

3. Необходимо правильно установить взаимосвязь между обнаруженными фактическими данными, расследуемым событием и участниками уголовного судопроизводства.

В развитие мысли Д.В. Бахтеева, на наш взгляд, следует также учитывать нижеследующие обстоятельства в процессе производства следственных действий по обнаружению доказательственной информации в компьютерных сетях:

– электронно-цифровая информация слишком чувствительна к наружным воздействиям и неквалифицированные действия могут легко привести к её утрате;

---

[142] См.: Гаврилин Ю.В., Шипилов В.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации / Ю.В. Гаврилин, В.В. Шипилов // Российский следователь. – 2013. – № 23. – С. 2.

[143] См.: Бахтеев Д.В. Основы теории электронных доказательств: монография / Под ред. д-ра юрид. наук С.В. Зуева. – М.: Юрлитинформ, 2019. – С. 284.

– искомые сведения не всегда могут храниться в обследуемом компьютере, а могут содержаться на удаленных компьютерах, соединённых с осматриваемым компьютером через сеть.

В следственной практике зачастую складывается ситуация, при которой в сети Интернет обнаруживается искомый объект в виде электронно-цифровых данных, однако местонахождение электронного носителя, хранящего эти данные остаётся неизвестным, либо оно может находиться за границей. В то же время, в связи с наличием технологической возможности дистанционного (удалённого) доступа к этим данным, наличие электронного носителя, его непосредственное исследование и физический контакт с ним не имеют значения для процесса доказывания. На данное обстоятельство, в частности, обращает внимание Т.Э. Кукарникова, по мнению которой в информационных сетях доступ к доказательственной информации и электронным носителям, сохранившим её, осуществляется только виртуально, так как не всегда возможно установить их физическое местонахождение, а в случае установления, оно может находиться за пределами досягаемости лица, проводящего следствие[144].

При наличии достаточных оснований полагать, что на определенном сетевом носителе имеется доказательственная электронно-цифровая информация, большое значение имеет фактор внезапности и своевременное принятие мер по пресечению возможности её уничтожения, блокирования, копирования или модификации.

Как показывает практика, в настоящее время для фиксации фактических данных в информационных сетях преимущественно используется следственный осмотр, криминалистические аспекты производства которого более подробно рассмотрим в следующем параграфе.

А.Л. Карлов совершенно верно отмечает, в настоящее время в уголовном процессе вопрос правового регулирования порядка фиксации и изъятия электронных доказательств, в частности, интернет-переписки остаётся открытым

[144] См.: Кукарникова Т.Э. Компьютерная информация как следообразующая система / Т.Э. Кукарникова // Криминалистика в системе правоприменения: материалы конф. (Москва, 27-28 октября 2008 г.). – 2008. – С. 148.

и нерешённым[145]. Для восполнения данного пробела в законодательстве он в качестве одного из вариантов решения предлагает дистанционную фиксацию электронно-цифровых доказательств, содержащихся в интернет-переписках, путём их осмотра, осуществляемого с использованием компьютера, подключенного к глобальной сети Интернет. Вместе с тем, автор предлагает считать интернет-страницу электронным документом и при фиксации использовать протокол осмотра электронного документа.

Схожую позицию занимают и В.Ф. Васюков и А.Н. Колычева. Они видят возможность фиксации сведений интернет-переписки путём осмотра электронной почты на электронно-вычислительной технике, электронного носителя с хранящейся на нём перепиской и бумажного носителя с содержанием электронной переписки. В последнем случае при производстве следственного осмотра применяются правила осмотра документов[146].

В.Д. Еськов и С.А. Чеботарев допускают фиксацию электронных доказательств, содержащихся на сайте сети Интернет, путём проведения следственного осмотра. Вместе с тем, они отмечают, что при оформлении результатов осмотра в протоколе процессуального действия, в первую очередь, должны быть зафиксированы использовавшиеся технические средства, к примеру, ноутбук с выходом в сеть Интернет[147]. По нашему мнению, указанные авторы под объектом осмотра в данном случае подразумевают электронный носитель информации.

Как известно, в зависимости от объекта исследования УПК Республики Таджикистан различает следующие виды осмотра: осмотр места происшествия, осмотр местности, осмотр помещения, осмотр предметов, осмотр документов и осмотр трупа. На примере исследования интернет-сайта и интернет-страницы в сети Интернет путём производства следственного осмотра ярко выражаются

---

[145] См.: Карлов А.Л. Использование в доказывании по уголовным делам сведений, составляющих тайну связи, расположенных в сети Интернет / А.Л. Карлов // Вестник Сибирского юридического института МВД России. – 2015. – №2. – С. 145.

[146] См.: Васюков В.Ф., Колычева А.Л. Осмотр и фиксация страниц интернет-сайта в сети Интернет / В.Ф. Васюков, А.Л. Колычева // Вестник экономической безопасности. – 2019. – № 1. – С. 116.

[147] См.: Еськов В.Д., Чеботарев С.А. Особенности осмотра страниц в сети Интернет / В.Д. Еськов, С.А. Чеботарев // Организационное, процессуальное и криминалистическое обеспечение уголовного производства: материалы VI Междунар. науч. конф. студентов и магистрантов. – 2017. – С. 39.

недостатки правовой регламентации вопроса фиксации электронных доказательств в уголовном судопроизводстве, так как эти объекты по своим свойствам никак не могут быть ни предметом, ни документом.

На практике осмотр сайта в сети Интернет чаще всего осуществляется посредством осмотра предметов и в протоколе данного следственного действия объектом осмотра указывается компьютер. Однако необходимо понимать, что в данном случае компьютер выступает в качестве используемого технического средства и обследуемые данные хранятся не в устройствах памяти данного компьютера.

А.Н. Иванов предлагает для исследования общедоступной информации, размещённой в открытых источниках информационных сетей, применять дистанционный (удалённый) осмотр. В качестве формы отражения результатов данного следственного действия он рассматривает протокол осмотра документов, к которому должны быть приложены распечатки исследованного ресурса и носитель со скопированной на него информацией[148].

Фиксация хода и результатов изъятия криминалистически значимой информации из ресурсов сети Интернет, также можно осуществить в рамках выемки. Когда следователь получит информацию о точном местонахождении объектов, содержащих доказательственную электронно-цифровую информацию, им принимается решение о производстве выемки. Подобная информация предварительно должна быть отражена в материалах расследуемого уголовного дела. К примеру, в ходе допросов, очных ставок, экспериментов и других следственных действий получаемые сведения о местонахождении искомых объектов должны быть зафиксированы в протоколах этих процессуальных действий, либо найти своё отражение в ответах на запросы органов следствия.

О производстве выемки следователь выносит постановление. В нём помимо общих данных, присущих для всех протоколов следственных действий, отражаются источники сведений о месте нахождения электронно-вычислительной

[148] См.: Иванов А.Н. О новом виде обыска / А.Н. Иванов // Актуальные проблемы криминалистики на современном этапе: сб. науч. ст. / Под ред. З.Д. Еникеева. – Уфа, 2003. – Ч. 1. – С. 105-109.

техники, подключённой к сети Интернет, носителях цифровой информации, сведений об интернет-соединениях и конкретные объекты, подлежащие выемке.

Данное следственное действие производится в соответствии со ст. 192 УПК Республики Таджикистан с обязательным участием понятых. Хотя, с законодательной точки зрения, участие специалиста при выемке не является обязательным, в данном случае его привлечение считается необходимым. Так как следователь не является сведущим лицом, не всегда может быть осведомлён об особенностях работы с электронно-вычислительной техникой, подключенной к сети Интернет, и его неквалифицированные действия легко могут привести к утрате электронных доказательств.

По результатам выемки составляется протокол, в котором описывается время и место его составления, обстоятельства обнаружения электронно-вычислительного устройства и его подсоединения в глобальную сеть, перечисляются объекты, подлежащие изъятию, с указанием идентифицирующих свойств, места хранения информации на электронном носителе обнаруженного устройства, название файлов, их реквизиты и объём содержимой информации, отражается факт копирования информации и другие сведения.

Также, большое доказательственное значение имеет обнаружение и изъятие в ходе выемки в помещении с компьютерной техникой, традиционных объектов, к которым можно отнести бумажные носители информации, записи реквизитов доступа, оптические диски, флэш-карты, записные книжки с данными, представляющими интерес для следствия (имена соучастников преступления, номера телефонов, банковских счетов и карт и т.п.) и пр.

Изъятые в ходе выемки электронные носители информации упаковываются и опечатываются способом, исключающим возможность ознакомления третьих лиц с находящейся на них информацией. Способ упаковки и опечатывания описывается в протоколе следственного действия.

Уголовно-процессуальный кодекс Республики Таджикистан оставляет открытым вопрос о возможности производства обыска в информационно-телекоммуникационных сетях. А.Г. Волеводз верно отмечает, что в настоящее

время законодательством не урегулирована проблема изъятия фактических данных о совершённом преступлении путём обыска в компьютерных сетях в целях получения искомой компьютерной информации[149].

На удобство производства обыска в компьютерных сетях обращает внимание А.Л. Осипенко, который отмечает, что процессуальное исследование доказательственной информации в телекоммуникационных сетях существенно отличается от изучения данных в рамках обыска помещений. Это отличие, главным образом, выражается в характере производимых действий, а также в том, что при обыске в компьютерных сетях требуются определённые знания, технические и программные средства. Он утверждает, что удалённое изучение и исследование электронно-цифровой информации, т.е. находясь за одной компьютерной техникой, просматривать содержимое другой, считается удобным способом собирания доказательств[150].

Несомненно, на данный момент при помощи существующих современных технологий возможно дистанционно обследовать криминалистически значимую информацию в компьютерных сетях. Однако, здесь нерешенным остается вопрос процессуального оформления результатов подобного обследования, в частности, допустимость фиксации доказательств в информационных сетях в рамках обыска или осмотра, необходимость для этого санкции суда, условия и порядок производства данных следственных действий, круг участвующих лиц и т.п.

Конвенция Совета Европы о преступности в сфере компьютерной информации (ETS №185, от 23.11.2001 г.) предусматривает возможность производства удалённого обыска в компьютерных сетях и электронных носителях. И к тому же, данный международный нормативно-правовой акт обязывает государства, подписавшие его, принимать законодательные и иные меры для предоставления компетентным органам полномочий на производство данного следственного действия[151].

---

[149] См.: Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Изд-во Юрлитинформ, 2001. – С. 13.

[150] См.: Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. – М., 2004. – С. 274-275.

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

А.Н. Иванов, рассуждая о возможности применения обыска для собирания цифровых доказательств, подчёркивает, что технологическое развитие позволяет дистанционно исследовать компьютерные системы и содержащихся в них данных. В качестве одного из вариантов исследования названных объектов он предлагает выделить дистанционный (удалённый) обыск компьютерной сети или её отдельных частей. При этом, он полагает, что данное следственное действие необходимо производить на основании санкции суда, в присутствии владельца электронно-цифровой информации. Перед проведением обыска владельцу предъявляется санкция суда, ему и другим участникам следственного действия разъясняется порядок проведения обыска, а также их права и обязанности, а также они предупреждаются о применении технических и иных средств. Затем, следователь предлагает владельцу выдать интересующие следствие материалы, содержащиеся на его компьютере в электронном виде. Безусловно, владелец при этом не допускается к компьютерной технике, он лишь представляет данные, необходимые для получения доступа к содержимому компьютерной системы (пароль, логин, IP-адрес и т.п.) [152].

Однако, необходимо помнить, что дистанционный обыск отличается от обыска в традиционном его понимании. При удалённом обыске изъятие обследуемых объектов не осуществляется, а производится копирование фактических данных о совершённом преступлении в форме электронно-цифровой информации.

В.А. Мещеряков также допускает возможность собирания доказательств посредством обыска в информационных системах. Наряду с этим, он в зависимости от объектов, подлежащих обследованию, выделяет сосредоточенный, рассредоточенный и открытый виды обыска. Первый вид обыска, т.е. сосредоточенный, проводится тогда, когда объектом обследования выступают один или несколько электронно-вычислительных машин, находящихся в одном

г.Будапешт) [Электронный ресурс]. – Режим доступа: URL: https://rm.coe.int/1680081580 (дата обращения: 23.05.2022).

[152] См.: Иванов А.Н. Удаленное исследование компьютерной информации: уголовнопроцессуальные и криминалистические проблемы / А.Н. Иванов // Известия Саратовского университета. – 2009. – Т. 9. Вып. 2. – С. 75.

помещении. Рассредоточенный обыск не ограничивается в пределах одного помещения и в его рамках обследованию подвергается локальная компьютерная сеть, которая может охватывать два или более помещений или зданий. Открытый обыск направлен на исследование отдельных электронно-вычислительных машин либо локальных сетей, которых объединяют общедоступные каналы связи[153].

С.В. Пропастин высказывает мнение о необходимости введения в уголовно-процессуальное законодательство особых видов следственных действий по фиксации доказательственной информации в компьютерных сетях. Вместе с тем, он не обозначает, какие именно процессуальные действия следует вводить для собирания электронно-цифровых доказательств[154].

Вместе с тем, И.И. Карташов не видит необходимости во введении нового вида следственного действия – удалённого обыска для фиксации доказательственной информации в электронно-вычислительных сетях. Он считает, что при удалённом обыске специальные познания применяются не только для обнаружения и фиксации информации, но и для доступа к ней, что приведёт к утрате доказательственного значения исходных данных вследствие их модификации. И к тому же объём применяемых специальных познаний при удалённом обыске сопоставим с производством судебной компьютерно-технической экспертизы и в связи с этим, предлагается осуществить исследование и последующее изъятие информации в компьютерных сетях в рамках данного вида экспертизы[155].

Таким образом, относительно вопроса совершенствования процессуального порядка собирания криминалистически значимой информации на электронных носителях, можно подытожить следующее:

1. Большинство авторов научных работ по изучению проблем собирания доказательственной информации в информационно-телекоммуникационных сетях

---

[153] См.: Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. – Воронеж, 2001. – С. 28.

[154] См.: Пропастин С.В. О проведении осмотра и обыска дистанционно / С.В. Пропастин // Сборник материалов Барнаульских криминалистических чтений. – 2012. – С. 75.

[155] См.: Карташев И.И. «Цифровые доказательства» в уголовном процессе / И.И. Карташев // Центральный научный вестник. – 2016. – № 155. – С. 24.

высказываются о необходимости совершенствования законодательства в целях создания процессуальных средств фиксации электронно-цифровых доказательств.

2. Вариантами подобного совершенствования видится во введении в уголовно-процессуальное законодательство специальных правовых процедур в рамках осмотра и обыска.

3. В названных работах недостаточно раскрыты сущностные различия в основаниях и порядке производства дистанционного (удалённого) осмотра и дистанционного (удалённого) обыска.

4. Не установлены условия допустимости «сетевого проникновения», а также не определены механизмы защиты прав и интересов собственников информационных ресурсов.

Рассматривая обозначенные выводы, относительно соотношения дистанционного осмотра и дистанционного обыска следует отметить, что эти следственные действия объединяет их содержание, т.е. поисково-познавательный характер. Оба действия предназначены для собирания фактических данных о совершённом общественно-опасном деянии в информационных системах, получить доступ к которым возможно только посредством компьютерных сетей. При этом, как при дистанционном осмотре, так и в ходе удалённого обыска используются программные и технические средства для трансформации электромагнитных импульсов, протекающих по каналам связи, в электронно-цифровую информацию.

Различие этих двух следственных действий заключается в том, что дистанционный обыск осуществляется в принудительном порядке, а дистанционный осмотр – без применения принудительных мер.

Так, фиксация и изъятие доказательственной информации, находящейся в открытом доступе без применения паролей или иной защиты, должны осуществляться в рамках дистанционного (удалённого) осмотра интернет-ресурсов, под которым следует понимать процессуальное (следственное) действие, выражающееся в визуальном исследовании информации, содержащейся в компьютерных сетях, доступ к которой предоставлен неограниченному

количеству лиц.

Сущность дистанционного обыска заключается в принудительном порядке обследования закрытых информационных ресурсов в целях получения доказательственной электронно-цифровой информации.

Нами предлагается под дистанционным (удалённым) обыском понимать процессуальное (следственное) действие, выражающееся в принудительном обследовании информационной системы посредством компьютерных сетей, доступ к содержимому которой ограничен её обладателем. Основанием для его проведения послужит наличие достаточных данных о возможном существовании в информационной системе сведений, относящихся к расследуемому событию или имеющих значение для правильного разрешения дела.

Ввиду того, что в ходе производства дистанционного обыска иные сведения, не относящиеся к предмету доказывания, но вместе с тем, составляющие охраняемую законом тайну (например, тайна личной жизни) могут стать достоянием других лиц, в частности, участников следственного действия, данное процессуальное действие должно быть санкционировано судом.

Дистанционный обыск необходимо проводить с обязательным участием специалиста, который способствует следователю в получении доступа в информационную систему, преодолении средств защиты от несанкционированного доступа, отыскании доказательственной информации, её копировании и выполняет иные поручения лица, проводящего следственное действие.

Перед началом дистанционного обыска присутствующим разъясняется порядок проведения следственного действия. В случае присутствия владельца обследуемых информационных ресурсов, должностное лицо, осуществляющее следственное действие, ознакомит его с санкцией суда и предлагает добровольно предоставить доступ к данным, представляющим интерес для следствия.

Результаты и итоги дистанционного обыска, а также все произведённые действия следует отражать в протоколе данного процессуального действия. При этом важно отметить, что в связи с отсутствием доступа к соответствующим

электронным носителям в процессе данного вида обыска, изъятие выявленных искомых данных из информационных сетей возможно только путём её копирования[156].

Наиболее удачно сформулировал определение копирования электронно-цифровой информации С.В. Зуев, по мнению которого «это познавательный приём уголовно-процессуального доказывания, представляющий собой получение информации посредством создания копии и сохранения информационного продукта (файлов, программных обеспечений и т.п.) на физический носитель в результате подсоединения к информационно-технологическим устройствам или дистанционно (удалённо) в целях выяснения обстоятельств, подлежащих доказыванию по уголовным делам»[157]. Вместе с тем, следует подчеркнуть, что при применении данной процессуальной процедуры исходная информация не подвергается изменению, а скопированная информация идентична оригиналу и послужит доказательством по уголовному делу.

С учётом проведённого исследования в настоящем параграфе, можно сформулировать следующие выводы.

1. Тактические приёмы обнаружения и фиксации электронно-цифровых следов зависят от следственной ситуации, сложившейся на конкретный момент расследования.

В следственной ситуации, характеризующейся наличием данных о нахождении в компьютерной или иной цифровой технике участника уголовного судопроизводства электронно-цифровых следов, необходимо осуществить следующие процессуальные действия: а) произвести осмотр электронных носителей при участии специалиста соответствующего профиля; б) исследование полученной информации и её сопоставление с данными, имеющимися в распоряжении органов следствия; в) допрос участника уголовного судопроизводства (свидетеля, потерпевшего, подозреваемого, обвиняемого) с

[156] См.: Гаврилин Ю.В., Балашова А.А. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах / Ю.В. Гаврилин, А.А. Балашова // Криминалистика: вчера, сегодня, завтра. – 2020. – №1. – С. 129-137.
[157] Зуев С.В. Основы теории электронных доказательств: монография. – М.: Юрлитинформ, 2019. – С. 302.

предъявлением изъятых с электронных носителей данных.

В том случае, когда в результате следственного осмотра не получены искомые данные, необходимым считается: а) изъятие электронного носителя; б) назначение судебной компьютерно-технической экспертизы; в) допрос участника уголовного судопроизводства с предъявлением результатов экспертизы.

При благоприятном развитии ситуации, когда со стороны участников уголовного судопроизводства не оказывается противодействие следствию, перед вышеотмеченным комплексом можно произвести допрос владельца электронного носителя и осмотр места происшествия при участии специалиста.

В следственной ситуации, когда в распоряжении органов предварительного следствия имеются сведения о конкретном месте совершения общественно-опасного деяния, о лице либо лицах, совершивших преступление, и при этом предварительному следствию оказывается противодействие, результативным является применение следующего тактического комплекса: а) осмотр места происшествия в целях поиска и обнаружения электронных носителей информации; б) обыск в местах жительства и работы подозреваемых в указанных целях; в) при участии специалиста в области информационных технологий осуществить оценку радиоэлектронной обстановки местности; г) установить номера сотовых аппаратов конкретных участников уголовного судопроизводства и запросить у операторов мобильной связи сведений о детализациях их телефонных переговоров с указанием месторасположения абонентов (геолокацией) на момент осуществления звонков, а также информацию о зонах обслуживания конкретных сервисных базовых станций; д) анализ или исследование полученных сведений; е) допрос участника уголовного судопроизводства с предъявлением детализации телефонных переговоров и результатов осмотра электронных носителей. Анализ может проводиться следователем самостоятельно либо с привлечением специалиста. При привлечении специалиста либо эксперта в исследовании, их выводы могут быть оформлены в форме заключения специалиста или эксперта.

Вышеописанные комплексы в зависимости от расследуемого события могут

уточняться и конкретизироваться.

2. В Уголовно-процессуальном кодексе Республики Таджикистан средства и механизмы собирания доказательственной информации в информационно-телекоммуникационных сетях не предусмотрены. Большинство в научных кругах считают, что в связи с распространением преступлений, совершаемых с использованием возможностей информационных технологий, назрела реальная необходимость совершенствования уголовно-процессуального законодательства в данном направлении.

Принимая во внимание вышесказанное, в целях правового регулирования процесса собирания доказательственной информации в информационно-телекоммуникационных сетях, диссертантом предлагается дополнить действующий Уголовно-процессуальный кодекс Республики Таджикистан статьями 183 (1) «Дистанционный осмотр электронно-цифровых информационных ресурсов» и 194 (1) «Дистанционный обыск» в следующей редакции:

«Статья 183 (1). Дистанционный осмотр электронно-цифровых информационных ресурсов

1. Дознаватель, следователь или прокурор в целях обнаружения следов преступных действий, выяснения иных обстоятельств, имеющих значение для правильного разрешения дела, проводит дистанционный (удалённый) осмотр информации, размещенной на электронно-цифровых информационных ресурсах и доступ к которой не ограничен.

2. В порядке, предусмотренном настоящим Кодексом, при производстве дистанционного осмотра в качестве специалиста может быть привлечено лицо, обладающее необходимыми знаниями в области информационных технологий.

3. О результатах проведения дистанционного осмотра составляется протокол, где помимо требований статей 172-173 настоящего Кодекса, также отражается сетевой адрес обследуемого электронного ресурса, содержащаяся на нём доказательственная информация, использованные программные и технические средства, модель и характерные свойства носителя, на котором

скопированы криминалистически значимые данные.

4. Носитель со скопированными данными упаковывается способом, исключающим возможность получения доступа к его содержимому посторонним лицам».

«Статья 194 (1). Дистанционный обыск

1. Дознаватель, следователь или прокурор в целях принудительного обследования данных, доступ к которым ограничен, проводит дистанционный (удалённый) обыск электронно-цифровых информационных ресурсов.

2. Основанием для производства дистанционного обыска является наличие достаточных данных о возможном наличии в информационных ресурсах сведений, относящихся к расследуемому событию.

3. Дистанционный обыск проводится на основании мотивированного постановления должностного лица, в производстве которого находится уголовное дело, согласия прокурора и разрешения суда.

4. Участие специалиста при производстве дистанционного обыска является обязательным. При его содействии преодолеваются возможные технические и программные средства защиты электронно-цифровой информации.

5. Перед началом дистанционного обыска присутствующим разъясняется порядок проведения следственного действия. В случае присутствия владельца обследуемых информационных ресурсов, должностное лицо, осуществляющее следственное действие, ознакомит его с санкцией суда и предлагает добровольно предоставить доступ к интересующим следствие данным.

6. О результатах проведения дистанционного обыска информационных ресурсов составляется протокол с соблюдением требований статьи 194 настоящего Кодекса. Также, в протоколе указываются сетевой адрес обследуемого информационного ресурса, содержащаяся в нём доказательственная информация, использованные программные и технические средства, модель и характерные свойства носителя, на котором скопированы криминалистически значимые данные.

7. Электронный носитель со скопированной информацией упаковывается и

опечатывается на месте производства следственного действия, что удостоверяется подписями лиц, участвующих в нём».

2.2. Тактика осмотра электронных носителей информации и мест их обнаружения

Одним из самых часто производимых процессуальных действий является следственный осмотр. На первый взгляд, из-за высокой частоты производства осмотра, кажется, что его планирование и осуществление не могут быть сложными. Тем не менее, проведение данного следственного действия, в рамках которого осуществляется исследование и фиксация электронно-цифровых следов, вызывает трудности у органов предварительного следствия.

Некоторые авторы рассматривают возможность исследования электронных носителей в рамках осмотра места происшествия как процессуального средства получения криминалистически значимой информации[158]. Вместе с тем, применительно к электронно-цифровым следам помимо осмотра места происшествия (например, при обнаружении места нахождения персональных устройств, использованных при совершении преступления) для нас представляют интерес осмотр предметов (например, электронных носителей) и осмотр документов (к примеру, текстовых документов, хранящихся в электронном виде).

Осмотр места происшествия применительно к исследуемой нами тематике – это неотложное следственное действие, в рамках которого обследуется, устанавливается и фиксируется обстановка места обнаружения электронных носителей, содержащихся на них электронно-цифровых следов и других обстоятельств, могущих способствовать правильному разрешению уголовного дела. От качества проведения осмотра зависит дальнейший ход сбора доказательств и расследования уголовного дела.

---

[158] См.: Васюков В.Ф. Способы получения доказательственной информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учебное пособие. – Москва: Проспект, 2017. – С. 23-24; Кузнецов А.А., Муленков Д.В., Пропастин С.В., Соколов А.В. Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей информации на них: учеб. пособие. – Омск: Омская академия МВД России, 2015. – С. 7.

Согласно ч. 4 ст. 183 УПК Республики Таджикистан осмотр фактических данных о совершённом преступлении и иных объектов материального мира может быть осуществлён как в ходе осмотра места происшествия, так и после него, при условии, что для осмотра необходимо длительное время или обследование предметов на месте их обнаружения вызывает трудности.

Следует отметить, что положения ст. 182 УПК Республики Таджикистан допускает производить осмотр места происшествия до возбуждения уголовного дела, если обстоятельства требуют принятия безотлагательных мер. А осмотр предметов, к числу которых относятся и электронные носители информации, разрешается только в рамках возбужденного уголовного дела.

Цели осмотра места происшествия по получению фактических данных с электронных носителей, не имеют специфики и аналогичны целям, решаемым в процессе осмотра места происшествия по другим преступлениям: а) получение новых и проверка имеющихся в наличии доказательств; б) получение исходных данных для выдвижения криминалистических версий и проверка имеющихся версий.

Круг задач осмотра места происшествия в данном случае имеет свою специфику. Эти задачи уточняют и определяют действия следователя по собиранию фактических данных в ходе данного следственного действия.

Указанные задачи заключаются в следующем:

1) Отыскание и фиксация электронно-цифровых следов расследуемого преступления. Эти следы могут быть образованы как при совершении преступлений против информационной безопасности (ст.ст. 298-304 УК РТ), так и в результате совершения иных преступных действий (краж, вымогательств, мошенничеств, преступлений в сфере незаконного оборота наркотических средств и т.д.).

2) Фиксация сложившейся обстановки на месте совершения преступления. Исследование обстановки позволяет установить факт использования электронных носителей, условия образования электронно-цифровых следов, а также обстоятельства их обнаружения и изъятия. Фиксация обстановки также

необходима для придания данных, содержащихся на электронных носителях, доказательственного значения по уголовным делам.

С тактической точки зрения осмотр места происшествия подразделяется на три этапа: подготовительный, рабочий и заключительный. На этот счёт М.А. Васильева и Р.Р. Рахмаджонзода справедливо отмечают, что разделение осмотра места происшествия на этапы способствует систематизации действий следователя[159] и тем самым, обеспечивает качественность данного следственного действия[160].

На подготовительном этапе деятельность следователя применительно к тематике нашего исследования можно условно разбить на две группы: действия, осуществляемые до выезда на место происшествия и действия, предпринимаемые после прибытия на место происшествия.

От действий следователя, предшествующих выезду на место, зависят своевременное прибытие на место происшествия и качественное проведение осмотра. На данной стадии следователю предстоит решать ряд вопросов.

1) Принимает меры для устранения обстоятельств, способных повлечь неблагоприятные последствия (модификации информации, уничтожение следов) или затруднять работу на месте происшествия. С этой целью, следователем осуществляется следующие действия (либо организуется их проведения другими лицами):

– устанавливается тип программного обеспечения и наличие соединения компьютерных устройств к локальной или глобальной сети. Здесь речь идёт об операционной системе Windows и её альтернативах (MacOs, Linux,и др.). Электронно-вычислительные устройства при этом могут функционировать автономно либо быть подсоединены в локальную сеть. Не исключается также тот факт, что и в первом и во втором варианте обследуемые устройства могут быть подключены к глобальной сети. Данное обстоятельство необходимо учитывать

[159] Осуществлять осмотр может не только следователь, но и другие уполномоченные уголовно-процессуальным законом лица (прокурор, дознаватель и др.). Для краткости субъект, проводящий осмотр, будет именоваться далее в тексте - следователь.

[160] См.: Криминалистика: учебник / Отв. ред. В.П. Лавров, Р.Х. Рахимзода, А.Ф. Волынский. – Душанбе, 2022. – С. 281–282.

для верного определения времени осмотра, определения участников осмотра, последовательность действий по прибытию на место происшествия и т.д. По этому поводу нельзя не согласиться с мнением В.В. Полякова, который верно замечает, что для правильного формирования следственной группы и обеспечения её специальными средствами, следователю до выезда на место происшествия важно ознакомиться с оперативно-розыскной информацией о расследуемом событии и программно-аппаратных средствах электронно-вычислительной техники, находящихся на месте происшествия[161].

– устанавливается наличие средств защиты в компьютерном устройстве. Для предотвращения несанкционированного доступа к информации используются следующие методы: организационные (наличие пропускного режима в осматриваемом месте, специальных мест для хранения электронных носителей и др.), технические (фильтры, устройства аутентификации, электронные ключи на микросхемах и др.), программные (блокировка экрана или клавиатуры, пароли и др.) и криптографические (шифрование, стенография).

– обеспечивается сохранность обстановки на месте происшествия;

– не допускается преждевременное восстановление компьютерной системы.

2) Определяет место и время проведения данного следственного действия.

При определении места осмотра следователь анализирует имеющиеся в его распоряжение сведения и определяет места вероятного нахождения носителей электронно-цифровой информации. Такими местами могут быть железные шкафы, металлические сейфы, помещения, где находятся сервер (главный компьютер) локальной сети, ноутбуки, персональные компьютеры и др.

Определение времени означает конкретную дату, планируемое время начала и окончания осмотра места происшествия.

3) Определяет круг участников осмотра места происшествия. Одним из участников, который вносит большой вклад в качество осмотра, является специалист. В соответствии со ст. 57 УПК Республики Таджикистан специалист

[161] См.: Поляков В.В. Этапы осмотра места происшествия по компьютерным преступлениям /В.В. Поляков // Закон и право. – 2016. – №11. – С. 112-114.

является лицом, не заинтересованным в исходе дела, обладает специальными знаниями и в ходе следственного действия оказывает содействие следователю в поиске доказательств, их фиксации и обосновании, а также в использовании технических устройств. Кроме того, он может помочь в установлении механизма функционирования компьютерного устройства, определении места нахождения носителя информации в электронно-вычислительной технике и разрешить возникающие непосредственно в ходе осмотра различные технические проблемы. На данное обстоятельство обращает внимание Н.П. Яблоков, который отмечает, что «в случае, если обстоятельства расследуемого события указывают на возможное возникновение в ходе проведения следственного действия «нештатных» ситуаций – привлечение специалиста необходимо»[162]. Вместе с тем, А.А. Балашова утверждает, что не всегда в процессе следственных действий исследуется содержимое изымаемых электронных носителей и в связи с этим, нет необходимости в обязательном участии специалиста в них[163]. Схожую позицию занимают К.А. Костенко[164] и Ю.В. Гаврилин[165].

С учетом изложенного, полагаем, что в зависимости от стоящих перед осмотром задач, следователь самостоятельно должен решать вопрос о привлечении в нём специалиста. Если в процессе осмотра места происшествия не предусмотрено исследование содержания электронного носителя информации и изъятие носителей не сопряжено со вскрытием электронно-вычислительной техники, то вполне допустимо его производство без участия специалиста.

Другим участником осмотра может быть эксперт-криминалист, который содействует в обнаружении и сборе традиционных фактических данных (к примеру, следов пальцев рук на деталях компьютерного устройства, на

---

[162] Яблоков Н.П. Криминалистика: практикум. – Москва: Юристъ, 2004. – С. 518.

[163] См.: Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. … канд. юрид. наук. – Москва, 2020. – С. 98.

[164] См.: Костенко К.А. К вопросу об особенностях изъятия электронных носителей информации при расследовании служебных преступлений / К.А. Костенко // Служебные преступления: вопросы теории и практики правоприменения: сб. материалов междунар. науч.-практ. конф. – Хабаровск, 2018. – С. 76.

[165] См.: Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве / Ю.В. Гаврилин // Труды Академии управления МВД России. – 2017. – №4. – С. 47; Гаврилин Ю.В., Победкин А.В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы / Ю.В. Гаврилин, А.В. Победкин // Труды Академии управления МВД России. – 2018. – №3 (47). – С. 109.

процессоре, экране, клавиатуре, мыши и т.п.). Также, в зависимости от вида расследуемого преступления, следователь может пригласить бухгалтера, искусствоведа и других лиц, обладающих специальными знаниями в других областях.

Целесообразным считается привлечение оперативных сотрудников для охраны помещения, где осуществляется осмотр, и пресечения возможного противодействия деятельности следственно-оперативной группы.

В соответствии со ст. 183 УПК Республики Таджикистан для засвидетельствования факта, процесса и результатов осмотра обязательным является приглашение понятых. По этому вопросу мы солидарны с мнением А.Н. Колычевой, которая рекомендует в процессе осмотра электронных носителей в качестве понятых привлекать лиц, обладающих знаниями в сфере информационных технологий, в частности компьютерной техники. Таковыми, например, могут быть студенты старших курсов, обучающихся в технических вузах по направлениям информатика, информационно-телекоммуникационные технологии, системы связи и др[166]. При этом, не желательно пригласить понятых из числа сотрудников организации, где проводится осмотр. Так как не исключается возможность их причастности к совершению расследуемого преступления.

Кроме того, для участия в следственном действии могут быть приглашены представители организации, где производится осмотр места происшествия.

4) Определяет перечень специальных средств и упаковочных материалов. Относительно специальных средств действия следователя заключается в проверке их наличия у специалиста. К таковым относятся:

– лабораторно-исследовательский переносной компьютер, оснащённый специальным аппаратным и программным обеспечением. Он предназначен для просмотра содержимого электронных носителей (жёстких дисков, компакт-дисков, флэш-карт и т.п.);

[166] См.: Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. … канд. юрид. наук. – Москва, 2018. – С. 90.

– аппаратные средства (блок питания, адаптер) и соединительные кабели;

– портативный принтер для возможной распечатки протокола осмотра и обнаруженных файлов;

– загрузочные носители (флэш-карты, компакт-диски, переносные накопители большой ёмкости и др.);

– цифровые фото-видеокамеры, фотовспышка;

– др.

Упаковочный материал подготавливается с учётом предполагаемого объёма и внешних характеристик объектов (компьютерная техника, электронные носители информации, документация и др.), подлежащих возможному изъятию на месте происшествия. В качестве упаковочного материала могут быть применены коробки (картонные либо пластиковые), полиэтиленовые пакеты, пластиковые контейнеры для компакт-дисков и др.

5) Проводит инструктаж участников следственного действия. В ходе инструктажа, который проводится перед выездом на место происшествия, следователь обращает внимание участников на недопустимость без его разрешения трогать компьютерную технику. В этом контексте А.Л. Осипенко совершенно верно указывает, что даже членам следственной группы при обращении с компьютерной техникой следует избегать всяких действий, последствия которых не могут быть предусмотрены[167].

Также, существует ряд правил, которые необходимо соблюдать при обращении с компьютерной техникой:

– все действия по включению и выключению компьютерной техники должны быть осуществлены только специалистами или под их руководством;

– разъединить и соединить кабельные линии только после того, как будут выяснены их назначение;

– демонтаж компьютерной техники и вскрытие системного блока осуществить исключительно с участием специалиста;

[167] См.: Осипенко А.Л. Особенности расследования сетевых компьютерных преступлений / А.Л. Осипенко // Рос. юрид. журнал. – 2010. – №2 (71). – С. 124.

– беречь устройства ввода и вывода компьютеров от попадания воды, мелких частиц и порошков;

– во избежание разрушения электронных носителей и повреждения хранящейся на них информации, только по согласованию со специалистом в ходе осмотра применить ультрафиолетовые осветители, магнитные искатели и другие подобные средства.

По прибытию на место происшествия следователем выполняется ряд неотложных действий:

– ограничивает доступ персонала, находящегося на месте осмотра, к средствам компьютерной техники в целях недопущения модификации, повреждения и удаления доказательственной информации;

– удаляет всех лиц, не участвующих в следственном действии, с места происшествия;

– организовывает охрану средств компьютерной техники и распределительных щитов;

– блокирует выход сервера локальной сети во внешнюю (глобальную) сеть[168].

На рабочем этапе осмотра места происшествия содержание деятельности следователя включает в себя следующее:

1) Осмотр помещения, где находится компьютерная техника. Это необходимо для фиксации обстановки объекта, содержащего электронный носитель, и установления его связи с событием преступления.

2) Осмотр рабочих мест с оснащёнными компьютерами. Необходимость в этом заключается также в фиксации обстановки обнаружения электронного носителя и установлении его связи с расследуемым событием.

3) Осмотр электронного носителя информации, что направлено на обнаружение, фиксацию и изъятие фактических данных.

В процессе осмотра помещений с компьютерной техникой следователь устанавливает границы места осмотра, размещения компьютерных устройств, места нахождения электронных носителей информации и схемы расположения

[168] См.: Давлатзода К.Д. Основания расследования киберпреступлений. – Душанбе, 2023. – С. 60.

рабочих мест. Основная цель на данном этапе заключается в фиксации объектов, находящихся в электронном взаимодействии.

В ходе осмотра помещения желательно воспользоваться тактическим приёмом «от центра к периферии». В данном случае центром выступает конкретный компьютер, который вероятнее всего содержит доказательственную информацию. От него идёт продвижение в сторону периферийных устройств.

Также не исключается при осмотре помещения использовать тактический приём «от периферии к центру». Конечно, в этом случае сервер компьютерной сети будет считаться центром.

Решение вопроса о том, какой тактический приём («от цента к периферии» или «от периферии к центру») следует применить при осмотре помещения, зависит от сложившейся следственной ситуации. В любом случае осмотр необходимо начинать с того участка места происшествия, где содержится наибольший объём доказательственной информации. В случае, если в помещении много компьютеров, то осмотр производится последовательно от одного компьютера к другому.

При осмотре рабочих мест с персональными компьютерами необходимо обратить внимание на: а) основной компьютер (сервер) локальной сети; б) компьютеры, не подключённые к локальной или глобальной сети; в) компьютеры, подключённые к информационным сетям; г) сетевые линии связи; д) принтеры, модемы, сканеры и другие периферийные устройства; е) соединительные кабели.

В ходе осмотра компьютерной техники следует уделять внимание на:

– месторасположение компьютера, принтера, сканера, клавиатуры, дисководов, мониторов и других периферийных устройств, а также их характеристики;

– механизм соединения между собой названных устройств;

– механизм подключения компьютера к локальной или глобальной сети;

– информацию, высвечиваемую на мониторе и световые сигналы различных индикаторов компьютерной техники;

– целостность кабелей, их соединений, наличие подключённой аппаратуры, не предусмотренной производителем;

– состояние корпуса и оборудований вычислительной техники, присутствие на них наклеек, знаков и других индивидуальных признаков;

– отсутствие или наличие механических повреждений на компьютерной технике;

– присутствие нестандартной аппаратуры внутри компьютера;

– наличие и технические особенности электронных носителей данных.

Фиксация процесса и результатов следственного действия является главной задачей заключительного этапа осмотра места происшествия. Результаты должны быть документально зафиксированы в установленной законом форме, то есть в протоколе. В нём целесообразно описывать обстоятельства, в которых происходит осмотр. И здесь, как верно отмечено С.А. Шейфером, предположения и обобщения о механизме следообразования, последовательности действий лица, совершившего преступления, и т.п. не фиксируются в протоколе осмотра места происшествия[169].

Во вводной части протокола осмотра указывается дата и место производства процессуального действия, временной интервал его продолжительности, должностное положение, фамилия и инициалы следователя, основание для проведения осмотра, установочные данные участников следственного действия, адреса понятых, статьи УПК РТ, на основании которых производится осмотр, используемые технические средства, условия (погода, освещённость), при которых проходит осмотр.

В описательной части протокола следственного действия подлежит фиксации следующее:

– общие сведения о расположении места происшествия, в том числе адрес, назначение здания, количество этажей в нём, входы и выходы в него и т.п.;

[169] См.: Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение. – Самара: Издательство «Самарский университет», 2004. – С. 59.

– месторасположение помещения, подлежащего осмотру, наличие сигнализаций, сохранность оконных и дверных проёмов, температура и влажность воздуха на момент осмотра;

– расположение электронно-вычислительной машины (компьютера) и других устройств в помещении относительно друг друга;

– название и тип (вид) конкретного объекта, входящего в комплект осматриваемого устройства компьютерной техники, инвентарный номер предприятия, его цвет, размер, форма, серийный номер, механические повреждения и иная информация;

– особенности соединения всех устройств компьютера;

– наличие линий связи для работы в сети, предназначенная в этих целях аппаратура и используемый номер телефонной связи с поставщиком сетевых услуг;

– наличие изменений, не предусмотренных стандартом, в состав персонального компьютера, соединённые к устройствам компьютера сторонние технические оборудования;

– наличие организационных, аппаратных и программных средств защиты компьютера от несанкционированного доступа;

– рабочее состояние (факт включения / выключения) компьютера на момент осмотра. Необходимо отметить, что в научных кругах в настоящее время нет единого мнения относительно того, как поступать следователю, если вычислительная техника на момент осмотра находится во включённом состоянии. Основные разногласия сводятся к тому, что стоит ли детально описать изображение на мониторе. Есть мнение, согласно которому изображение на мониторе необходимо детально описать в протоколе осмотра с использованием фото- и видеофиксации. Так, А.И. Дворкин считает, что «при осмотре работающего компьютера следует с участием специалиста установить, какая программа выполняется, для чего осмотреть изображение на экране дисплея и детально описать его (а проще произвести фотографирование или

видеозапись)»[170]. Противники данной позиции считают, что поскольку фиксация картины монитора приводит к потере времени и это обстоятельство увеличивает риск уничтожения или модификации электронных следов, не является целесообразным детально описать изображение на экране дисплея в протоколе осмотра[171]. Также в юридической литературе встречается точка зрения, согласно которой решение вопроса о целесообразности фиксации изображения на мониторе следует принимать на основании мнения привлечённого к осмотру специалиста[172]. То есть, если высвечиваемая на мониторе информация представляет интерес – её необходимо фиксировать детально, в противном случае, не стоит тратить на это время. На наш взгляд, более правильной представляется позиция А.И. Дворкина относительно действий следователя при осмотре включённого компьютера;

– произведённые манипуляции с устройствами вычислительной техники в процессе осмотра для поиска доказательственной информации;

– использованные аппаратные и программные средства для обнаружения и фиксации следов преступлений;

– обнаруженные электронные носители.

В заключительной части протокола осмотра отражаются: факт применения фотосъёмки и видеозаписи в ходе следственного действия; факт отключения компьютерных устройств от электропитания; наименование изъятых с места происшествия предметов, способ их упаковки, пояснительные надписи на них, сведения о печати на упаковках, данные о лице, которому переданы на хранение изъятые предметы; какие файлы и программы были скопированы, с каких электронных носителей на какие носители была скопирована интересующая следствие информация (в случае распечатки компьютерной информации на бумаге, указывается тип печатного устройства (принтера), место хранения

[170] Дворкин А.И. Осмотр места происшествия: практическое пособие. – Москва: Юристъ: Библиотека следователя, 2001. – С. 248.
[171] См.: Менжега М.М. Методика расследования создания и использования вредоносных программ для ЭВМ. – М.: Юрлитинформ, 2010. – С. 96.
[172] См.: Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук. – Москва, 2016. – С. 140.

скопированной информации; наличие приложений к протоколу следственного действия в виде планов, схем места осмотра, фото-таблиц, распечаток и т.п.; факт ознакомления участников осмотра с составленным протоколом, описание поступивших от участников замечаний к протоколу осмотра или отметка об их отсутствии.

Протокол подписывается лицом, составившим его, а также всеми участниками осмотра места происшествия.

Помимо протокола, для фиксации хода и результатов осмотра применяется видео- и фотосъёмка. При фотосъёмке сначала необходимо зафиксировать общий вид здания и помещения с компьютерами. После запечатлеть отдельные компьютеры и их периферийные устройства. Детальная съёмка потребуется при вскрытии системного блока для фиксации отдельных узлов, которые представляют интерес для следствия.

Видеосъёмка должна охватить все действия, производимые на месте осмотра, в том числе совершаемые манипуляции с компьютерной техникой, которые должны быть сопровождены комментарием следователя или привлечённого специалиста.

Важным и полезным элементом осмотра места происшествия, связанного с исследованием информационных технологий, является составление схем осматриваемых помещений. Эти схемы выступают в качестве приложений к протоколу осмотра и в них указываются месторасположения компьютеров и периферийных устройств, места обнаружения электронных носителей и следов расследуемого преступления.

При изъятии компьютерных объектов, имеющих электронные носители, необходимо завершить работу компьютерной техники, отключить её от электропитания, отметить изымаемые устройства компьютера, наклеить места их подсоединения к кабелю липкими листами или лентами с подписями участников осмотра и указанием даты. Также необходимо наложить тонкие слои бумаги (пломбирование) с подписями участников осмотра на все кнопки и разъёмы в целях исключения возможности включения компьютера и отдельных его

устройств. Кроме того, можно опечатывать системный блок путём помещения его в полиэтиленовый пакет.

Компьютерную технику и соединительные кабели необходимо упаковывать таким способом, чтобы исключить возможность их повреждения при транспортировке.

Следует отметить, что отсутствие на электронном носителе (флэш-карте, жёстком диске) информации не означает, что его не стоит изымать. Так как имеются специальные программы, с помощью которых возможно восстановить удалённую информацию. В настоящее время существуют множество подобных программ (Recuva PhotoRec, DMDE (DM Disk Editor and Data Recovery Software), R-studio и др.), которые могут помочь восстановить фото, документы, видео и другие файлы.

Изъятие компьютера производится лишь в случаях, когда его необходимо направить на экспертизу, на нём установлено аппаратное или программное обеспечение, не позволяющее на месте происшествия получить доступ к его содержимому, не получены пароли и коды доступа к компьютерной информации, на месте осмотра не удалось полностью изучить содержание имеющихся файлов и произвести их копирование. При этом, следует знать, что для получения доказательственной информации не всегда обязательно изымать всю компьютерную систему и все периферийные устройства. Поскольку не все устройства компьютера предназначены для хранения информации и они могут быть исследованы независимо друг от друга. В отдельных случаях можно ограничиваться только изъятием, например, жесткого диска. Так, в ходе расследования уголовного дела №12434 по факту совершения террористического акта возле здания ресторана «Лесная сказка» г.Душанбе 08 марта 2011 года, следователем при осмотре места происшествия было принято решение изымать только жёсткий диск компьютера, где записывались данные с камер видеонаблюдения периметра заведения. Данное решение было верным и следователю без труда удалось путём подключения жёсткого диска к рабочему компьютеру исследовать содержащуюся на нём информацию и тем самым

установить конкретное время совершения взрыва, свидетелей преступления и другие обстоятельства, имеющие значение для правильного разрешения дела. А владелец ресторана без ущерба от следственных действий, подключив другой жёсткий диск, продолжил свою работу[173].

При возникновении необходимости в изъятии электронных носителей информации с места происшествия следует придерживаться следующих рекомендаций:

– каждый изымаемый носитель необходимо упаковать в твёрдую коробку и опечатать её;

– на бумажном листе сделать отметку об изъятых носителях с указанием марки и их количества;

– коробку с изъятыми носителями и лист с описанием поместить в полиэтиленовый пакет и заклеить его.

Обобщая вышесказанное, необходимо отметить, что от выбора тактики осмотра места происшествия зависит продуктивность деятельности следователя при осмотре помещений с компьютерными устройствами и рабочих мест, оборудованных компьютерной техникой. В ходе производства данного следственного действия следователь должен исходить от типичных следов, возникающих в результате совершения преступлений с использованием электронно-вычислительных технологий. Фиксация содержания и результатов данного вида осмотра, а также изъятие предметов с места происшествия должны осуществляться с соблюдением определённых правил.

Осмотр предметов – электронных носителей информации осуществляется для фиксации внешних признаков носителя и восприятия содержащейся на нём информации в электронной форме. В данном исследовании мы будем рассматривать порядок осмотра широко распространённых электронных носителей и отдельных современных средств, содержащих устройства памяти.

В ходе осмотра электронных носителей необходимо уделять внимание таким обстоятельствам, как:

[173] См.: Уголовное дело №12434 // Архив ГКНБ РТ.

– место обнаружения (шкаф, сейф, стол) электронного носителя информации;

– наличие или отсутствие упаковки у обнаруженного электронного носителя, характерные признаки упаковки;

– наличие пометок и надписей на электронном носителе и его упаковке;

– вид, размеры носителя и сведения о его изготовителе;

– наличие повреждений и иных примет на нём;

– вместимость электронного носителя в килобайтах, мегабайтах или гигабайтах.

Также важным считается соблюдение определённых правил при обращении с электронными носителями в процессе следственного осмотра. Например, при работе с компакт-дисками не стоит прикасаться руками их рабочей поверхности, сгибать диски и подвергать их электромагнитному воздействию.

В ходе осмотра содержимого электронного носителя осуществляется поиск и обнаружение файлов, содержащих искомые данные о совершённом преступлении, а также прикладных программ обеспечения. Прикладные программы обеспечения, к числу которых относятся текстовые редакторы, программы работы с графикой, программы планирования и организации работ и т.п., предназначены для выполнения определенных пользовательских задач и непосредственного взаимодействия с пользователем. Данные программы позволяют получить криминалистически значимую информацию о дате и времени создания, модификации и распечатки файлов, количестве времени, которое было затрачено на работу с документом, источниках происхождения документов, движении финансовых и материальных средств, переписке подозреваемых лиц, круге его знакомых и деловых партнёров и др.

Кроме прикладного программного обеспечения важным является осмотр системного программного обеспечения (операционной системы), которое используется для обеспечения работы компьютера и выполнения прикладных программ. Они позволяют получить информацию о дате и времени начала работы компьютера, установки тех или иных программ и т.п.

Для получения доказательственной информации большое значение имеет осмотр содержащихся на электронных носителях документов в электронной форме. К таковым относятся:

– технический паспорт компьютерной аппаратуры и программного обеспечения или другой документ, его заменяющий;

– документы, регламентирующие работу с компьютером, системой или сетью;

– различные учётные документы (журнал учёта электронных носителей и электронных документов, а также их приёма-передачи, акты уничтожения электронных носителей, книга учёта технических неисправностей и т.п.);

– документы, разрешающие доступ к компьютерной технике (удостоверения личности, персональные идентификационные номера, электронные ключи, пароли);

– учетно-регистрационные и бухгалтерские документы (лицензии, сертификаты соответствия техники и программ, договоры на пользование компьютерным оборудованием).

Для определения порядка осмотра содержимого электронного носителя необходимо учитывать факт подключения компьютера к сети или отсутствия соединения к ней. В первом случае, сначала исследованию подвергаются сведения, содержащиеся на жестком диске главной вычислительной техники, после в устройствах памяти остальных компьютеров и на отдельных электронных носителях.

Для обеспечения сохранности данных рекомендуется перед осмотром электронно-цифровой информации скопировать её на другой носитель и исследовать копию. В целях исключения возможных сомнений участников уголовного судопроизводства о соответствии скопированной информации с её оригиналом, копирование необходимо выполнить на месте производства следственного действия.

Содержащиеся на электронном носителе текстовые данные для непосредственного восприятия человеком лучше всего распечатать. Это

позволяет удобнее использовать их в процессе доказывания. При этом распечатки подписываются участниками осмотра и в качестве приложения к протоколу следственного действия приобщаются к материалам уголовного дела. И как справедливо отмечает В.А. Камышин, всякое приложение в отдельности от протокола процессуального действия не может быть признан доказательством по уголовному делу и не имеет юридической силы[174]. Примером сказанному могут послужить материалы уголовного дела №13212 по факту хищения денежных средств фонда заработной платы работников бюджетной организации в отношении Н.Э. по ч. 2 ст. 245 УК Республики Таджикистан. Так, в ходе осмотра содержимого жёстких дисков компьютеров хозяйственного отдела и бухгалтерии были обнаружены, распечатаны и приобщены к протоколу следственного действия электронные версии табелей использования рабочего времени и ведомостей начисления заработной платы лицам, фактически не работающим в этой организации. В процессе судебного разбирательства судя ограничивался исследованием только вышеназванных распечатанных документов, их сопоставлением с оригиналами и не стал просматривать скопированные на компакт-диск данные с вышеназванных компьютеров[175].

В заключение заметим, что в зависимости от вида электронного носителя информации определяется тактика его осмотра. Осмотр всякого электронного носителя условно можно разделить на внешний осмотр и осмотр содержимого носителя. При производстве данного следственного действия необходимо учитывать особенности функционирования электронного носителя и специфику фиксации содержащейся на нём электронно-цифровой информации.

Осмотр мобильного телефона. Как показывает практика, в последнее время для получения доказательственной информации в рамках процесса доказывания часто используется осмотр мобильного телефона. Данное телекоммуникационное устройство в современном обществе используется при совершении различных видов преступлений, в частности преступлений террористического и

[174] См.: Камышин, В.А. Иные документы как «свободное» доказательство в уголовном процессе: автореф. дис. ...канд. юрид. наук. – Ижевск, 1998. – С. 12.
[175] См.: Уголовное дело №13212 // Архив ГКНБ РТ.

экстремистского характера, в сфере незаконного оборота наркотических средств и психотропных веществ, мошенничеств, экономической направленности и т.д[176].

Мобильный телефон изначально был разработан для голосовых вызовов. Затем, по прошествии некоторого времени, у него появилась функция обмена текстовыми сообщениями. С развитием информационных технологий мобильный телефон приобрёл множество функций, и тенденция по усовершенствованию его возможностей продолжается. Данное обстоятельство обусловлено, прежде всего, наличием высокой конкуренции среди производителей сотовых телефонов. В настоящее время сотовый телефон может хранить все виды информации, в том числе, криминалистически значимую, может создавать и воспроизводить текстовые, графические, аудио- и видеофайлы.

Е.И. Третьякова верно замечает, что «в настоящее время средство мобильной связи становится чаще всего не предметом преступного посягательства, а средством его совершения. И в этом случае наибольший интерес представляет не сам предмет с его внешними индивидуальными характеристиками, а информация, хранящаяся в его памяти»[177]. Действительно, мобильное устройство, являясь источником фактических данных о совершённом общественно-опасном деянии, может хранить в себе информацию о конкретных лицах, причастных к расследуемому преступлению, признаках, характеризующих внешнее проявление преступления и иные интересующие органы следствия сведения[178].

Осмотр мобильного телефона должен отвечать требованиям своевременности, объективности, полноты и активности[179]. Своевременность осмотра заключается в том, что данное следственное действие нужно проводить незамедлительно, как только в этом возникает необходимость. Промедление

---

[176] См.: Назаров А.К., Салимов Б.А. Криминалистическая тактика осмотра устройства мобильной связи (мобильного телефона) как источника доказательственной информации / А.К. Назаров , Б.А. Салимов // Наука и безопасность. – Душанбе, 2023. – №3 (5). – С. 104.

[177] Третьякова Е.И. Мобильный телефон как источник криминалистически значимой информации /Е.И. Третьякова // Вестник Уральского финансово-юридического института. – №3 (13). – С. 49-51.

[178] См.: Шувалов М.Н., Шувалова А.М. Применение криминалистической техники при расследовании коррупционных преступлений / М.Н. Шувалов, А.М. Шувалов // Гуманитарные, социально-экономические и общественные науки. – 2016. – №12. – С. 210-214.

[179] См.: Бутенко А.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия [Электронный ресурс]. – Режим доступа: https: //cyberleninka.ru/article/n/ (дата обращения: 25.07.2022).

может привести к уничтожению хранящейся в нём информации путём удалённого доступа либо повлечь к иным негативным последствиям. От своевременности производства осмотра зависит продуктивность предпринимаемых следователем мер по поиску криминалистически значимой информации.

Требование объективности обеспечивается точным запечатлением и последовательной фиксацией всего обнаруженного в ходе осмотра мобильного устройства. Осмотр должен производиться без предвзятости, предубеждений и предпочтений. В протоколе не должны отражаться выводы, заключения и предположения следователя.

Соблюдение полноты следственного осмотра позволяет выявить, фиксировать и исследовать все сведения, могущие стать доказательством по уголовному делу. Осмотр мобильного устройства необходимо провести так, чтобы не упустить ни одного значимого для следствия обстоятельства.

Требование активности осмотра включает в себя активную профессиональную позицию следователя и предполагает без дополнительных ходатайств заинтересованных лиц и указаний надзорных органов проводить данное следственное действие. Следователь должен принимать все возможные и необходимые меры для того, чтобы найти следы преступления в ходе осмотра мобильного устройства.

В целях исключения утраты и модификации доказательственной информации следователь принимает меры по недопущению участников следственного осмотра и других присутствующих лиц прикасаться к мобильному устройству и осмотр проводит в помещении, где исключено вероятность воздействия на него.

Мобильные устройства сохраняют в себе три вида следов: электронно-динамические, электронно-цифровые и следы на SIM-карте.

К электронно-динамическим следам относятся всякие сведения, сохранившиеся в памяти устройства связи, о его соединениях с другими абонентами и подключениях к компьютерным серверам посредством сетей. Эти сведения могут быть о времени, частоте и содержании подобных соединений и подключений.

Записи и отметки в телефонных книгах, в контактах, в разделе звонков, а также текстовые и другие мультимедийные файлы, настроенные программы и т.п. считаются электронно-цифровыми следами.

Следы на SIM-карте могут образоваться как при физическом контакте человека с её поверхностью, так и в результате электромагнитных взаимодействий в её памяти.

Осмотр мобильного телефона осуществляется в рамках осмотра предметов. На данное обстоятельство обращают внимание К.А. Виноградова и Л.А. Савина и справедливо отмечают, что «уголовно-процессуальное законодательство не предоставляет следователю возможность проводить осмотр электронных устройств и электронной информации в качестве самостоятельного следственного действия. Следовательно, все, что ему остается – это проводить осмотр предметов»[180]. При этом, следует отметить, что изъятие телефонных аппаратов, как правило, происходит в рамках других процессуальных действий, к числу которых можно отнести обыск, личный обыск, выемку, осмотр места происшествия, осмотр местности и осмотр помещения. Также не исключена вероятность представления мобильного аппарата с результатами оперативно-розыскной деятельности на стадии решения вопроса о возбуждении уголовного дела.

В настоящее время существуют разные мнения относительно того, в каком состоянии (включенном или выключенном) следует изымать мобильное устройство. К примеру, А.Н. Архипова сторонник изъятия мобильного телефона в выключенном состоянии. Она считает, что в процессе следственного действия необходимо в рабочем режиме исследовать содержимое мобильного устройства, в протоколе фиксировать это и сфотографировать его, затем выключить и изъять устройство. Данную рекомендацию она аргументирует тем, что к современным

[180] Виноградова К.А., Савина Л.А. Изъятие и осмотр мобильных телефонов и находящейся на них электронной информации по преступлениям, совершенным военнослужащими / К.А. Виноградова, Л.А. Савина // Вестник военного права. – 2019. – №2. – С. 55-58.

устройствам связи можно дистанционно получить доступ и тем самым модифицировать или удалить фактические данные, содержащиеся в них[181].

Г.В. Семенов высказывает противоположное мнение и отмечает, что «в случае изъятия мобильного устройства, его не следует выключать, так как его активация в дальнейшем может вызвать проблемы с разблокировкой»[182].

Представляется, что позиция А.Н. Архипова более правильная. Вместе с тем, считаем необходимым при обнаружении телефонного аппарата в ходе следственных действий, в случае невозможности его полного исследования на месте, в протоколе следственных действий фиксировать его внешнее описание, изменить коды активации устройства и пароль доступа к интернет-аккаунту пользователя, затем выключить устройство и произвести его изъятие. Данное действие исключает возможность блокировки телефонного аппарата и получения удаленного доступа подозреваемого и его сообщников, как к аппарату, так и к интернет-аккаунту. Невыполнение этих действий может привести к утрате доказательственной информации и другим неблагоприятным последствиям в ходе расследования уголовных дел.

В подтверждение сказанного можно привести в пример ситуацию, возникшую в ходе следствия по уголовному делу №23131 в отношении гражданина Республики Таджикистан Д.Д. по признакам преступления, предусмотренного ч. 2 ст. 307 (2) УК Республики Таджикистан. Так, по подозрению в участии в деятельности экстремистского сообщества сотрудниками органов национальной безопасности в г. Куляб был задержан гражданин Республики Таджикистан Д.Д. На месте задержания был оформлен протокол его задержания и личного обыска. При личном обыске у него, помимо других вещей, был изъят мобильный телефон марки «Samsung». Следователь, принимавший участие при задержании подозреваемого, произвёл только внешний осмотр мобильного устройства и в активном режиме, без изменения паролей доступа к

[181] См.: Архипова Н.А. К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений / Н.А. Архипова // Криминалистические чтения: сб. материалов. – 2014. – №10. – С. 16-17.

[182] Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций: монография. – М.: Юрлитинформ, 2008. – С. 133.

аппарату и интернет-странице пользователя, изъял телефон для дальнейшего исследования. Содержимое телефона и зарегистрированная в нём интернет-страница в «Фейсбуке» не были осмотрены по той причине, что в них было много файлов с материалами экстремистского содержания и их осмотр на месте потребовал бы продолжительное время. По прибытии в свой кабинет, следователь приглашает специалиста в области информационных технологий и приступает к детальному осмотру содержимого аппарата мобильной связи. Однако, обнаруживает, что в телефоне исчезли все файлы с экстремистскими материалами, которые он ранее видел при его изъятии на месте задержания подозреваемого. В результате организации комплекса оперативно-следственных мероприятий и при содействии подозреваемого Д.Д., который уже сотрудничал со следствием, выяснилось, что данные с его телефона и интернет-страницы вскоре после задержания были удалены его другом и единомышленником В.А. посредством удалённого доступа. Впоследствии при помощи специалистов удалось частично восстановить удалённые файлы[183].

Необходимо помнить, что в ходе осмотра мобильного устройства при составлении протокола следственного действия не следует применять бытовые выражения («симка», «флэшка» «трубка», «мобильник» и т.п.), а его результаты необходимо фиксировать с использованием официальных терминов, определяемых производителями и нормативными актами.

Осмотр мобильного устройства делится на внешний осмотр и осмотр содержимого телефона. Внешний осмотр начинается с упаковки устройства, если она есть. В протоколе следственного действия описывается материал изготовления упаковки, размеры, форма, цвет и надписи на ней. Затем фиксируются нижеследующие признаки мобильного телефона:

– модель (тип) телефона, его серийный и идентификационные номера;

– материал, из которого изготовлен корпус телефона (пластмассовый или частично металлический), его целостность;

[183] См.: Уголовное дело №23131 // Архив ГКНБ РТ.

– наличие и характеристика клавиатуры, сетевых индикаторов, разъёмов и портов для подсоединения аксессуаров;

– свойство дисплея и содержащаяся на нём информация во включённом состоянии (фиксируются все значки и их характеристики).

При осмотре содержимого мобильного телефона необходимо иметь в виду, что он содержит несколько групп информации, в том числе список вызовов, контактов, принятые и отправленные сообщения, установки и т.д. Вся электронно-цифровая информация в мобильном устройстве хранится в файлах в виде фотоизображений, видеоклипов, аудио-звуков, текстовой, числовой и графической информации.

Для активизации функций телефона понадобится пароль и для получения доступа к данным SIM-карты – PIN-код. Получить информацию о PIN-коде можно в сотовых компаниях, для чего необходимо направить следственный запрос.

В случае, если в ходе следственного действия не удаётся установить пароль мобильного устройства и его собственник всячески воспрепятствует активизации телефона, то проводится только внешний осмотр устройства и подключенной к нему SIM-карты. Вместе с тем, мобильный телефон изымается для детального исследования в рамках судебной компьютерно-технической экспертизы.

Информационное содержание мобильного устройства исследуется с помощью специалиста. При необходимости следователь может привлекать к осмотру владельца мобильного телефона. Каждое действие с устройством связи должно быть пояснено понятым и другим участникам осмотра. В протоколе не обязательно отражать всю информацию, содержащуюся в мобильном телефоне, которая не имеет доказательственное значение. Вместе с тем, относящаяся к расследуемому событию информация описывается подробно, с указанием всех произведённых действий с телефоном.

При осмотре в первую очередь устанавливается идентификационный номер (IMEI-код) мобильного телефона. Его можно определить путём нажатия комбинации цифр «*#06#». При наличии SIM-карты устанавливается его номер и

оператор мобильной связи. Для определения номера SIM-карты у различных операторов сотовой связи есть своя комбинация цифр.

Большое значение для расследования имеет информация, хранящаяся в разделе «Телефонная записная книга» («Контакты» и др.), где содержатся телефонные номера контактов заподозренного лица, то есть круг его общения.

Также, существенные сведения о расследуемом преступлении и лиц, причастных к его совершению, могут храниться в разделе «Звонки» мобильного аппарата. В данном разделе в автоматическом режиме сохраняется информация об исходящих, принятых и непринятых вызовах. При составлении протокола осмотра необходимо фиксировать дату, время начала и время завершения соединения осматриваемого абонента с конкретным номером.

Информация о SMS (Short Message Service – служба коротких сообщений), MMS (Multimedia Messaging Service – система передачи мультимедийных сообщений (изображений, мелодий, видео), EMS (Enhanced Messaging Service – улучшенная служба сообщений), голосовых сообщениях и отчёт о доставке этих сообщений содержится в разделе «Сообщения». Он включает в себя сведения о дате и времени полученных и отправленных сообщений, а также номера абонентов, которые отправили или получили соответствующие сообщения. Входящие и исходящие сообщения, кроме текста, также могут содержать фотографии, видео- и звукозаписи. В протоколе осмотра подробно отражаются данные о сообщениях и их содержании, а в необходимых случаях эти сведения могут быть распечатаны или скопированы на электронном носителе и как приложение приобщены к нему.

Таким образом, можно подытожить, что в современном обществе мобильные телефоны широко используются в механизме совершения большого количества общественно-опасных деяний и в связи с чем, они являются источником криминалистически значимой информации. Исследование мобильного устройства происходит в рамках следственного осмотра предметов. Данное следственное действие нужно проводить незамедлительно, как только в этом возникает необходимость, при соблюдении требований объективности, полноты и

активности. В целях исключения возможности блокировки и получения удаленного доступа подозреваемого и его сообщников, как к аппарату, так и к его интернет-аккаунту, при изъятии мобильного телефона необходимо изменить коды активации устройства и пароль доступа к интернет-аккаунту пользователя, затем выключить устройство и произвести его изъятие. Невыполнение этих действий может привести к утрате доказательственной информации и другим неблагоприятным последствиям в ходе расследования уголовных дел.

Особенности следственного осмотра ресурсов сети Интернет. Осмотр интернет-страницы и интернет-сайта. Особенность исследования данных, содержащихся на ресурсах глобальной сети, зависит от специфики функционирования сети Интернет. При совершении преступных действий с использованием возможностей сети Интернет место преступления часто остается не определённым, в связи с чем, поиск криминалистически значимой информации следует осуществлять на местах:

– обработки и хранения электронно-цифровой информации;

– применения компьютерной техники с выходом в глобальную сеть в преступных целях;

– хранения данных, полученных при совершении преступлений с использованием возможностей сети Интернет;

– нахождения информационной системы, предназначенной для хранения, поиска и обработки данных, на которую совершено преступное посягательство;

– нарушения правил эксплуатации средств обращения с компьютерными данными и сетями, ставших предметом преступного посягательства;

– наступления общественно-вредных последствий от совершения преступлений.

Исследование вышеуказанных мест осуществляется в рамках осмотра места происшествия. Порядок производства данного вида осмотра и фиксации доказательственной информации применительно к электронным носителям выше нами рассмотрен, и здесь повторяться не будем.

Интернет-страница или веб-страница – документ или информационный

ресурс Всемирной паутины, доступ к которому осуществляется с помощью веб-браузера[184]. Слово «веб» происходит от сокращённого английского названия Всемирной сети: WWW, W3 или Web. Сеть, паутина или веб – всемирная система публичных веб-страниц в сети Интернет. Сеть не является Интернетом, она лишь использует Интернет как среду передачи информации и данных.

Типичная веб-страница представляет собой текстовый файл в формате HTML, который может содержать ссылки на файлы в других форматах (текст, графические изображения, видео, аудио и прочее), а также гиперссылки для быстрого перехода на другие веб-страницы или доступа к ссылочным файлам. Информационно значимое содержимое веб-страницы обычно называется контентом (от англ. content – «содержание»).

Несколько веб-страниц, объединённых общей темой и дизайном, а также связанных между собой ссылками, образуют веб-сайт (интернет-сайт)[185].

При осмотре информации, размещённой на веб-страницах или веб-сайтах, необходимо определить, каким способом она размещена в сети. Размещать информацию произвольного характера можно как на страницах популярных ресурсов, таких как социальные сети, форумы, блоги и т.п, имея при этом минимальные знания в области информационных технологий, так и на собственно созданные полнофункциональные веб-сервисы[186] (казино, онлайн-тотализаторы, ресурсы интернет-мошенничества).

Исследование интернет-страницы в рамках осмотра можно осуществить путём её открытия на персональном устройстве пользователя, на другом электронном устройстве, а также посредством другой страницы в социальных сетях.

Анализ правоприменительной деятельности показал, что чаще всего фиксация электронно-цифровых доказательств на ресурсах сети Интернет

---

[184] Браузер или веб-обозреватель – прикладное программное обеспечение для просмотра страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения иных задач.

[185] См.: Веб-страница [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/ (дата обращения: 19.07.2022).

[186] Веб-сервис (Веб-служба) – идентифицируемая уникальным веб-адресом (URL- адресом) программная система со стандартизированными интерфейсами.

осуществляется путём осмотра интернет-страницы в социальной сети участника уголовного судопроизводства на его персональном компьютере или ином электронном устройстве. Конечно, для открытия страницы в социальной сети необходимо вводить логин и пароль, их может предоставить пользователь. Однако, большинство пользователей социальных сетей для удобства и экономии личного времени в своих устройствах настраивают функцию автосохранения, при активизации которой логин и пароль вводятся в автоматическом режиме и повторный их ввод не требуется. Так, например, в рамках расследования уголовного дела №22909, 22 сентября 2022 года по подозрению в причастности к деятельности экстремистской организации был задержан гражданин Х.Р. При личном обыске у него был изъят мобильный телефон и осмотрен. В связи с тем, что в мобильном устройстве была активирована функция автосохранения, следователю без проблем удалось войти в его интернет-страницу под названием «АХИ» в социальной сети «Телеграмм» и осмотреть её содержимое, где были размещены материалы экстремистского содержания, в основном, видеозаписи[187].

В случаях, когда осмотр страницы в социальной сети невозможно производить на устройстве участника уголовного судопроизводства в связи с его отсутствием, данное следственное действие осуществляется посредством электронного устройства следователя. Однако данный способ, как справедливо отмечает А.Г. Себякин, имеет определённые недостатки. Он к числу недостатков относит невозможность осмотра интернет-страницы, если пользователь является участником закрытой группы, а также отсутствие анонимности осмотра. То есть, функциональная система интернет-ресурса при обращении стороннего пользователя к странице фиксирует данный факт и об этом направляет оповещение владельцу страницы. В данном случае, в зависимости от следственной ситуации, повышается риск утраты информации на интернет-странице, поскольку её содержимое может быть изменено или удалено пользователем в любой момент[188].

---

[187] См.: Уголовное дело №22909 // Архив ГКНБ РТ.

[188] См.: Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. ... канд. юрид. наук. – М., 2021. – С.141.

Также, нельзя не соглашаться с мнением А.Н. Колычевой, которая считает, что при исследовании страницы в социальной сети могут возникнуть проблемы, связанные с анонимностью пользователя. Данное обстоятельство позволяет последнему свободно и легко получить доступ к содержимому страницы и управлять им, то есть размещать информацию, модифицировать её, распространить и удалить её первоисточник[189].

Учитывая особенности следообразования электронно-цифровых следов, в протоколе осмотра страницы социальной сети необходимо отразить следующие данные:

– название социальной сети («Instagram», «Facebook», «Одноклассники», «Twitter» и т.д.), в которой размещена веб-страница;

– способ осмотра страницы;

– ID пользователя и его идентификационные данные;

– число «подписчиков»;

– повторяемость посещения интернет-страницы пользователем;

– сведения об общении с другими пользователями социальных сетей;

– информация о графическом представлении пользователя и иных криминалистически значимых фотографиях на странице;

– данные о текстовых и мультимедийных файлах и комментарии к ним;

– полные сведения о группах, в которых зарегистрирован пользователь и т.п.

Наряду с протокольной фиксацией электронно-цифровых доказательств, также для наилучшего восприятия доказательственной информации можно применять фото и видеозапись. На практике чаще всего для фиксации исследуемых следов используют, так называемые скриншоты с внесением в протокол все процедуры в установленном процессуальном порядке. Скриншот (англ. screenshot) – это снимок экрана монитора электронно-вычислительной машины. Снимок экрана осуществляется нажатием клавиши «Print Screen», после полученный снимок можно вставить в документ в формате Word для дальней

[189] См.: Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. … канд. юрид. наук. – Москва, 2018. – С.11.

распечатки. Используя данную клавишу, можно запечатлеть ситуацию, как на компьютере, так и на веб-странице. Обычно страница социальной сети имеет много вертикального контента, и при фотографировании страницы следует использовать такой приём, как панорамирование.

В настоящее время единого способа придания снимкам экрана процессуальной формы не разработано. На практике приобщение скриншотов к материалам уголовного дела происходит путём включения их в описательную часть протокола осмотра, размещение снимков в фототаблицу и копирование на электронном носителе, таких как флэш-карта, компакт-диск и т.п.

В распечатке снимка экрана следует фиксировать дату и время снятия снимка, адрес интернет-страницы (URL), свойства технических и программных средств, использованных для осмотра, в том числе принтер, на котором произведена распечатка, данные о провайдере и другие сведения.

Осмотр электронной почты. Электронная почта – технология и служба по пересылке и получению электронных сообщений между пользователями компьютерных сетей. По принципу работы она практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, конверт, вложение, ящик, доставка и другие), так и характерные особенности – простоту использования, задержки передачи сообщений, достаточную надёжность и, в то же время, отсутствие гарантии доставки[190].

На практике можно встретить различные варианты написания электронной почты: электронная почта, эл.почта, интернет-почта, «email», «e-mail», имейл (транскрипция с английского), е-мейл, емейл, емайл, е-мэйл, мейл.

Электронная почта в зависимости от активности пользователя может быть источником большого объёма криминалистически значимой информации. Посредством исследования её содержимого можно установить многие обстоятельства, подлежащие доказыванию по уголовному делу, в том числе, время, место и механизм совершения общественно-опасного деяния, круг

[190] См.: Электронная-почта [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki (дата обращения: 20.07.2022).

соучастников расследуемого преступления, а также иные обстоятельства, представляющие оперативный интерес. Так, например, в ходе расследования уголовного дела №15337 по обвинению гражданина Республики Таджикистан Р.Х. в совершении преступлений, предусмотренных ч. 4 ст. 200 (Незаконный оборот наркотических средств) и ч. 4 ст. 289 (Контрабанда наркотических средств, совершённая организованной группой) УК Республики Таджикистан, в его мобильном телефоне была выявлена электронная почта. При осмотре содержимого электронной почты в папках «Принятые сообщения» и «Отправленные сообщения» была обнаружена переписка обвиняемого с другими членами организованной группы. Анализ обнаруженных данных позволил установить личность и роль каждого в совершённом общественно-опасном деянии, а также получить криминалистически значимые сведения о времени, месте и механизме совершения контрабанды через государственную границу, а также представляющие оперативный интерес данные о действующих каналах переброски наркотических средств с территории Афганистана[191].

Исследование электронной почты и фиксация содержащейся на ней информации возможно путём осмотра почты на электронно-вычислительной машине участника уголовного судопроизводства, материального носителя с электронной перепиской, представленного почтовым сервисом, и бумажного носителя с содержанием электронной почты. В последнем случае применяется правила осмотра обычных документов.

Порядок осмотра электронной почты, в принципе, аналогичен тактике осмотра интернет-сайтов. Посредством браузера, путём введения пароля открывается электронная почта, исследуется её содержимое и обнаруженные искомые данные о расследуемом событии, а также иные сведения, идентифицирующие обследуемую почту, фиксируются в протокольной форме и методом снятия скриншотов. Следует отметить, что при работе с электронной почтой специалисты могут использовать программу почтовые клиенты. Это необходимо для получения доступа к электронной почте. Основные функции

[191] См.: Уголовное дело №15337 // Архив ГКНБ РТ.

почтовых клиентов это приём сообщений, обеспечение их просмотра, сортировка сообщений, автоматизация создания ответных сообщений и поддержка адресной книги.

Осмотр данных об интернет-соединениях, полученных от провайдеров. Интернет-провайдеры предоставляют сведения об интернет-соединениях на основании запроса органов следствия. В связи со сложностями в восприятии предоставляемых данных, следователь, производящий осмотр, часто испытывает затруднения в составлении протокола следственного действия, так как не всегда имеет необходимые навыки для анализа подобных сведений и понимание о том, что следует отразить в нём. На данное обстоятельство обращает внимание Д.А. Илюшин и верно замечает, что «следователи и оперативные сотрудники не всегда понимают юридическую силу статистических сведений, предоставленных оператором связи, с отраженной в них информацией»[192].

Специфика формирования статистических сведений об интернет-соединениях заключается в том, что провайдеры на основании договора о предоставлении услуг, в электронном виде фиксируют интернет-соединения каждого абонента. Данная статистика предоставляется правоохранительным органам, как в электронной форме, так и на бумажном носителе. Для придания юридической силы необходимо в процессуальном порядке протоколировать полученную информацию.

Сведения обо всех действиях и манипуляциях в информационно-телекоммуникационных сетях, в том числе в сети Интернет последовательно в автоматическом режиме фиксируются в устройствах памяти электронных средств и log-файлах сетевого оборудования интернет-провайдеров и сайтов. Каждое событие записывается отдельно с указанием временных параметров в сетевых протоколах.

Сетевой протокол представляет собой набор правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между

[192] Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дис. ... канд. юрид. наук. – Волгоград, 2008. – С. 130-140.

двумя и более включёнными в сеть устройствами[193].

Записи в протоколах о соединениях с глобальной сетью бывают трех видов: start, update и stop, каждый из которых занимает одну строчку. Первый тип записи означает начало сеанса, второй – вспомогательная информация о сеансе и третий – окончание сеанса.

Эти записи включают в себя такие параметры, как дата и время соединения, IP-адрес маршрутизатора, имя учётной записи пользователя, название линии и другие сведения. Данные записи подлежат обязательной фиксации в протоколе осмотра.

Несмотря на то, что нормы уголовно-процессуального законодательства не предусматривают обязательное участие специалиста при осмотре данных об интернет-соединениях, однако плодотворным считается их исследование с его участием. По результатам осмотра составляется протокол и в отдельных случаях для внесения ясности в определённых технических моментах можно допросить специалиста.

Как мы выше отметили, важным аспектом при проведении различных видов осмотра, сопряжённых с ресурсами сети Интернет, является распечатывание на бумажном носителе криминалистически значимой электронной информации. Подобные распечатки, сделанные с соблюдением уголовно-процессуальных норм в рамках следственных действий, послужат доказательствами по уголовным делам. В этом отношении А.Л. Осипенко справедливо отмечает, что любые формы вывода электронно-цифровой информации, в том числе распечатка, допустимы для того, чтобы человек непосредственно её воспринимал[194].

Таким образом, можно утверждать, что особенность следственного осмотра электронно-цифровых доказательств на ресурсах сети Интернет, обусловлена спецификой функционирования глобальной сети. Самыми распространёнными источниками фактических данных о совершённом преступлении, содержащихся в

---

[193] См.: Протоколы + соединения [Электронный ресурс]. – Режим доступа: https://www.google.com/search?q (дата обращения: 21.07.2022).

[194] См.: Осипенко А.Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс / А.Л. Осипенко // Научный вестник Омской академии МВД России. – 2009. – №4(35). – С. 31-34.

сети Интернет, являются веб-страница, веб-сайт, электронная почта и статистические сведения об интернет-соединениях электронного устройства участника уголовного судопроизводства. Результаты осмотра электронно-цифровой информации в сети Интернет оформляется протоколом.

Анализ материалов уголовных дел свидетельствуют о том, что сведения, содержащиеся на ресурсах сети Интернет, имеют большое значение в расследовании преступлений и их исследование позволяет получить неопровержимые доказательства виновности конкретных лиц в совершении общественно-опасного деяния, а также установить подлежащие доказыванию обстоятельства по уголовным делам.

С учётом изложенного в данном параграфе, можно подытожить следующее.

Самым распространённым и информативным способом фиксации электронно-цифровых доказательств на локальных и сетевых носителях является следственный осмотр. Исследование электронных носителей и их содержимого происходит в рамках таких следственных действий, как осмотр места происшествия, осмотр помещения, осмотр предметов и осмотр документов, так как законодательство не предусматривает иное самостоятельное процессуальное действие по их осмотру. Невзирая на то, что законодатель не обязывает органы следствия привлекать при осмотре рассмотренных объектов специалиста, однако в целях полной, объективной и качественной фиксации криминалистически значимой информации, его участие считается необходимым. Фиксация содержания и результатов осмотра должна осуществляться в протокольной форме с соблюдением определённых правил. Помимо протокольной фиксации электронно-цифровых доказательств, для наилучшего их познания рекомендуется применять фото и видеозапись. При оформлении результатов осмотра также необходимо использовать так называемые скриншоты с внесением в протокол все процедуры в установленном процессуальном порядке.

На основании собранных в ходе осмотра доказательств, следователь принимает решение о необходимости производства судебной компьютерно-технической экспертизы.

2.3. Судебная компьютерно-техническая экспертиза как процессуальное средство исследования электронно-цифровой информации и её носителей

Начиная с 90-х годов прошлого столетия, с началом формирования цифрового общества и использования электронно-цифровых следов в процессе доказывания, возникла потребность в судебной компьютерно-технической экспертизе (далее СКТЭ). В нынешних условиях эффективное расследование и полное раскрытие преступлений, сопряженных с использованием электронно-вычислительных систем, а также собирание и исследование доказательств по ним невозможно осуществить без применения специальных познаний в области информационных технологий. Самой результативной формой процессуального использования специальных познаний по делам данной категории является СКТЭ.

Следует отметить, что использование термина «судебная компьютерно-техническая экспертиза» является оптимальным для определения названия этого вида экспертизы, так как по смыслу он объединяет в себе как само электронно-вычислительное устройство, так и его составляющие, информационные данные, программное обеспечение, а также составные части информационно-телекоммуникационной сети. И здесь Е.Р. Россинская совершенно верно отмечает, что «вид экспертизы, в ходе каких изучается техника и её компоненты, называется компьютерно-технической экспертизой, потому что своим началом вычислительная (или же компьютерная) техника напрямую обязана как раз инженерно-техническим наукам. Известный термин «компьютерная техника», который исторически включает в себя все виды обеспечения автоматизированных систем управления (математическое, лингвистическое, техническое, программное, информационное и другие), по сути, является прародителем сегодняшнего названия СКТЭ»[195].

СКТЭ входит в систему судебных экспертиз и относится в класс инженерно-технических экспертиз[196]. Суть СКТЭ заключается в исследовании электронно-

[195] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. – М.: Норма: Инфра-М, 2018. – С.233.
[196] См.: Криминалистика: учебник / Отв. ред. В.П. Лавров, Р.Х. Рахимзода, А.Ф. Волынский. –Душанбе, 2022. – С. 376.

цифровой информации, технических и программных средств, а также информационно-телекоммуникационных сетей в целях выявления и фиксации фактических данных о совершённом преступлении. На наш взгляд, наиболее удачно сформулировал понятие рассматриваемого вида экспертизы Усов А.И., который считает, что «судебная компьютерно-техническая экспертиза – самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимая в целях определения статуса объекта как компьютерного средства, выявления и изучения его следовой картины в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним её исследованием»[197]. Вместе с тем, отнесение СКТЭ к названному классу экспертиз не является окончательным, так как стремительное развитие информационных технологий несомненно приводит к формированию нового специфического класса информационно-технологических экспертиз, куда будет включена и судебная компьютерно-техническая экспертиза.

Схожее с Усовым А.И. определение даётся Е.Р. Россинской и Е.И. Галяшиной, по мнению которых «судебные компьютерно-технические экспертизы производятся в целях определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним её исследованием»[198]. В целом данное определение характеризует сущность данных экспертиз. Тем не менее, А.Р. Сысенко, И.С. Смирнова и С.Е. Тимошенко считают, что Е.Р. Россинская и Е.И. Галяшина неоправданно узко трактуют СКТЭ как техническое средство. Они данное утверждение обосновывают тем, что при расследовании сетевых преступлений главной задачей является установление наличия общественно-опасного деяния и причастности конкретного лица к его совершению путём выявления и фиксации электронно-цифровых следов в глобальной сети. В связи с чем, компьютер, его

[197] Усов А.И. Основы методического обеспечения судебно-экспертного исследования компьютерных средств и систем. – М.: Право и закон, 2002. – С. 33-36.
[198] Российская Е.Р., Галяшина Е.И. Настольная книга судьи: судебная экспертиза. – М.: Проспект, 2011. – С. 275.

периферийные устройства и носители электронных данных могут выступать в качестве объектов СКТЭ, но не всегда являются предметами экспертного исследования. Техническое исследование электронно-вычислительной техники не всегда приводит к достижению целей расследования сетевого преступления, главным аспектом здесь считается установление обстоятельств использования компьютера для совершения преступления[199].

В научной литературе единого подхода к классификации СКТЭ нет, разными учёными выделяются от двух то пяти видов данных экспертиз.

На первоначальном этапе развития СКТЭ выделялись всего два её вида: программно-техническая и техническая экспертиза компьютеров и их комплектующих[200]. Целью первого вида СКТЭ являлось исследование информации, хранящейся в устройствах памяти компьютера и иных электронных носителях. Второй вид СКТЭ проводился для исследования технических свойств и состояния электронно-вычислительной техники, её комплектующих, электронных носителей, информационно-телекоммуникационных сетей, а также для выявления причин и условий возникновения неисправностей в их работе.

Е.Р. Россинская и А.И. Усов в зависимости от объекта исследования и характера применяемых специальных знаний, условно выделяют судебную аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную и компьютерно-сетевую экспертизы[201].

Судебная аппаратно-компьютерная экспертиза проводится для изучения технических средств компьютерной системы. В качестве предмета данного вида экспертизы выступают факты и обстоятельства, подлежащие установлению путём исследования закономерностей эксплуатации данных средств, в том числе материальных носителей информации. Её объектами могут быть персональные компьютеры, как настольные, так и портативные, их системные блоки, жёсткие

---

[199] См.: Сысенко А.Р., Смирнова И.С., Тимошенко С.Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы / А.Р. Сысенко, И.С. Смирнова, С.Е. Тимошенко // Сибирское юридическое обозрение. – 2020. – Том 17, – №4., – С. 524-532.

[200] См.: Андреев Б. В., Пак П. Н., Хорст В. П. Расследование преступлений в сфере компьютерной информации. – М.: Юрлит- информ, 2001. – С. 64.

[201] См.: Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. – М.: Норма: Инфра-М, 2018. – С. 236.

диски, периферийные устройства, принтеры, сетевые аппаратные средства, планшеты, мобильные телефоны и т.п.

Судебная программно-компьютерная экспертиза проводится в отношении программного обеспечения электронно-вычислительной системы. Естественность разработки и применения программного обеспечения компьютерной техники являются предметом её экспертного исследования. Она назначается в целях установления предназначения представленного на исследование программного средства, его характеристик, структурных особенностей, алгоритма функционирования, а также текущего состояния. В качестве объекта выступают операционные системы (ОС MS DOS, Windows, Unix и др.), вспомогательные программы (утилиты и др.), прикладные программные обеспечения (MS Office, PhotoShop и др.).

Судебная информационно-компьютерная экспертиза назначается для исследования информации, запечатлённой в электронно-цифровой форме. Данный вид экспертизы является ключевым, так как она позволяет решить большинство диагностических и идентификационных задач, сопряжённых с электронно-цифровой информацией. Её целью является поиск, обнаружение и исследование электронно-цифровой информации, созданной человеком или зафиксированной программами по организации информационных процессов в компьютерных системах. Текстовые и графические документы, информация в мультимедийной форме (видео, аудио и т.п), данные в форматах баз данных и другие сведения являются типичными объектами названного экспертного исследования.

Исследование компьютерных систем, соединённых сетевыми информационными технологиями, осуществляется в рамках судебной компьютерно-сетевой экспертизы. В качестве предмета данного вида СКТЭ выступают события и обстоятельства, возникающие вследствие использования сетевых и телекоммуникационных систем. Здесь особое место отводится экспертному исследованию фактов и обстоятельств, сопряжённых с интернет-технологиями. Следует отметить, что для судебной компьютерно-сетевой

экспертизы объекты исследования отдельно не выделяются. Здесь устанавливается функциональное предназначение и связь вышеупомянутых объектов к сетевым технологиям. К примеру, определение места, роли и предназначение какого-либо аппаратного устройства в сети.

В.А. Мещеряков предлагает разделить СКТЭ на аппаратно-техническую, программно-технологическую, информационную и интегральную компьютерно-техническую экспертизы[202].

Объекты и задачи первых три вида во многом совпадают с аналогичными видами классификации, предложенной Е.Р. Россинской и А.И. Усовым. Вызывает интерес четвёртый вид данной классификации – интегральная компьютерно-техническая экспертиза.

По мнению В.А. Мещерякова, интегральная компьютерно-техническая экспертиза назначается в целях установления возможности и действительного использования компьютерной техники для решения некоторых технических задач.

В предложенной В.А. Мещеряковым классификации отсутствует вид экспертизы, предназначенной для исследования вопросов, связанных с использованием сетевых технологий. Он считает, что решение вопросов относительно исследования возможностей технических комплексов или предназначения программного обеспечения в сетевом пространстве возможно в рамках соответствующих видов компьютерно-технических экспертиз.

Действительно, в отдельных случаях в рамках указанных видов экспертиз можно проводить исследование и ответить на вопросы, разрешение которых другие авторы ставят перед компьютерно-сетевой экспертизой. Например, в рамках судебной аппаратно-компьютерной экспертизы существует возможность установления выхода в сеть Интернет посредством представленного на исследование технического устройства, в ходе программно-компьютерной экспертизы – предназначение программных средств и путём назначения

[202] См.: Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж: Изд-во Воронеж. гос. ун-та, 2002. – С. 325.

информационно-компьютерной экспертизы выяснить наличие на представленном электронном носителе информации, свидетельствующей о работе в сети Интернет в определённый период времени.

Однако данный подход не всегда может отвечать интересам следствия, так как может возникнуть такой случай, при котором в ходе установления обстоятельств преступления, совершённого путём удалённого доступа, потребуется специальные знания в сфере сетевых технологий для обобщения данных об объектах исследования, формировании представления о картине происшествия и формулировании окончательных выводов.

А.А. Бессоновым выделяется и такой вид СКТЭ, как «судебная информационно-аналитическая экспертиза». В рамках данного вида экспертизы исследуются сведения о соединениях абонентов мобильной связи и персональных устройств в определённый период времени на интересующей следствие местности, т.е. месте совершения преступления[203]. Данное исследование позволяет установить соединения абонентов, их номера, IP-адреса и иные сведения, с помощью которых можно выявить взаимосвязь между действием в компьютерной системе и конкретным лицом, а также установить примерное его местонахождение.

Порядок назначения и производства экспертизы регламентирован главой 24 Уголовно-процессуального кодекса Республики Таджикистан. Так, согласно положениям ст. 208 УПК Республики Таджикистан при необходимости в судебной экспертизе, следователь, в производстве которого находится уголовное дело, принимает об этом решение в форме постановления. В постановлении о назначении экспертизы отражаются основания для её назначения, установочные данные эксперта или наименование учреждения, которому поручается проведение экспертизы, вопросы, необходимые решить и материалы, предоставляемые в распоряжение эксперта.

[203] См.: Бессонов А.А. Особенности использования специальных знаний при расследовании незаконной добычи рыбных ресурсов / А.А. Бессонов // Эксперт-криминалист. – 2015. – №3. – С. 3.

Анализируя положения уголовно-процессуального законодательства Республики Таджикистан можно определить порядок назначения СКТЭ. Во-первых, устанавливается необходимость в производстве экспертизы. После, определяется вид экспертизы и учреждение, которому будет поручено её производство. Далее составляется перечень вопросов для решения в рамках СКТЭ и определяются материалы, предоставляемые в распоряжение экспертного учреждения.

Следует отметить, что вопросы, решаемые в рамках СКТЭ, не включены согласно ст. 209 УПК Республики Таджикистан в перечень обстоятельств, для установления которых назначение и производство экспертизы обязательно. В связи с этим, при принятии решения о назначении экспертизы следователь должен уяснить два момента. Во-первых, требуются ли специальные познания для решения возникших проблем в ходе предварительного следствия. Во-вторых, необходимо ли для решения возникших вопросов назначение СКТЭ.

Итак, могут возникнуть различные следственные ситуации. В одних применение специальных компьютерных знаний считается необходимым (например, для решения вопроса о наличии на жестком диске электронно-вычислительной техники специальных программ, с помощью которых возможно обойти лицензионные средства защиты), в других – решение о применении специальных знаний, то есть назначение экспертизы, принимается по усмотрению следователя (например, для установления факта набора на компьютере текста фиктивного договора может не требоваться специальные знания). Например, в процессе расследования уголовного дела №13212 в отношении гражданина Н.Э. по ч. 2 ст. 245 (Присвоение или растрата) УК Республики Таджикистан выяснилось, что фиктивно составленные трудовые договоры о принятии на работу в бюджетное учреждение лиц, фактически не работающих в нём, были удалены с компьютера бухгалтерии. Для восстановления и изъятия фиктивных договоров при осмотре компьютера был привлечён специалист в области информационных технологий, которому удалось с применением специальных

программ восстановить на диске D удалённые файлы, и тем самым миновала необходимость в назначении СКТЭ[204].

Приведенный пример свидетельствует о том, что существует возможность вместо СКТЭ использовать иные формы применения специальных знаний. Так, УПК Республики Таджикистан, наряду с проведением судебной экспертизы, предусматривает право следователя вызвать для участия в производстве следственных действий специалиста соответствующего профиля (ст. 179), который, имея специальные знания в области компьютерной техники, может решить вопросы по поиску, обнаружению и фиксации доказательственной информации без экспертного исследования. Согласно ст. 57 УПК Республики Таджикистан специалист не заинтересован в исходе уголовного дела и ввиду его компетентности в той или иной области науки и техники привлекается к расследованию уголовного дела в целях оказания содействия следователю в поиске, обнаружении и фиксации доказательств, их обосновании, а также в использовании технических средств[205].

Специалист представляет свои суждения по поставленным перед ним вопросам в письменном виде, в форме заключения. Также, положения ч. 2 ст. 72 УПК Республики Таджикистан допускает допрос специалиста об обстоятельствах, требующих специальных познаний, а также для разъяснения им своих суждений. Так, например, при расследования уголовного дела №22903, возбужденного по признакам преступления, предусмотренного ч. 2 ст. 307(3) УК Республики Таджикистан, в ходе осмотра мобильного телефона подозреваемого Дж.Б. был привлечён специалист соответствующего профиля. В результате проведенного осмотра на интернет-странице Дж.Б. в социальной сети «Фейсбук» были обнаружены 6 видеозаписей экстремистского содержания. По поручению надзирающего прокурора, в целях установления обстоятельств получения и распространения данных материалов, был допрошен привлечённый специалист. В ходе допроса специалист на основе алгоритма функционирования компьютерной

[204] См.: Уголовное дело №13212 // Архив ГКНБ РТ.
[205] Уголовно-процессуальный кодекс Республики Таджикистан от 03.12.2009 // Ахбор Маджлиси Оли Республики Таджикистан. – 2016. – №3. – ст.128.

сети и сохранившихся на мобильном устройстве электронно-цифровых следов дал подробное разъяснение об источниках появления этих записей в телефоне, а также назвал электронные адреса, куда они были направлены, после скачивания[206].

Необходимо признать, что в условиях Республики Таджикистан выбор экспертного учреждения для проведения СКТЭ не большой и как показывает проведенный опрос следователей органов национальной безопасности, все, кто в рамках уголовных дел назначал СКТЭ, то её производство поручал Республиканскому центру судебных и криминалистических экспертиз Министерства юстиции Республики Таджикистан.

Вместе с тем, уголовно-процессуальное законодательство предусматривает возможность назначения и проведения СКТЭ в иностранном государстве. Так, согласно ст. 470 УПК Республики Таджикистан при необходимости проведения на территории иностранного государства отдельных следственных и судебных действий, в частности СКТЭ, следователь поручает их производство компетентным органам иностранного государства. При этом, важным условием для этого является наличие международного договора с этим государством об оказании взаимной правовой помощи. Данный механизм может быть применён в случае отсутствия возможности проведения определённого вида СКТЭ на территории Республики Таджикистан либо ввиду повышенной сложности предстоящего экспертного исследования.

Республика Таджикистан в период своей независимости подписала и ратифицировала ряд двусторонних договоров об оказании правовой помощи с иностранными государствами, а также является участником двух международных конвенций по правовым отношениям, к числу которых относятся Минская конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 22 января 1993 года и Кишинёвская конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам от 07 октября 2002 года. В соответствии со ст. 10 последней

[206] См.: Уголовное дело №22903 // Архив ГКНБ РТ.

Конвенции «учреждения юстиции Договаривающихся Сторон (государства-участники Содружества Независимых Государств) оказывают взаимную правовую помощь в организации и проведении экспертиз по гражданским, семейным и уголовным делам в специальных экспертных, научно-исследовательских и иных компетентных учреждениях Договаривающихся Сторон. Заключения экспертов, данные в запрашиваемой Договаривающейся Стороне в соответствии с законодательством этой Договаривающейся Стороны, имеют такую же юридическую силу и в запрашивающей Договаривающейся Стороне и принимаются учреждениями юстиции этой Договаривающейся Стороны без какого-либо специального удостоверения»[207].

После определения экспертного учреждения важным моментом является формулировка вопросов для разрешения СКТЭ. На данном этапе целесообразным считается предварительная консультация и согласование вопросов с экспертами в целях устранения возможных трудностей в исследовании. Однако, как показывает практика, следователи редко согласовывают вопросы с экспертами, так как перечень вопросов типовой, и они берут их друг у друга.

Необходимо отметить, что выносимые на разрешение экспертов вопросы зависят от обстоятельств, при которых совершено преступление, предоставляемых на исследование объектов, наличия образцов для сравнительного исследования и др.

Для эффективного решения поставленных перед экспертами задач необходимо соблюдать требования, предъявляемые к вопросам, выносимым на СКТЭ. На практике эти требования разделяются на две группы. Первая группа характерна любым вопросам, выносимым на СКТЭ, и называют их общими требованиями. Вторая группа требований именуется частными требованиями и они присущи вопросам, относящимся к конкретному виду СКТЭ.

Общие требования заключаются в следующем:

---

[207] Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (07 октября 2002 г., г. Кишинёв) [Электронный ресурс]. – Режим доступа: URL: https://cis.minsk.by/page/614 (дата обращения: 23.05.2022).

– при составлении вопросов необходимо исключить жаргонные и непрофессиональные термины («флэшка», «симка», «винчестер» и т.п.) и использовать только тот понятийный аппарат, который определён нормативными актами и документациями производителей компьютерных и программных средств;

– вопросы не должны носить справочный характер, а быть понятными и однозначными;

– вопросы должны быть поставлены в пределах правомочности и компетентности эксперта и не иметь правовой характер;

– необходимо соблюдать соответствие вопросов имеющейся методической и технической базе экспертного учреждения;

Анализ изученных уголовных дел показал, что следователи при назначении СКТЭ часто допускают ошибки при формулировке вопросов эксперту. Самой грубой ошибкой при этом является постановка вопросов правового характера, которые выходят за компетенцией специалиста, что не следует допустить. Подобная постановка вопроса может привести к смешению полномочий следователя, как участника процесса, осуществляющего уголовное преследование, и эксперта, как участника, не заинтересованного в исходе уголовного дела. Например, при расследовании уголовного дела №22834 в отношении гражданина К.Ф.Ш. по ч. 2 ст. 307 УК Республики Таджикистан была назначена комплексная компьютерно-техническая и политическая экспертиза, производство которой было поручено Республиканскому центру судебных и криминалистических экспертиз Министерства юстиции Республики Таджикистан. В постановлении о назначении экспертизы был сформулирован такой вопрос: «имеются ли на представленном электронном носителе материалы экстремистского содержания, если да, то усматривается ли в них участие в деятельности организации, деятельность которой запрещена судом в связи с осуществлением ей экстремистской деятельности?». Подобная постановка вопроса совсем не корректна, поскольку этот вопрос выходит за рамки компетенции экспертов и носит уголовно-квалифицирующий характер. Дать

оценку об участии того или иного лица в деятельности экстремистской организации должны только органы предварительного расследования и суд. Также, в части вопроса, относящейся к исследованию компьютерных данных, эксперт не может ответить на вопрос о наличии или отсутствии материалов экстремистского содержания на представленном электронном носителе. В данном случае он правомочен ответить, например, на вопрос: «какого вида информации содержится на представленном электронном носителе (текстовая, числовая, графическая, звуковая, видео), каковы их параметры и свойства?»[208].

Частные требования, предъявляемые к вопросам, выносимым на СКТЭ, состоят в следующем:

– вопросы должна быть направлены на установление конкретных обстоятельств расследуемого события;

– вопросы должны быть составлены так, чтобы их решения не требовали больших затрат;

– вопросы должны быть сформулированы с учётом технического оснащения экспертного учреждения;

– вопросы необходимо составить с учётом наличия электронных носителей, предоставляемых в распоряжение эксперта[209].

Относительно каждого рассматриваемого вида экспертизы существует перечень типовых вопросов, которые ставятся на разрешение экспертов.

Примерный перечень вопросов для разрешения **аппаратно-компьютерной экспертизы** можно составить следующим образом:

– Относится ли представленное на экспертизу средство к электронно-вычислительной технике?

– Каковы тип, модель и характерные свойства представленного на исследование технического устройства?

– Какова функциональная задача технического устройства?

---

[208] См.: Уголовное дело №22834 // Архив ГКНБ РТ.

[209] См.: Практическое руководство по производству судебных экспертиз для экспертов и специалистов: науч.-практ. пособие / Под ред. Т.В. Аверьяновой, В.Ф. Статкуса. 2-е изд., перераб. и доп. [Электронный ресурс]. – Режим доступа: https://fse.ms/library/prakticheskoe-rukovodstvo-po-proizvodstvu-sudebnyh-ekspertiz-dlya-ekspertov-i-spetsialistov-averyanova-t-v-statkusa-v-f/ (дата обращения: 09.03.2023).

– Какова роль и функция этого устройства в конкретной вычислительной системе?

– Какие функциональные задачи решаются посредством технического устройства, представленного на экспертное исследование?

– Каким было первоначальное состояние подлежащего исследованию технического устройства?

– Каково реальное состояние технического устройства и исправно ли оно для решения своих функциональных задач?

– Могли ли нарушения правил эксплуатации привести к неисправностям данного устройства?

– Является ли представленное техническое устройство носителем электронно-цифровой информации?

– К какому виду (модели, марке) относится представленный на исследование электронный носитель?

– Возможен ли доступ к данным, содержащимся на электронном носителе, представленном на экспертизу? Если нет, то по какой причине отсутствует доступ к его содержимому?

Перечень примерных вопросов, выносимых на **программно-компьютерную экспертизу**, выглядит так:

– Из каких элементов образовано программное обеспечение компьютерных систем, представленное на исследование, и каковы его общие свойства?

– К какой версии относится программное средство и каков вид его представления (явный, скрытый, удаленный)?

– Каковы реквизиты разработчика представленного на исследование программного средства и его владельца?

– Каковы содержания и характеристики файлов программного обеспечения?

– Какие функциональные задачи решаются посредством представленного на исследование программного средства?

– Какое программное обеспечение содержит представленный на исследование электронный носитель для решения определённой задачи?

– Какие требования предъявляет компьютерная система к данному программному обеспечению?

– Совместимо ли программное обеспечение с аппаратным обеспечением компьютерной системы?

– Адаптирован ли исследуемый программный инструмент для решения конкретных функциональных задач?

– Каково фактическое состояние программного средства и исправно ли оно для решения конкретных задач?

– Имеют ли конкретные программные средства исследуемого программного обеспечения признаки контрафактной продукции?

– Имеет ли программное средство отклонения от обычных программных продуктов, если да, то в чём они заключаются?

– Имеются ли в программном средстве защитные функции от несанкционированного доступа, если да, то какова их организованность?

– Какова последовательность работы данного программного средства?

– С помощью каких программных инструментов (языки программирования, стандартные библиотеки, компиляторы) разработано данное программное средство?

– Модифицирован ли алгоритм программного средства, если да, то в чём заключаются произведённые изменения?

– Каков был первоначальный вид программного средства до его модификации?

– Каковы цели модификации функций программного средства?

– Предназначены ли внесенные изменения для снятия защиты программного средства?

– Позволяют ли внесённые изменения в программное средство решить конкретные задачи?

– Какова последовательность и способы внесения изменений в программном средстве?

– Имеются ли в данном программном средстве функции, которые могут привести к нарушению функций компьютерной системы, модификации, уничтожению, блокированию или либо копированию данных?

– К каким последствиям может привести дальнейшая эксплуатация программного средства?

Примерные типичные вопросы, решаемые в рамках **информационно-компьютерной экспертизы** можно сформулировать следующим образом:

– Каким способом на представленном электронном носителе зафиксирована информация?

– В чём заключается специфика размещения сведений на электронном носителе?

– Какие свойства характерны информации на электронном носителе?

– Какой вид информации хранится на представленном электронном носителе?

– Каким образом можно получить доступ к содержимому электронного носителя?

– Ограничены ли данные на электронном носителе для общего доступа посредством введения средств защиты, если да, то каким образом можно их преодолевать?

– Сохранились ли на электронном носителе признаки взлома защиты от несанкционированного доступа?

– Каково содержание данных, имеющихся на представленном электронном носителе?

– Совпадают ли обнаруженные сведения обычному их состоянию на электронном носителе?

– В случае обнаружения несовпадения, то в чём заключаются это?

– Для чего предназначены данные, хранящиеся на электронном носителе?

– Содержит ли электронный носитель сведения, определённые для решения конкретной задачи?

– Какие данные сохранились на электронном носителе о фактах и обстоятельствах конкретного уголовного дела?

– Содержит ли данный носитель сведения о собственнике (пользователе) компьютерной системы, если да, то какие?

– Какие сведения с представленных на экспертизу документов (образцов) содержатся на электронном носителе?

– Каким был первоначальный вид данных на электронном носителе до их удаления или модификации?

– Каким способом осуществлены действия по модификации, блокированию, копированию или удалению определённых данных на представленном носителе?

– Какая очерёдность действий с выявленными данными осуществлялась при решении определённой задачи?

– В чём заключается причинная связь между операциями с данными и наступившим событием?

– Соответствуют ли действия с конкретными данными регламенту эксплуатации определенной компьютерной системы?

Перечень примерных вопросов на разрешение **компьютерно-сетевой экспертизы:**

– Имеются ли на представленной электронно-вычислительной технике следы её подключения к сети Интернет?

– Каким образом и посредством каких технических устройств происходило подключение компьютерной техники к глобальной сети?

– К каким ресурсам сети Интернет обратился пользователь посредством представленной на экспертизу электронно-вычислительной техники?

– Какие программы удаленного доступа[210] содержатся в представленном компьютерном средстве?

[210] Удаленный доступ – это возможность управления другим компьютером на расстоянии через глобальную сеть Интернет или локальную сеть.

– Содержит ли электронная почта, прикреплённая к представленной на исследование компьютерной технике, сообщения, если да, то каковы их содержания?

Отмеченные перечни вопросов не являются окончательными и в зависимости от расследуемого события, развития технологий и методик экспертного исследования они будут расширяться.

Необходимо отметить, что качество экспертного исследования и признание его результатов в качестве весомого доказательства зависят от правильной формулировки вопросов, выносимых на экспертизу. И здесь нельзя не соглашаться с А.Р. Сысенко, И.С. Смирновой и С.Е. Тимошенко, которые отмечают, что «вопросы, выносимые на СКТЭ, должны быть сформулированы так точно и полно, чтобы ответы на них позволили суду (судье), не обладающему специальными знаниями в области информационно-вычислительных технологий и электронно-вычислительной техники, вынести мотивированный, законный и обоснованный судебный акт»[211].

После выбора экспертного учреждения и уточнения вопросов для разрешения СКТЭ, на этапе подготовки материалов следователь определяет объекты, подлежащие экспертному исследованию, и прилагает их к постановлению о назначении СКТЭ для передачи экспертному учреждению. Как правило, на данном этапе в распоряжение экспертов предоставляются не образцы, а сами объекты, возможно содержащие доказательственную электронно-цифровую информацию.

При определении материалов для передачи в распоряжение эксперта необходимо сопоставить свой выбор с примерным перечнем типичных объектов, подлежащих направлению эксперту по конкретному составу преступления.

Так, к примеру, по уголовным делам, связанным с хищением денежных средств с использованием поддельных пластиковых карт, при назначении СКТЭ типичными объектами могут быть системный блок компьютера, электронный

[211] Сысенко А.Р., Смирнова И.С., Тимошенко С.Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы / А.Р. Сысенко, И.С. Смирнова, С.Е. Тимошенко // Сибирское юридическое обозрение. – 2020. – Том 17, – №4. – С. 529.

носитель с программным обеспечением и поддельная банковская карта. Системный блок электронно-вычислительной техники исследуется для установления обстоятельств подключения к сети Интернет и получения доступа к банковской карте. Экспертное изучение электронного носителя, в нашем случае, позволит установить наличие программ, предназначенных для изготовления «слепок» банковской карты. Исследование поддельной банковской карты необходимо для установления данных, идентичных данным подлинной банковской карты.

Постановление о назначении СКТЭ выносится после прохождения выше обозначенных этапов. С учётом требований ч. 1. ст. 208 УПК Республики Таджикистан специфичными элементами постановления о назначении данного вида экспертизы являются:

а) название экспертизы. По этому поводу В.В. Поляков и А.В. Шебалин верно отмечают, что «при составлении постановления о назначении компьютерно-технической экспертизы следователи в названии этого документа обычно не указывают вид назначаемой СКТЭ, ограничиваясь родовым названием, о виде экспертизы можно получить представление из анализа вопросов, ставящихся перед экспертом и предоставляемых в распоряжение эксперта материалов»[212]. При этом нормы уголовно-процессуального законодательства не считают обязательным указать в постановлении конкретный вид СКТЭ, однако, по нашему мнению, это говорит о том, что следователь при назначении экспертизы полным образом не понимает того, какого результата он хочет получить от экспертного исследования.

б) обстоятельства совершения преступления. Здесь необходимо показать суть произошедшего события, источник изъятия электронного носителя информации и других объектов;

в) отметка о необходимости использования специальных знаний для исследования представленных объектов. Для конкретизации необходимо

[212] Поляков В.В., Шебалин А.В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон, по преступлениям в сфере компьютерной информации / В.В. Пляков, А.В. Шебалин // Сборник материалов криминалистических чтений. – 2013. – №9. – С. 83.

указывать область назначаемой экспертизы. В зависимости от расследуемого преступления здесь может быть указаны такие области СКТЭ, как программирование, исследование электронно-цифровой информации, электронно-вычислительной техники или сетевых технологий;

г) наименование экспертного учреждения. Если производство экспертизы поручается частному эксперту, не являющемуся государственным, то следует предварительно запросить сведения о нём. В постановлении необходимо указать информацию о его компетенции, образовании, специальности, трудовом стаже в должности эксперта и другие сведения о его профессионализме[213];

д) вопросы, выносимые на экспертизу. Перечень вопросов зависит от вида СКТЭ, исследуемых объектов и применяемых методов;

е) предоставляемые в распоряжение эксперта материалы. Обязательным считается указание в постановлении индивидуальных признаков объектов экспертного исследования, так как это позволит устранить возможные вопросы и сомнения участников уголовного судопроизводства о том, что исследовался другой объект.

Следует отметить, что при назначении СКТЭ, кроме постановления, другие материалы уголовного дела эксперту не предоставляются и это отличительная черта данного вида экспертизы. В распоряжение эксперта предоставляются только материальные объекты, подлежащие экспертному исследованию, к числу которых можно относить электронные носители информации, системные блоки электронно-вычислительной техники, её периферийные устройства, в том числе устройства для подключения к сети и т.п.

Необходимо знать, что следователь имеет право присутствовать при производстве СКТЭ, в ходе которой может получить разъяснения об осуществляемых экспертом действиях. Также, согласно ст. 210 УПК Республики Таджикистан, с разрешения следователя, во время проведения экспертизы могут присутствовать подозреваемый, обвиняемый, потерпевший и их защитники. Факт

[213] См.: Дуленко В.А., Мамлеев Р.Р, Пестриков В.А. Преступления в сфере высоких технологий: учеб. пособие. – М., 2010. – С. 200.

присутствия данных участников уголовного судопроизводства должен быть зафиксирован в заключении эксперта.

Однако, как показывает практика, следователь изредка воспользуется своим правом присутствовать в ходе экспертного исследования, так как для проведения СКТЭ требуется много времени. Вместе с тем, он, проконсультировавшись с экспертом о временных промежутках своего целенаправленного присутствия, может без ущерба для своего рабочего времени присутствовать в ходе данного следственного действия. Такое присутствие поможет следователю уяснять технические моменты совершения расследуемого преступления и облегчить понимание заключения экспертизы и его доказательственного значения.

По результатам проведённого исследования эксперт составляет заключение. На основании ст. 217 УПК Республики Таджикистан в нём указывается:

– сведения о времени и месте проведения экспертного исследования;

– личные данные эксперта и его компетентность;

– обстоятельства, послужившие основанием для производства экспертизы;

– запись об уведомлении эксперта об ответственности за дачу ложного заключения или отказ от предоставления заключения;

– отметка о присутствии других участников уголовного дела при проведении экспертного исследования;

– сведения об использованных веществ и материалов, а также произведённых действиях эксперта;

– вопросы, вынесенные на экспертизу и аргументированные ответы на них.

Если решение поставленных вопросов не входят в компетенцию эксперта или материальные объекты, предоставленные в его распоряжение непригодны и недостаточны для исследования и дачи ответов на поставленные вопросы, он на основании мотивированного письма возвращает материалы следователю.

Согласно положениям ст.ст. 87 и 88 УПК Республики Таджикистан собранные доказательства по уголовному делу подлежат проверке и оценке. Получив заключение эксперта, следователь определяет, решены ли все вопросы, поставленные перед экспертом, в рамках СКТЭ и нет ли необходимости в

проведении дополнительного исследования, а также оценивает представленное заключение на предмет относимости, допустимости и достоверности.

С точки зрения относимости, заключения СКТЭ удостоверяется тем, что в нём указывается номер конкретного уголовного дела, в рамках которого назначена экспертиза, сходство исследованных в ходе экспертизы объектов материалам дела, а также относимость выводов эксперта соответствующим элементам состава расследуемого преступления[214].

Для оценки заключения эксперта с точки зрения допустимости необходимо устанавливать следующие обстоятельства:

– верный выбор экспертного учреждения;

– соответствующая квалификация эксперта;

– соблюдение норм уголовно-процессуального законодательства при составлении заключения;

– верное применение методики проведения СКТЭ.

Достаточно сложной является оценка заключения экспертизы с позиции достоверности, так как для оценки электронно-цифровой информации, порядка проведённого исследования, применяемых методов и методик требуются специальные квалифицированные знания, которых зачастую нет у следователя. На этом счёт Р.С. Белкин справедливо полагает, что «следователь и суд не способны оценить экспертное заключение с позиции достоверности, поскольку они должны обладать схожими с экспертом знаниями»[215]. Аналогическую позицию занимает и Т.В. Аверьянова, которая отмечает, что «заключения сложных экспертиз, каковым является и заключение СКТЭ, практически может оценить только специалист того же профиля и не считаться с этим – значит обманывать самих себя и уходить от решения насущно важных вопросов»[216].

Таким образом, можно утверждать, что процесс назначения и производства СКТЭ в зависимости от сферы применения специальных знаний имеет свои

[214] См.: Аверьянова Т.В. Судебная экспертиза. Курс общей теории. – Москва: Норма: ИНФРА-М, 2014. – С. 460.
[215] Белкин Р.С. Курс криминалистики. – Москва: ЮНИТИ-ДАНА, Закон и право, 2001. – С. 623.
[216] Аверьянова Т.В. Проблемы теории и практики судебной экспертизы / Т.В. Аверьянова // Информационный бюллетень II Международной научно-практической конференции «Дискуссионные вопросы теории и практики судебной экспертизы». – Москва, 2017. – С. 1-8.

особенности во всех стадиях. Следователь при принятии решения о назначении СКТЭ, в первую очередь, должен уяснить требуется ли для получения фактических данных производство экспертизы. Если да, то необходимо определиться с видом СКТЭ и по согласованию с экспертом уточнить перечень вопросов, выносимых на разрешение экспертного исследования. При этом следует строго соблюдать существующие требования, предъявляемые к вопросам, решаемым в рамках СКТЭ. Результаты СКТЭ во многом зависят от квалифицированной фиксации доказательственных данных на этапе подготовки к её назначению. Неправильная, с нарушением процессуальных норм фиксация информации может впоследствии послужить основанием для признания данного экспертного заключения недопустимым доказательством. Также, важным является верное определение круга объектов, предоставляемых в распоряжение эксперта, и правильное составление постановления о назначении СКТЭ согласно ст. 208 УПК Республики Таджикистан.

Установленные в ходе экспертного исследования фактические данные о преступлениях, совершаемых с использованием компьютерных и информационно-телекоммуникационных систем, являются весомым доказательством, которое стороне защиты трудно будет опровергнуть, и суд, основываясь на них в совокупности с другими доказательствами, может принять верное решение по уголовному делу.

ЗАКЛЮЧЕНИЕ

В современном информационном обществе, в котором социально-экономическое развитие сопряжено с производством, переработкой и распространением информации среди его членов, техническая вооружённость стала новым качеством преступности. Стремительный переход общества в цифровую среду и внедрение инновационных технологий в управление общественными и производственными процессами порождают новые способы совершения общественно-опасных деяний, связанных с применением информационных технологий [5-А].

Преступники, используя широкую распространённость и доступность компьютерных и телекоммуникационных технологий, умело применяют их как при совершении преступлений, так и при сокрытии следов преступной деятельности. В связи с этим, неуклонно растет роль и значение электронно-цифровой информации в процессе доказывания по уголовным делам.

В настоящей диссертационной работе с учётом намеченных целей и поставленных задач на монографическом уровне осуществлено всестороннее исследование проблем обнаружения и фиксации доказательственной электронно-цифровой информации и её использования в процессе доказывания по уголовным делам. В том числе, определено правовое положение электронно-цифровой информации в системе доказательств по уголовным делам, на основе авторского подхода к классификации преступлений данной категории, определён весь спектр преступлений, в механизме совершения которых используются информационные технологии, сформулировано авторское определение преступлений рассматриваемого вида, с учётом механизма следообразования и особенностей производства отдельных следственных действий, предложены тактические приёмы обнаружения и фиксации доказательств, содержащихся на электронных носителях, разработаны и научно обоснованы рекомендации, направленные на совершенствование законодательства, в части определения понятия электронно-цифровой информации, включения её в систему доказательств и создания

процессуальных средств собирания доказательств на локальных и сетевых носителях.

По итогам проведенного исследования автор приходит к следующим выводам:

1. С развитием информационных технологий расследование преступлений практически невозможно представить без получения и использования информации с электронных носителей, которые содержат большой объём криминалистически значимых сведений, необходимых для правильного разрешения дела. Электронные носители достаточно информативны и содержащиеся на них данные необходимо правильно фиксировать, извлекать и приобщать к уголовным делам. Вместе с тем, работа с электронно-цифровой информацией вызывает определённые сложности у органов предварительного следствия. Это связано, прежде всего, с особенностью образования цифровых следов, отсутствием специальных технических знаний у сотрудников, а также недостаточным правовым регулированием данного вопроса [3-А].

2. В современном обществе информационные технологии используются в механизме совершения большой части общественно-опасных деяний, предусмотренных уголовным законом. Понятие преступлений, совершаемых с использованием информационных технологий, не ограничивается только противоправным вмешательством в работу ЭВМ, компьютерных программ, информационно-телекоммуникационных сетей и несанкционированной модификацией цифровых данных, а оно охватывает и иные противозаконные общественно-опасные деяния, совершаемые посредством или с помощью компьютерной техники, компьютерных сетей и программ. В связи с этим, предлагается авторское определение преступлений данной категории, под которыми следует понимать противоправные деяния, запрещённые уголовным законом, наносящие ущерб или создающие угрозу нанесения ущерба интересам личности, общества и государства, совершаемые посредством цифровой и (или) электронно-вычислительной техники, компьютерных сетей и программ [9–А].

3. Путём проведения авторской классификации преступлений в сфере информационных технологий, за основу которой взята структура объектов уголовно-правовой охраны, определён весь спектр общественно-опасных деяний, совершение которых возможно с использованием информационных технологий. По этому основанию преступления рассматриваемой категории разделены на семь групп:

– преступления, совершаемые с применением информационных технологий против личности;

– преступления, совершаемые с применением информационных технологий против общественной безопасности и здоровья населения;

– преступления, совершаемые с применением информационных технологий против общественного порядка и нравственности;

– преступления, совершаемые с применением информационных технологий против информационной безопасности;

– преступления, совершаемые с применением информационных технологий против государственной власти;

– преступления, совершаемые с применением информационных технологий против военной службы;

– преступления, совершаемые с применением информационных технологий против мира и безопасности человечества [4-А].

4. В настоящее время в научных кругах нет единого мнения относительно того, какой термин стоит применять к электронно-цифровым следам: «электронные», «бинарные», «цифровые», «электронно-цифровые», «компьютерные», «виртуальные» и т.п.

Автор утверждает, что для содержательного определения рассматриваемого вида следов необходимо использовать термин «электронно-цифровые следы» и под ним следует понимать всякую связанную с расследуемым событием трансформацию в информационном поле, зафиксированную в форме электромагнитных сигналов на материальном носителе и отражающую события действительности.

Электронно-цифровые следы по своей сути схожи со многими невидимыми материальными следами и имеют материальную природу происхождения [4-А].

5. В механизме формирования рассматриваемой категории следов основой считается электронное отображение изменений, связанных с событием преступления. Ввиду того, что в информационном пространстве следообразующие объекты не имеют физическую форму, электронно-цифровые следы формируются в результате взаимодействия дискретных сигналов и среды в виде электромагнитных изменений, которые фиксируются на электронных носителях компьютерных или цифровых устройств.

Для установления и фиксации следов названной категории надлежит выявить пересекающееся взаимосоединение между образовавшимися изменениями, вычислительной системой и оставившим свое отражение действием или событием [6-А].

6. При механизме следообразования электронно-цифровых следов в качестве отражающего объекта выступает вычислительная система, а отражаемого – пользователь. Инструментами отражения могут быть команды и электромагнитные сигналы, активизированные пользователем или прикладным программным обеспечением. Следообразующим объектом считается системное программное обеспечение, а в качестве следовоспринимающего объекта выступает массив памяти соответствующего устройства. Механизм образования данных следов зависит от конструкции информационного пространства, в котором они запечатлены [7-А].

7. Решение о применении того или иного тактического комплекса по обнаружению, фиксации и изъятию электронно-цифровых следов необходимо принимать с учётом конкретной следственной ситуации. Разработанные и рекомендованные автором тактические комплексы включены в основные положения диссертации, выносимые на защиту [5-А].

8. Несмотря на особенности доказательственной электронно-цифровой информации, её собирание осуществляется предусмотренными УПК Республики Таджикистан процессуальными средствами, т.е. следственными действиями,

основными из которых являются осмотр места происшествия, осмотр предметов, осмотр документов, обыск, выемка и экспертиза. Самым распространённым и информативным способом обнаружения, фиксации и изъятия доказательственной электронно-цифровой информации, содержащейся на локальных и сетевых носителях, является следственный осмотр.

Законодатель не обязывает органы следствия привлекать при работе с электронными доказательствами специалиста, однако в целях полной, объективной и качественной фиксации криминалистически значимой информации, его участие считается необходимым [1-А].

9. Следователь при принятии решения о судебной компьютерно-технической экспертизе, в первую очередь, должен уяснить требуется ли для получения фактических данных производство экспертизы. Если да, то необходимо определиться с видом СКТЭ и по согласованию с экспертом уточнить перечень вопросов, выносимых на разрешение экспертного исследования. При этом следует строго соблюдать существующие требования, предъявляемые к вопросам, решаемым в рамках СКТЭ. Результаты СКТЭ во многом зависят от квалифицированной фиксации доказательственных данных на этапе подготовки к её назначению. Также, важным является верное определение круга объектов, предоставляемых в распоряжение эксперта, и правильное составление постановления о назначении СКТЭ согласно требованиям ст. 208 УПК Республики Таджикистан [2-А].

РЕКОМЕНДАЦИИ ПО ПРАКТИЧЕСКОМУ ИСПОЛЬЗОВАНИЮ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Выводы, имеющие практическое значение в виде рекомендаций и предложений, направленные на совершенствование законодательства по определению понятия электронно-цифровой информации, установлению её места в системе доказательств и созданию процессуальных средств собирания электронно-цифровых доказательств:

1) С развитием информационных технологий термин «компьютерная информация» устарел, поскольку в современном обществе появилось большое количество цифровых средств, имеющих функции создания, обработки, хранения и передачи информации, но, вместе с тем, не являющиеся компьютерным устройством, и применить слово «компьютер» к данным, содержащимся в этих средствах, не является правильным. В связи с чем, предлагается в статьях главы 28 Уголовного кодекса Республики Таджикистан (Преступления против информационной безопасности) слова «компьютерная информация» заменить на «электронно-цифровую информацию» и статью 298 данной главы дополнить примечанием, где определить понятие «электронно-цифровой информации» в следующей редакции: «Электронно-цифровая информация – данные, записанные в памяти компьютерных или иных микропроцессорных устройств, предназначенные для обработки с помощью электронно-вычислительной либо цифровой техники, а также сведения, передаваемые по каналам связи посредством дискретных сигналов» [3-А].

2) Автор научно обосновывает, что положения ст. 82 УПК Республики Таджикистан об отнесении электронно-цифровой информации (её носителей) как один из видов доказательств к иным документам, а в отдельных случаях к вещественным доказательствам, подлежат пересмотру. Так как рассматриваемый вид информации в отличие от документов не составляется человеком, а создаётся путём набора определённых команд или записи процессов, протекающих в окружающем мире, посредством технических устройств. Электронно-цифровую информацию невозможно воспринимать без использования технических

устройств, тогда как документ или вещественное доказательство доступны для непосредственного восприятия человеком. В связи с чем, необходимо определить электронно-цифровую информацию как отдельный вид доказательств и с этой целью внести соответствующее дополнение и изменение в УПК Республики Таджикистан: а) ч. 2 ст. 72 (Доказательства) дополнить новым подпунктом – «электронно-цифровая информация»; б) из ч. 2 ст. 82 исключить слова «электронные источники информации» [4-А].

3) В целях правового регулирования процесса собирания доказательственной информации из информационно-телекоммуникационных сетей, доступ к которой предоставлен неограниченному кругу лиц, необходимо дополнить действующий Уголовно-процессуальный кодекс Республики Таджикистан статьёй 183 (1) «Дистанционный осмотр электронно-цифровых информационных ресурсов» в следующей редакции:

«Статья 183 (1). Дистанционный осмотр электронно-цифровых информационных ресурсов

1. Дознаватель, следователь или прокурор в целях обнаружения следов преступных действий, выяснения иных обстоятельств, имеющих значение для правильного разрешения дела, проводит дистанционный (удалённый) осмотр информации, размещенной на электронно-цифровых информационных ресурсах и доступ к которой не ограничен.

2. В порядке, предусмотренном настоящим Кодексом, при производстве дистанционного осмотра в качестве специалиста может быть привлечено лицо, обладающее необходимыми знаниями в области информационных технологий.

3. О результатах проведения дистанционного осмотра составляется протокол, где помимо требований статей 172-173 настоящего Кодекса, также отражается сетевой адрес обследуемого электронного ресурса, содержащаяся на нём доказательственная информация, использованные программные и технические средства, модель и характерные свойства носителя, на котором скопированы криминалистически значимые данные.

4. Носитель со скопированными данными упаковывается способом,

исключающим возможность получения доступа к его содержимому посторонним лицам» [6–А].

4) Для создания уголовно-процессуальных норм по фиксации доказательственной информации в информационно-телекоммуникационных сетях, доступ к которой ограничен, предлагается дополнить действующий Уголовно-процессуальный кодекс Республики Таджикистан статьёй 194 (1) «Дистанционный обыск» следующего содержания:

«Статья 194 (1). Дистанционный обыск

1. Дознаватель, следователь или прокурор в целях принудительного обследования данных, доступ к которым ограничен, проводит дистанционный (удалённый) обыск электронно-цифровых информационных ресурсов.

2. Основанием для производства дистанционного обыска является наличие достаточных данных о возможном наличии в информационных ресурсах сведений, относящихся к расследуемому событию.

3. Дистанционный обыск проводится на основании мотивированного постановления должностного лица, в производстве которого находится уголовное дело, согласия прокурора и разрешения суда.

4. Участие специалиста при производстве дистанционного обыска является обязательным. При его содействии преодолеваются возможные технические и программные средства защиты электронно-цифровой информации.

5. Перед началом дистанционного обыска присутствующим разъясняется порядок проведения следственного действия. В случае присутствия владельца обследуемых информационных ресурсов, должностное лицо, осуществляющее следственное действие, ознакомит его с санкцией суда и предлагает добровольно предоставить доступ к интересующим следствие данным.

6. О результатах проведения дистанционного обыска информационных ресурсов составляется протокол с соблюдением требований статьи 194 настоящего Кодекса. Также, в протоколе указываются сетевой адрес обследуемого информационного ресурса, содержащаяся в нём доказательственная информация, использованные программные и технические

средства, модель и характерные свойства носителя, на котором скопированы криминалистически значимые данные.

7. Электронный носитель со скопированной информацией упаковывается и опечатывается на месте производства следственного действия, что удостоверяется подписями лиц, участвующих в нём» [6-А].

СПИСОК ЛИТЕРАТУРЫ (ИСТОЧНИКОВ)

I. Нормативные правовые акты и официальные документы:

1. Конституция Республики Таджикистан (принята 06 ноября 1994 года, с внесёнными изменениями и дополнениями от 26 сентября 1999 г., от 22 июня 2003 г., от 22 мая 2016 г.). – Душанбе, 2016. – 64 с.
2. Конвенция Совета Европы о преступности в сфере компьютерной информации, ETS №185 (23 ноября 2001 г., г. Будапешт) [Электронный ресурс]. – Режим доступа: URL: https://rm.coe.int/1680081580 (дата обращения: 23.05.2022).
3. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (22 января 1993 г., г. Минск) [Электронный ресурс]. – Режим доступа: www.consultant.ru/document/cons_doc_LAW_5942/ (дата обращения: 23.05.2022).
4. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (07 октября 2002 г., г. Кишинёв) [Электронный ресурс]. – Режим доступа: URL: https://cis.minsk.by/page/614 (дата обращения: 23.05.2022).
5. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (28 сентября 2018 г., г. Душанбе) [Электронный ресурс]. – Режим доступа: URL: https://www.cisatc.org/1289/9115/135/9126/9128/9034 (дата обращения: 23.05.2022).
6. Уголовно-процессуальный кодекс Республики Таджикистан. Действующий кодекс. Дата принятия: 03.12.2009 // Ахбор Маджлиси Оли Республики Таджикистан. – 2016. – №3. – ст. 128.
7. Уголовный кодекс Республики Таджикистан. Действующий кодекс. Дата принятия: 21.05.1998 // Ахбор Маджлиси Оли Республики Таджикистан. – 2020. – №1. – ст. 8-9.
8. Закон Республики Таджикистан «Об информации». Действующий закон. Дата принятия: 10.05.2002 г. // В редакции закона от 03.07.2012г. №848 [Электронный ресурс]. – Режим доступа: URL: http://www.adlia.tj/show_

doc.fwx?rgn=3251&conttype=2 (дата обращения: 21.06.2022).

9. Закон Республики Таджикистан «Об электронном документе» от 10.05.2002г., №51 (в редакции Закона РТ от 26.12.2005 г. №122; от 28.12.2012 г., №908; от 22.07.2013 г., №995) [Электронный ресурс]. – Режим доступа: URL: http://www.adlia.tj/show_doc.fwx?rgn=123088 (дата обращения: 23.05.2022).
10. Закон Республики Таджикистан «Об информатизации» // Ахбор Маджлиси Оли Республики Таджикистан. – 2001 год. – №7. – ст. 502.
11. Закон Республики Таджикистан «Об оперативно-розыскной деятельности» от 28 июня 2011 г. // Ахбор Маджлиси Оли Республики Таджикистан. – 2011 г. – №3. – ст. 155; – 2014 г. – №7. – ч. 1. – ст. 387.
12. Закон Республики Таджикистан «О противодействии экстремизму» от 02 января 2020 года, №1655 [Электронный ресурс]. – Режим доступа: URL: http://ncz.tj/system/files/Legislation/1655_ru.pdf (дата обращения: 21.06.2022).
13. Закон Республики Таджикистан «О противодействии терроризму» от 23 декабря 2021 года, №1808 [Электронный ресурс]. – Режим доступа: URL: http://ncz.tj/system/files/Legislation/1808_ru.pdf (дата обращения: 15.08.2022).
14. Концепция правовой политики Республики Таджикистан на 2018-2028 годы от 6 февраля 2018 года, №1005 [CD-ROM] / Адлия: Централиз. банк правовой информации РТ. Версия 7.0. / Министерство юстиции РТ. – Душанбе, 2021 г.
15. Правила предоставления услуг Интернета на территории Республики Таджикистан, утверждённые Постановлением Правительства Республики Таджикистан от 8 августа 2001 года, №389 [Электронный ресурс]. – Режим доступа: URL:http://www.adlia.tj/show_doc.fwx?rgn=6507&conttype=2 (дата обращения: 15.08.2022).
16. Указ Президента Республики Таджикистан «О Концепции информационной безопасности Республики Таджикистан» от 07 ноября 2003 г., №1175 [Электронный ресурс]. – Режим доступа: URL://http://www.adlia.tj/show_doc.fwx?rgn=5104&conttype=2 (дата обращения: 15.08.2022).
17. Указ Президента Республики Таджикистан «О Концепции государственной

информационной политики Республики Таджикистан» от 30 апреля 2008 г., №451 [Электронный ресурс]. – Режим доступа: URL:http://www.adlia.tj/show_doc.fwx?rgn=12903 (дата обращения: 15.08.2022).

18. Постановление Правительства Республики Таджикистан «О Программе обеспечения информационной безопасности Республики Таджикистан» от 30 июня 2004 г., №290 [Электронный ресурс]. – Режим доступа: URL:http://www.adlia.tj/show_doc.fwx?rgn=5103 (дата обращения: 15.08.2022).

II. Монографии, комментарии и учебники, учебные пособия:

19. Аверьянова, Т.В. Судебная экспертиза. Курс общей теории [Текст] / Т.В. Аверьянова. – Москва: Норма: ИНФРА-М, 2014. – 479 с.
20. Андреев, Б.В., Пак, П.Н., Хорст, В.П. Расследование преступлений в сфере компьютерной информации [Текст] / Б.В. Андреев, П.Н. Пак, В.П. Хорст. – М.: Юрлит-информ, 2001. – 152 с.
21. Бахтеев, Д.В. Основы теории электронных доказательств [Текст]: монография / Под ред. д-ра юрид. наук С.В. Зуева. – М.: Юрлит-информ, 2019. – 284 с.
22. Белкин, Р.С. Криминалистическая энциклопедия [Текст] / Р.С. Белкин. – 2-е изд., доп. – М.: Мега-трон XXI, 2000. – 334 с.
23. Белкин, Р.С. Курс криминалистики [Текст] / Р.С. Белкин. – М.: ЮНИТИ-ДАНА, Закон и право, 2001. – 837 с.
24. Белкин, Р.С. Курс криминалистики. Частные криминалистические теории [Текст]: В 3 т. Т. 2. / Р.С. Белкин. – М.: Юристъ, 1997. – 521 с.
25. Белкин, Р.С. Курс криминалистики [Текст]: в 3 т. Т. 1: Общая теория криминалистики / Р.С. Белкин. – М.: Юристъ, 1997. – 408 с.
26. Белкин, Р.С. Собирание, исследование и оценка доказательств. Сущность и методы [Текст] / Р.С. Белкин. – М.: Наука, 1966. – 296 с.
27. Большой энциклопедический словарь [Текст] / Под ред. А.М. Прохорова. – Т. 2. – Москва, 1991. – 768 с.
28. Вехов, В.Б. Компьютерные преступления: способы совершения и раскрытия [Текст] / Под общ. ред. Б.П. Смагоринского. – Москва, 1996. – 182 с.
29. Вехов, В.Б. Основы криминалистического учения об исследовании и

использовании компьютерной информации и средств ее обработки [Текст] / В.Б. Вехов. – Волгоград: ВА МВД России, 2008. – 401 с.

30. Винберг, А.И. Криминалистика [Текст]: Вып. 1. Введение в криминалистику / А.И. Винберг. – М., 1950. – 304 с.
31. Волеводз, А.Г. Противодействие компьютерным преступлениям [Текст] / А.Г. Волеводз. – М., 2002. – 485 с.
32. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества [Текст] / А.Г. Волеводз. – М.: ООО Изд-во Юрлитинформ, 2001. – 496 с.
33. Гаврилин, Ю.В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы: монография [Текст] / Ю.В. Гаврилин. – Тула, 2009. – 361 с.
34. Гаврилов, Б.Я. Получение доказательств и информации с электронных носителей: вопросы законодательного регулирования и правоприменения [Текст] / Б.Я. Гаврилов // Уголовное судопроизводство: проблемы теории и практики. – Т. 3. – М., 2018. – 216 с.
35. Давлатзода, К.Д. Основания расследования киберпреступлений [Текст] / К.Д. Давлатзода. – Душанбе, 2023. – 150 с.
36. Давлатзода, К.Д. Угрозы виртуальной среды: практика и теория киберпреступлений: монография [Текст] / К.Д. Давлатзода. – Душанбе, 2023. – 248 с.;
37. Дворкин, А.И. Осмотр места происшествия: практическое пособие [Текст] / А.И. Дворкин. – Москва: Юрист: Библиотека следователя, 2001. – 248 с.
38. Дуленко, В.А., Мамлеев, Р.Р., Пестриков, В.А. Преступления в сфере высоких технологий [Текст]: учеб, пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. – М., 2010. – 200 с.
39. Зуев, С.В. Основы теории электронных доказательств [Текст]: монография / Под ред. д-ра юрид. наук С.В. Зуева. – М.: Юрлитинформ, 2019. – 304 с.
40. Колдин, В.Я. Вещественные доказательства: Информационные технологии

процессуального доказывания [Текст] / В.Я. Колдин. – М: Издательство НОРМА, 2002. – 768 с.

41. Криминалистика [Текст]: учебник / Отв. ред. В.П. Лавров, Р.Х. Рахимзода, А.Ф. Волынский. – Душанбе, 2022. – 660 с.
42. Кузнецов, А.А., Муленков, Д.В., Пропастин, С.В., Соколов, А.В. Тактика следственных действий, направленных на отыскание, обнаружение, изъятие и исследование электронных носителей информации на них [Текст]: учеб. пособие / А.А. Кузнецов, Д.В. Муленков, С.В. Пропастин, А.Б. Соколов. – Омск: Омская академия МВД России, 2015. – 237 с.
43. Меликов, У.А. Правовой режим объектов гражданских прав в интернете [Текст] / У.А. Меликов. – Душанбе, «ЭР-граф», 2017. – 244 с.
44. Менжега, М.М. Методика расследования создания и использования вредоносных программ для ЭВМ [Текст] / М.М. Межега. – М.: Юрлитинформ, 2010. – 296 с.
45. Мещеряков, В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования [Текст] / А.В. Мещеряков. – Воронеж: Изд-во Воронеж. гос. ун-та, 2002. – 407 с.
46. Нехорошев, А.Б. Компьютерные преступления: квалификация, расследование, экспертиза [Текст] / А.Б. Нехорошев. – Саратов, 2004. – 371 с.
47. Ожегов, С.И., Шведова, Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений [Текст] / С.И. Ожегов, Н.Ю. Шведова / Российская академия наук. Институт русского языка им. В.В. Виноградова. – 4-е изд., – Москва: ООО «А ТЕМП», 2013. – 874 с.
48. Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт [Текст] / А.Л. Осипенко. – М., 2004. – 432 с.
49. Рассолов, И.М. Право и Интернет. Теоретические проблемы [Текст] / И.М. Рассолов. – М.: Норма, 2009. – 384 с.
50. Ратинов, А.Р. Судебная психология для следователей [Текст] / А.Р. Ратинов. – М.: Юрлитинформ, 2008. – 350 с.
51. Россинская, Е.Р. Судебная экспертиза в гражданском, арбитражном,

административном и уголовном процессе [Текст]: монография / Е.Р. Россинская. – М.: Норма: Инфра-М, 2018. – 576 с.

52. Россинская, Е.Р., Галяшина, Е.И. Настольная книга судьи: судебная экспертиза [Текст] / Е.Р. Россинская, Е.И. Галяшина. – М.: Проспект, 2011. – 458 с.
53. Семенов, Г.В. Расследование преступлений в сфере мобильных телекоммуникаций [Текст]: монография / Г.В. Семенов. – М.: Юрлитинформ, 2008. – 336 с.
54. Советский энциклопедический словарь – М.: «Советская энциклопедия», 1985. – 1600 с.
55. Уголовное право Российской Федерации. Особенная часть [Текст] / Под ред. Здравомыслова Б.В. – М.: БЕК, 2000. – 552 с.
56. Фатьянов, А.А. Правовое обеспечение безопасности информации в Российской Федерации [Текст]: учебное пособие / А.А. Фатьянов. – М.: Издательская группа «Юрист», 2001. – 412 с.
57. Федоров, А.В. Информационная безопасность в мировом политическом процессе [Текст]: учеб. пособие / А.В. Федоров. – М., 2006. – 220 с.
58. Шейфер, С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение [Текст] / С.А. Шейфер. – Самара: Издательство «Самарский университет», 2004. – 192 с.
59. Яблоков Н.П. Криминалистика: практикум [Текст] / Н.П. Яблоков. – Москва: Юристъ, 2004. – С. 570.

III. Статьи и доклады:

60. Аверьянова, Т.В. Проблемы теории и практики судебной экспертизы [Текст] / Т.В. Аверьянова // Информационный бюллетень II Международной научно-практической конференции «Дискуссионные вопросы теории и практики судебной экспертизы». – Москва, 2017. – С. 1-8.
61. Агибалов, В.Ю., Мещеряков, В.А. Природа и сущность виртуальных следов [Текст] / В.Ю. Агибалов, В.А. Мещеряков // Воронежские криминалистические чтения: сб. науч. трудов. – 2010. – Вып. 12. – С. 6-21.

62. Алексеев, С.В. Особенности раннего становления групповых преступлений в киберпространстве [Текст] /С.В. Алексеев // Вопросы российского и международного права. – 2020. – Том 10. – №10 А. – С. 183-191.
63. Антонов, О.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами в России: сущность, этапы и пути совершенствования тактического обеспечения [Текст] / О.Ю. Антонов // Вестник Томского государственного университета. – 2020. – №459. – С. 221-229.
64. Архипова, Н.А. К вопросу об использовании возможностей средств мобильной связи в раскрытии и расследовании преступлений [Текст] / Н.А. Архипова // Криминалистические чтения: сб. материалов. – 2014. – №10. – С. 16-17.
65. Баранов, А.М. Электронные доказательства: иллюзия уголовного процесса XXI в [Текст] / А.М. Баранов // Уголовная юстиция. – 2019. – №13. – С. 64-69.
66. Батухтин, М.Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия [Текст] / М.Е. Батухтин // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе. Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. – 2018. – С. 25-27.
67. Бессонов, А.А. Особенности использования специальных знаний при расследовании незаконной добычи рыбных ресурсов [Текст] / А.А. Бессонов // Эксперт-криминалист. – 2015. – №3. – С. 3-5.
68. Борисов, В.В. Об особенностях фиксации информационных следов в практике защиты информации [Текст] / В.В. Борисов // Известия Южного федерального университета. Технические науки. – 2009. – Т. 94. – №5. – С. 164-168.
69. Васюков, В.Ф. Некоторые особенности расследования преступлений, совершаемых с использованием электронных платежных единиц [Текст] / В.Ф. Васюков // Российский следователь. – 2017. – №23. – С. 8-10.
70. Васюков, В.Ф., Колычева, А.Л. Осмотр и фиксация страниц интернет-сайта в сети Интернет [Текст] / В.Ф. Васюков, А.Л. Колычева // Вестник

экономической безопасности. – 2019. – №1. – С. 115-118.

71. Вехов, В.Б., Смагоринский, Б.П., Ковалев, С.А. Электронные следы в системе криминалистики [Текст] / В.Б. Вехов, Б.П. Смагорский, С.А. Ковалёв // Судебная экспертиза. – 2016. – №2 (46) – С. 10-19.
72. Виноградова, К.А., Савина, Л.А. Изъятие и осмотр мобильных телефонов и находящейся на них электронной информации по преступлениям, совершенным военнослужащими [Текст] / К.А. Виноградова, Л.А. Савина // Вестник военного права. – 2019. – №2. – С. 55-58.
73. Волеводз, А.Г. Следы преступлений, совершённых в компьютерных сетях [Текст] / А.Г. Волеводз // Российский следователь. – 2002. – №1. – С. 4-12.
74. Гаврилин, Ю.В. Электронные носители информации в уголовном судопроизводстве [Текст] / Ю.В. Гаврилин // Труды Академии управления МВД России. – 2017. – №4 (44). – С. 45-50.
75. Гаврилин, Ю.В., Победкин, А.В. Собирание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы [Текст] / Ю.В. Гаврилин, А.В. Победкин // Труды Академии управления МВД России. – 2018. – №3 (47). – С. 106-114.
76. Гаврилин, Ю.В., Шипилов, В.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации [Текст] / Ю.В. Гаврилин, В.В. Шилов // Российский следователь. – 2013. – №23. – С. 2-6.
77. Гаврилин, Ю.В., Балашова, А.А. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах [Текст] / Ю.В. Гаврилин, А.А. Балашова // Криминалистика: вчера, сегодня, завтра. – 2020. – №1. – С. 129-137.
78. Голик, Ю.В. Меняется мир – меняется преступность [Текст] / Ю.В. Голик // Криминология: вчера, сегодня, завтра. – 2015. – №3 (38). – С. 33-37.
79. Гончаров, А.В. Использование возможностей современных инновационных технологий при исследовании цифровых устройств мобильной связи и компьютерных носителей информации при расследовании преступлений

[Текст] / А.В. Гончаров // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития. Мат. Междунар. науч.-практ. конф. – Москва, 2019. – С. 186-201.

80. Григорьев, В.Н., Максимов, О.А. Понятие электронных носителей информации в уголовном судопроизводстве [Текст] / В.Н. Григорьев, О.А. Максимов // Вестник Уфимского юридического института МВД России. – 2019. – №2 (84). – С. 33-44.
81. Давлатзода, К.Д. Классификация киберпреступлений [Текст] / К.Д. Давлатзода // Вестник Таджикского национального университета. – 2022. – №8. – С. 279-284.
82. Давлатзода, К.Д. Кибертерроризм как новый вид террористического акта [Текст] / К.Д. Давлатзода // Вестник Таджикского национального университета. – 2023. – №1. – С. 207-213.
83. Долгинов, С.Д. Следы электронных устройств в криминалистике [Текст] / С.Д. Долгинов // В сб.: Шестой пермский конгресс ученых-юристов: Российская национальная правовая система: современное состояние, тенденции и перспективы развития. Мат. Междунар. науч.-практ. конф. – 2015. – С. 266-267.
84. Еськов, В.Д., Чеботарев, С.А. Особенности осмотра страниц в сети Интернет [Текст] / В.Д. Еськов, С.А. Чеботарев // Организационное, процессуальное и криминалистическое обеспечение уголовного производства: материалы VI Междунар. науч. конф. студентов и магистрантов. – 2017. – С. 39-40.
85. Зоир, Дж.М. Оперативно-розыскное мероприятие получение компьютерной информации и права человека [Текст] / Дж.М. Зоир // Труды Академии МВД Республики Таджикистан. – 2018. – №1 (37). – С. 26-37.
86. Иванов, А.Н. О новом виде обыска [Текст] / А.Н. Иванов // Актуальные проблемы криминалистики на современном этапе: сб. науч. ст. / Под ред. З.Д. Еникеева. – Уфа, 2003. – Ч. 1. – С. 105-109.
87. Иванов, А.Н. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы [Текст] / А.Н. Иванов // Известия Саратовского университета. – 2009. – Т. 9. – Вып. 2. – С. 74-77.

88. Иванов, Н.А. О понятии «цифровые доказательства» и их месте в общей системе доказательств [Текст] / Н.А. Иванов // Проблемы профилактики и противодействия компьютерным преступлениям: материалы межд. науч.-практ. конф. (г. Челябинск, 30 мая 2007 г.) и «круглого стола» (г. Челябинск, 18 мая 2007 г.) – Челябинск: Челябинский центр по исследованию проблем противодействия организованной преступности и коррупции. – 2008. – С. 96-100.
89. Кабанова, Ж.Ю. Электронный след в уголовно-исполнительной системе [Текст] / Ж.Ю. Кабанова // В сборнике: Уголовно-исполнительная система сегодня: взаимодействие науки и практики. Мат. науч.-практ. конф. – 2016. – С. 123-124.
90. Карлов, А.Л. Использование в доказывании по уголовным делам сведений, составляющих тайну связи, расположенных в сети Интернет [Текст] / А.Л. Карлов // Вестник Сибирского юридического института МВД России. – 2015. – №2. – С. 142-146.
91. Карташов, И.И. Цифровые доказательства» в уголовном процессе [Текст] / И.И. Карташов // Центральный научный вестник. – 2016. – №155. – С. 23-25.
92. Карташов, И.И. Проблемы формирования доказательств в уголовном судопроизводстве на основе цифровой информации [Текст] / И.И. Карташов // Юридическая наука. – 2018. – №3. – С. 99-103
93. Колычева, А.Л. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет [Текст] / А.Л. Колычева // Вестник Удмуртского университета. – 2017. – Т. 7. – Вып. 2. – С. 109-113.
94. Костенко, К.А. К вопросу об особенностях изъятия электронных носителей информации при расследовании служебных преступлений [Текст] / К.А. Костенко // Служебные преступления: вопросы теории и практики правоприменения: сб. материалов междунар. науч.-практ. конф. – Хабаровск, 2018. – С. 76-80.
95. Кукарникова, Т.Э. Компьютерная информация как следообразующая система [Текст] / Т.Э. Кукарникова // Криминалистика в системе правоприменения:

материалы конф. (Москва, 27-28 октября 2008 г.). – 2008. – С. 147-150.

96. Мухаммад, А.Н., Саидзода, Д. Информационные войны – угроза национальной безопасности. Социальные интернетсети как реальная угроза национальной безопасности [Текст] / А.Н. Мухаммад, Д. Саидзода // Материалы республиканской научно-теоретической конференции (г. Душанбе, 29 ноября 2022 г.). – С. 11-14.
97. Назаров, А.К., Салимов, Б.А. Криминалистическая тактика осмотра устройства мобильной связи (мобильного телефона) как источника доказательственной информации / А.К. Назаров, Б.А. Салимов // Наука и безопасность. – Душанбе, 2023. – №3 (5). – С. 104-109.
98. Оконенко, Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права [Текст] / Р.И. Оконенко // Актуальные проблемы российского права. – 2015. – №3. – С. 120-124.
99. Осипенко, А.Л. Особенности расследования сетевых компьютерных преступлений [Текст] / А.Л. Осипенко // Рос. юрид. журнал. – 2010. – №2 (71). – С. 121-126.
100. Осипенко, А.Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс [Текст] / А.Л. Осипенко // Научный вестник Омской академии МВД России. – 2009. – №4 (35). – С. 31-34.
101. Павловец, В.И. России нужны не биороботы, а креативный средний класс: о направлениях эффективного реформирования экономики и образования / В.И. Павловец // Альманах современной науки и образования. – 2013. – №1 (68). – С. 102-105.
102. Пастухов, П.С. Электронное вещественное доказательство в уголовном судопроизводстве [Текст] / П.С. Пастухов // Вестник Томского государственного университета. – 2015. – №396. – С. 149-153.
103. Поляков, В.В. Этапы осмотра места происшествия по компьютерным преступлениям [Текст] / В.В. Поляков // Закон и право. – 2016. – №11. – С. 112-114.

104. Поляков, В.В., Шебалин, А.В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон, по преступлениям в сфере компьютерной информации [Текст] / В.В. Поляков, А.В. Шебалин // Сборник материалов криминалистических чтений. – 2013. – №9. – С. 83-86.
105. Послание Президента Республики Таджикистан уважаемого Эмомали Рахмона «Об основных направлениях внутренней и внешней политики республики» (г. Душанбе, 23.12.2022 г.) [Электронный ресурс]. – Режим доступа: https://president.tj (дата обращения: 04.02.2023).
106. Пропастин, С.В. О проведении осмотра и обыска дистанционно [Текст] / С.В. Пропастин // Сборник материалов Барнаульских криминалистических чтений. – 2012. – С. 75-76.
107. Россинская, Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности [Текст] / Е.Р. Россинская // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – №3-2. – С. 109-117.
108. Россинская, Е.Р., Шамаев, Г.П. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники. Уголовно-процессуальные и криминалистические средства обеспечения эффективности уголовного судопроизводства [Текст] / Е.Р. Россинская, Г.П. Шамаев // Материалы междунар. науч.-практ. конф. – Иркутск, – 2014. – С. 317-325.
109. Савельева, М.В., Степанов, В.В. О понятии криминалистической информации [Текст] / М.В. Савельева, В.В. Степанов // Вестник криминалистики / Отв. ред. Филиппов А.Г. – 2009. – Вып. 4 (32). – С. 14-21.
110. Семенов, А.Ю. Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации [Текст] / А.Ю. Семенов // Сибирский юридический вестник. – 2004. – №1. – С. 53-55.

111. Скобелин, С.Ю. Использование специальных знаний при работе с электронными следами [Текст] / С.Ю. Скобелин // Российский следователь. – 2014. – №20. – С. 31-33.
112. Смагин, П.Г. О понятии «компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД [Текст] / П.Г. Смагин // Вестник Воронежского института МВД России. – 2008. – №1. – С. 80-81.
113. Смушкин, А.Б. Виртуальные следы в криминалистике [Текст] / А.Б. Смушкин // Законность. – 2012. – №8 (934). – С. 43-45.
114. Старикова, М.Р. Значение электронных следов в расследовании преступлений. Обеспечение прав и свобод человека в уголовном судопроизводстве: организационные, процессуальные и криминалистические аспекты [Текст] / М.Р. Старикова // Сб. статей по мат. междунар. студ. науч.-практ. конф. – 2017. – С. 232-234.
115. Старичков, М.В. Понятие «компьютерная информация» в российском уголовном праве [Текст] / М.В. Старичков // Вестник Восточно-Сибирского института МВД России. – 2014. – №1. – С. 16-20.
116. Сысенко, А.Р., Смирнова, И.С., Тимошенко, С.Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы [Текст] / А.Р. Сысенко, И.С. Смирнова, С.Е. Тимошенко // Сибирское юридическое обозрение. – 2020. – Том 17. – №4. – С. 524-532.
117. Третьякова, Е.И. Мобильный телефон как источник криминалистически значимой информации [Текст] / Е.И. Третьякова // Вестник Уральского финансово-юридического института. – 2018. – №3 (13). – С. 49-51.
118. Усов, А.И. Основы методического обеспечения судебно-экспертного исследования компьютерных средств и систем [Текст] / А.И. Усов // Право и закон. – М., 2002. – С. 33-36.
119. Хусяинов, Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве [Текст] / Т.М. Хусяинов // Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования. Материалы всероссийского круглого стола. – 2015. – С.

120-125.

120. Шувалов, М.Н., Шувалова, А.М. Применение криминалистической техники при расследовании коррупционных преступлений [Текст] / М.Н. Шувалов, А.М. Шувалова // Гуманитарные, социально-экономические и общественные науки. – 2016. – №12. – С. 210-214.

121. Щетилов, А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом [Текст] / А. Щетилов // Информатизация и информационная безопасность правоохранительных органов: материалы XI междунар. конф. – М., 2002. – С. 186-188.

IV. Диссертации и авторефераты:

122. Агибалов, В.Ю. Виртуальные следы в криминалистике и уголовном процессе [Текст]: дис. ... канд. юрид. наук: 12.00.09 / Агибалов Владимир Юрьевич. – Воронеж, 2010. – 198 с.

123. Андрющенко, Е.С. Интернет-отношения: государственное регулирование и саморегулирование [Текст]: автореф. дис. … канд. юрид. наук: 12.00.14 / Андрющенко Екатерина Сергеевна. – Саратов, 2010. – 26 с.

124. Балашова, А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании [Текст]: дис. … канд. юрид. наук: 12.00.12 / Балашова Анна Александровна. – Москва, 2020. – 214 с.

125. Ворожбит, С.П. Электронные средства доказывания в гражданском и арбитражном процессе [Текст]: автореф. дис. … канд. юрид. наук: 12.00.15 / Ворожбит Светлана Петровна. – Санкт-Петербург, 2011. – С. 25.

126. Гаврилин, Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы [Текст]: автореф. дис. … д-ра юрид. наук: 12.00.09 / Гаврилин Юрий Викторович. – Москва, 2010. – 56 с.

127. Григорьев, А.Н. Теоретические аспекты информации и ее защиты в предварительном расследовании преступлений [Текст]: автореф. дис. … канд. юрид. наук: 12.00.09 / Григорьев Анатолий Николаевич. – Калининград, 2002. – 23 с.

128. Гузеева, О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы) [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.08 / Гузеева Ольга Сергеевна. – Москва, 2008. – 25 с.
129. Илюшин, Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет [Текст]: дис. ... канд. юрид. наук: 12.00.09 / Илюшин Денис Анатольевич. – Волгоград, 2008 – 233 с.
130. Камышин, В.А. Иные документы как «свободное» доказательство в уголовном процессе [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.09 / Камышин Владимир Анатольевич. – Ижевск, 1998. – 23 с.
131. Колычева, А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет [Текст]: дис. … канд. юрид. наук: 12.00.12 / Колычева Алла Николаевна – Москва, 2018. – 199 с.
132. Краснова, Л.Б. Компьютерные объекты в уголовном процессе и криминалистике [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.09 / Краснова Людмила Борисовна. – Воронеж, 2005. – 24 с.
133. Крылов, В.В. Основы криминалистической теории расследования преступлений в сфере информации [Текст]: дис. ... д-ра юрид. наук: 12.00.09 / Крылов Владимир Вадимович. – М., 1998. – 334 с.
134. Лыткин, Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности [Текст]: дис. … канд. юрид. наук: 12.00.09 / Лыткин Николай Николаевич. – Москва, 2007. – 201 с.
135. Лыткин, Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.09 / Лыткин Николай Николаевич. – М., 2007. – 24 с.
136. Мещеряков, В.А. Основы методики расследования преступлений в сфере компьютерной информации [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.09 / Мещеряков Владимир Алексеевич. – Воронеж, 2001. – 39 с.
137. Милашев, В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ [Текст]:

автореф. ... канд. юрид. наук: 12.00.09 / Милашев Вадим Александрович. – Москва, 2004. – 21 с.

138. Паршина, Е.Н. Проблемы информационного обеспечения и защиты информации в предварительном расследовании [Текст]: автореф. дис. … канд. юрид. наук: 12.00.09 / Паршина Елена Николаевна. – Ижевск, 2004. – 24 с.
139. Простосердов, М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им [Текст]: дис. … канд. юрид. наук: 12.00.08 / Простосердов Михаил Александрович. – Москва, 2016. – 232 с.
140. Рахимзода, Р.Х. Оперативно-розыскная политика по обеспечению экономической безопасности Республики Таджикистан: проблемы теории, методологии и практики (историко-правовой и общетеоретический анализ) [Текст]: дис. … д-ра юрид. наук: 12.00.12 / Рахимзода Рамазон Хамро. – Душанбе, 2018. – 581 с.
141. Рудых, А.А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.12 / Рудых Алексей Александрович. – Ростов н/Д., 2020. – 26 с.
142. Салихов, И.И. Информация с ограниченным доступом как объект гражданско-правовых правоотношений [Текст]: автореф. дис. … канд. юрид. наук: 12.00.03 / Салихов Ильсур Ильгизович. – Казань, 2004. – 24 с.
143. Себякин, А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации [Текст]: дис. ... канд. юрид. наук: 12.00.09 / Себякин Алексей Геннадьевич. – Москва, 2021. – 271 с.
144. Смирнова, Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации [Текст]: дис. … канд. юрид. наук: 12.00.08 / Смирнова Татьяна Георгиевна. – Москва, 1999. – 161 с.
145. Усов, А.И. Концептуальные основы судебной компьютернотехнической экспертизы [Текст]: дис. … д-ра юрид. наук: 12.00.09 / Усов Алексей Иванович. – Москва, 2002. – 402 с.

146. Шевченко, Е.С. Тактика производства следственных действий при расследовании киберпреступлений [Текст]: дис. ... канд. юрид. наук: 12.00.12 / Шевченко Елизавета Сергеевна. – Москва, 2016. – 249 с.

V. Электронные источники [Электронный ресурс]:

147. Бутенко А.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия [Электронный ресурс]. – Режим доступа: https: //cyberleninka.ru/article/n/ (дата обращения: 25.07.2022).

148. Габриэль Вейманн. Террор в Интернете: новая арена, новые вызовы [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=31577354 (дата обращения: 25.07.2022).

149. Документ [Электронный ресурс]. – Режим доступа: https:// ru.wikipedia.org/wiki (дата обращения: 22.02.2023).

150. Европейская комиссия, Экспертная группа по насильственной радикализации, «Процессы радикализации, ведущие к террористическим актам» (2008) [Электронный ресурс]. – Режим доступа: https: www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf (дата обращения: 09.03.2023).

151. Интернет и соцсети в начале 2023 года – главные цифры Global Digital 2023 [Электронный ресурс]. – Режим доступа: URL: https://vc.ru/marketing/596126-internet-i-socseti-v-nachale-2023-goda-glavnye-cifry-global-digital-2023 (дата обращения: 20.08.2023).

152. Использование Интернета в террористических целях [Электронный ресурс]. – Режим доступа: https://www.academia.edu/34098438/ International Terrorism Assignment (дата обращения: 09.03.2023).

153. Маура Конвей. Использование Интернета террористами и борьба с ними [Электронный ресурс]. – Режим доступа: https://www.academia.edu/34098438/International_Terrorism_Assignment (дата обращения: 09.03.2023).

154. Обзор Глобальной контртеррористической стратегии ООН (A/RES/70/291), пункт 42, 19 июля 2016 [Электронный ресурс]. – Режим доступа:

https://www.isdglobal.org/wp-content/uploads/2019/12/Policy-Toolkit-on-Z-L-Recommendations-RUS.pdf (дата обращения: 09.03.2023).

155. Платёнкин А.В. Особенности использования электронных доказательств при проведении допроса подозреваемого [Электронный ресурс]. – Режим доступа:https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-elektronnyh-dokazatelstv-pri-provedenii-doprosa-podozrevaemogo (дата обращения: 25.08.2023).
156. Практическое руководство по производству судебных экспертиз для экспертов и специалистов: науч.-практ. пособие / Под ред. Т.В. Аверьяновой, В.Ф. Статкуса. 2-е изд., перераб. и доп. [Электронный ресурс]. – Режим доступа: https://fse.ms/library/prakticheskoe-rukovodstvo-po-proizvodstvu-sudebnyh-ekspertiz-dlya-ekspertov-i-spetsialistov-averyanova-t-v-statkusa-v-f/ (дата обращения: 09.03.2023).
157. Резолюция Совета Безопасности ООН 2322 (2016). Угрозы международному миру и безопасности, создаваемые террористическими актами [Электронный ресурс]. – Режим доступа: URL: https://capve.org/components/com_jshopping/files/demo_products/2322.pdf (дата обращения: 04.07.2023).
158. Резолюция Совета Безопасности ООН 2331 (2016) [Электронный ресурс]. – Режим доступа: URL: https://www.hrnk.org/uploads/pdfs/ N1640753.pdf (дата обращения: 04.07.2023).
159. Резолюция Совета Безопасности ООН 2341 (2017) [Электронный ресурс]. – Режим доступа: URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf?OpenElement (дата обращения: 04.07.2023).
160. Резолюция Совета Безопасности ООН 2396 (2017) [Электронный ресурс]. – Режим доступа: URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/27/PDF/N1746027.pdf?OpenElement (дата обращения: 04.07.2023).
161. Скотт Гервер и Сара Дейли, «Аль-Каида: отбор и вербовка террористов», в Справочнике по национальной безопасности McGraw-Hill, Дэвид Камьен, изд. (Нью-Йорк, McGraw-Hill, 2006) [Электронный ресурс]. – Режим доступа: https:

www.clingendael.nl/publications (дата обращения: 09.03.2023).

162. Словарь терминов Интернет [Электронный ресурс]. – Режим доступа: URS: http/your-hosting.ru/terms/i/internet/ (дата обращения: 25.04.2022).

VI. Правоприменительная практика:

163. Уголовное дело №12434 // Архив ГКНБ РТ. – 2011

164. Уголовное дело №13212 // Архив ГКНБ РТ. – 2016

165. Уголовное дело №15337 // Архив ГКНБ РТ. – 2016

166. Уголовное дело №19630 // Архив ГКНБ РТ. – 2019.

167. Уголовное дело №15185 // Архив ГКНБ РТ. – 2021

168. Уголовное дело №23131 // Архив ГКНБ РТ. – 2021

169. Уголовное дело №23139 // Архив ГКНБ РТ. – 2021

170. Уголовное дело № 22834 // Архив ГКНБ РТ. – 2021

171. Уголовное дело №22903 // Архив ГКНБ РТ. – 2021

172. Уголовное дело №22909 // Архив ГКНБ РТ. – 2022

ПЕРЕЧЕНЬ

НАУЧНЫХ ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

I. Монографии, учебники, учебные пособия:

[1-А]. Салимов, Б.А. Криминалистическая тактика осмотра электронно-цифровой информации, хранящейся на локальных и сетевых носителях: практическое пособие [Текст] / Б.А. Салимов. – Душанбе: Высшая школа ГКНБ Республики Таджикистан, 2023. – 56 с.; УДК: 343.9 (575.3). ББК: 67.99 (2) 8 (2 тадж.).

[2-А]. Салимов, Б.А. Тактикаи криминалистии азназаргузаронии иттилооти электронӣ-рақамӣ: дастури амалӣ [Матн] / Б.А. Салимов. – Душанбе: Мактаби олии КДАМ Ҷумҳурии Тоҷикистон, 2023. – 72 с.; ТДУ: 343.9 (575.3). ТКБ: 67.99 (2) 8 (2 тоҷик).

II. Статьи, опубликованные в рецензируемых и рекомендованных Высшей аттестационной комиссией при Президенте Республики Таджикистан журналах:

[3-А]. Салимов, Б.А. Понятие и значение цифровой информации в криминалистике [Текст] / Б.А. Салимов // Вестник Таджикского национального университета. – 2021. – №1. – С. 111-117; ISSN 2413-5151.

[4-А]. Салимов, Б.А. Иттилооти электронӣ-рақамӣ ва мавқеи он дар низоми далелҳо оид ба парвандаҳои ҷиноятӣ [Матн] / Б.А. Салимов // Осори Академияи ВКД Ҷумҳурии Тоҷикистон. – 2022. – №2 (54). – С. 88-94; ISSN 2412-141X.

[5-А]. Салимов, Б.А. Тактические особенности собирания доказательственной электронно-цифровой информации [Текст] / Б.А. Салимов // Научно-аналитический журнал «Законодательство». – 2022. – №3 (47). – С. 92-99; ISSN 2410-2903.

[6-А]. Салимов, Б.А. Особенности обнаружения и фиксации электронно-цифровых следов, содержащихся на ресурсах сети Интернет [Текст] / Б.А. Салимов // Труды Академии МВД Республики Таджикистан. – 2022. – №4 (56). – С. 162-171; ISSN 2412-141X.

[7-А]. Назаров, А.К., Салимов, Б.А. Тактикаи криминалистии азназаргузаронии дастгоҳи алоқаи мобилӣ (телефони мобилӣ) ҳамчун манбаи иттилооти исботкунанда [Матн] / А.К. Назаров, Б.А. Салимов // Маҷаллаи илмии Мактаби олии КДАМ Ҷумҳурии Тоҷикистон «Илм ва амният». – 2023. – №3 (5). – С. 104-109; ISSN: 2959-6394.

III. Научные статьи, опубликованные в сборниках и других научно-практических изданиях:

[8-А]. Салимов, Б.А. Паҳнкунии идеологияи терроризм ва экстремизм бо истифода аз технологияҳои иттилоотӣ [Матн] / Б.А. Салимов // Маҷмуаи мақолаҳои II–юмин Конференсияи илмӣ-амалии байналмилалӣ дар мавзуи «Илми ҳуқуқшиносӣ ва амалияи он» бахшида ба Рӯзи илми тоҷик (Душанбе, 29 апрели с. 2023). – Душанбе, 2023. – С. 284-287.

[9-А]. Салимов, Б.А. Информационное общество: безграничные возможности – новые угрозы [Текст] / Б.А. Салимов // Материалы Международной научно-практической конференции «Таджики в зеркале истории», посвященной 115-летию академика АН СССР Б. Гафурова (Душанбе, 27 октября 2023 г.). – Душанбе, 2023. – С. 163-168.

ПРИЛОЖЕНИЕ 1

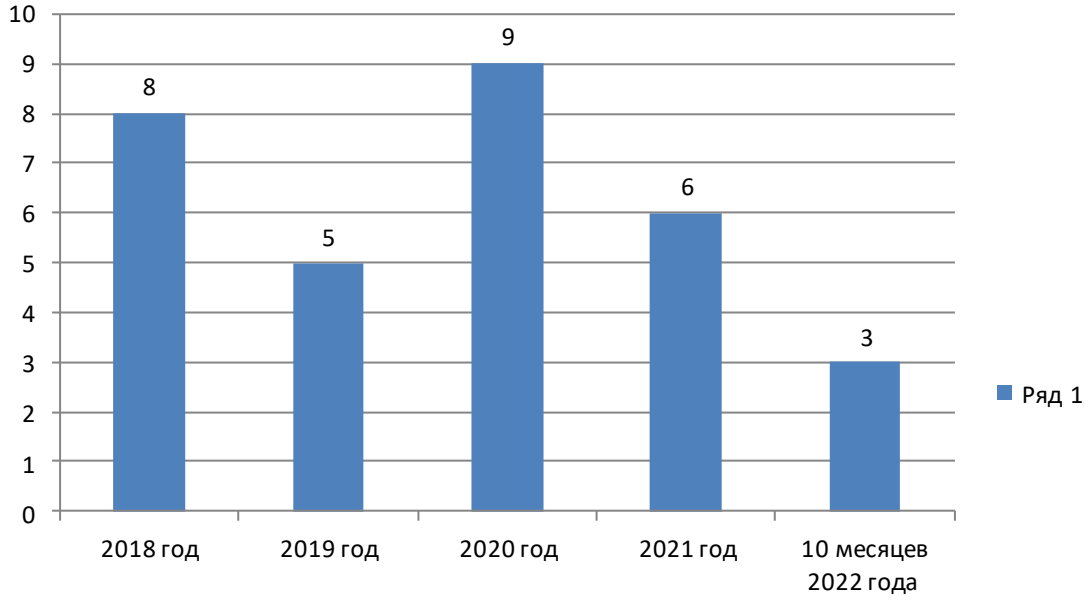

Рисунок №1.1. Количество зарегистрированных преступлений по ч. 2 ст. 137, ч. 2 ст. 137 (1) УК РТ

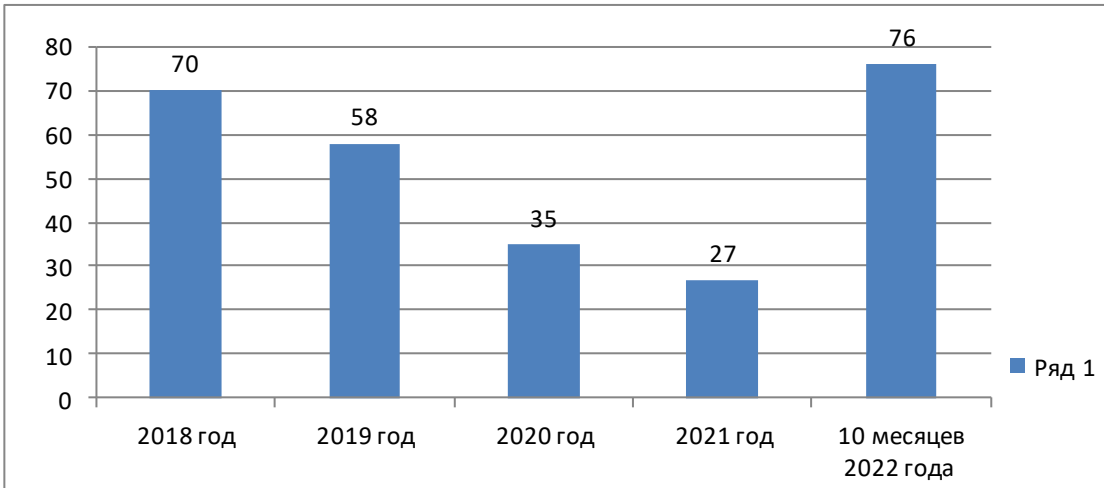

Рисунок №1.2. Количество зарегистрированных преступлений по п. «г» ч. 2 ст. 179 (1), ч. 2 ст. 179 (3) УК РТ

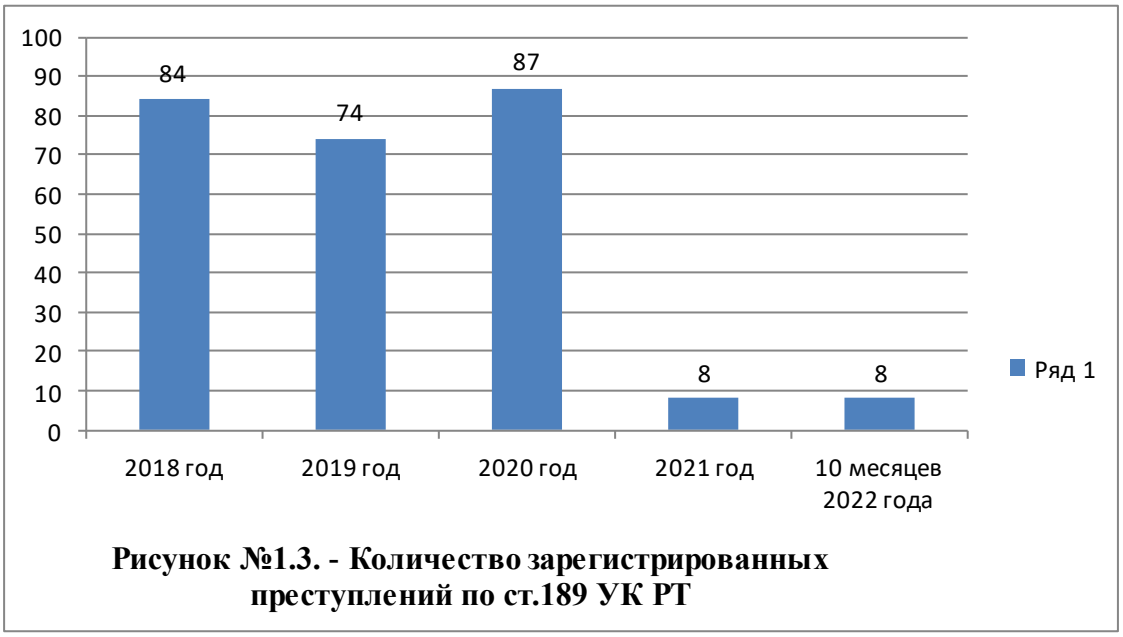

Рисунок №1.3. - Количество зарегистрированных преступлений по ст.189 УК РТ

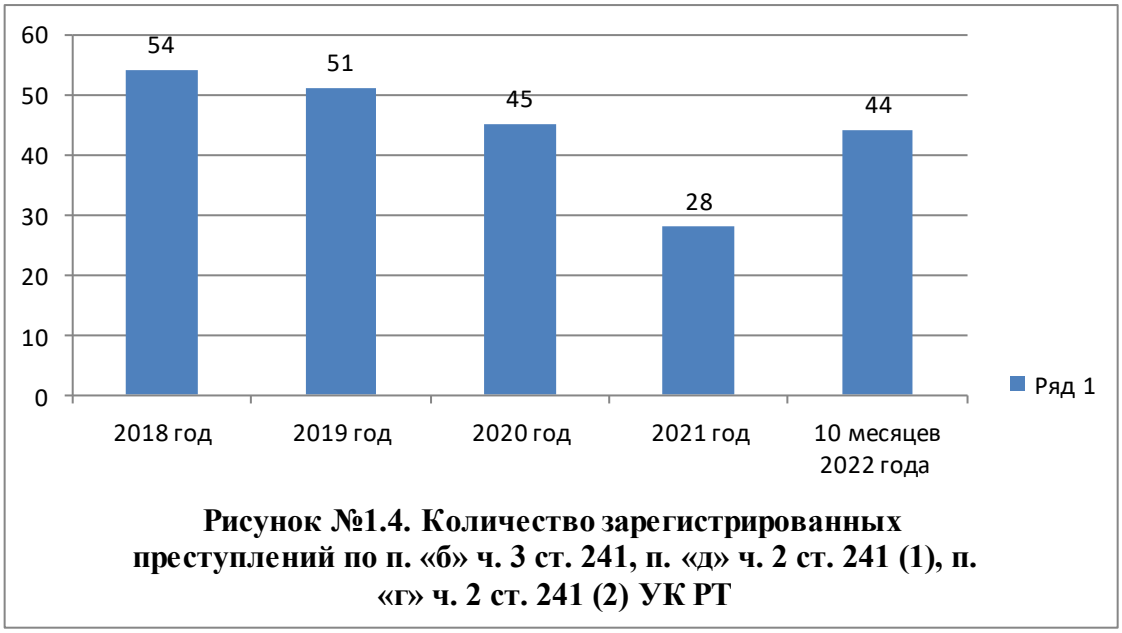

Рисунок №1.4. Количество зарегистрированных преступлений по п. «б» ч. 3 ст. 241, п. «д» ч. 2 ст. 241 (1), п. «г» ч. 2 ст. 241 (2) УК РТ

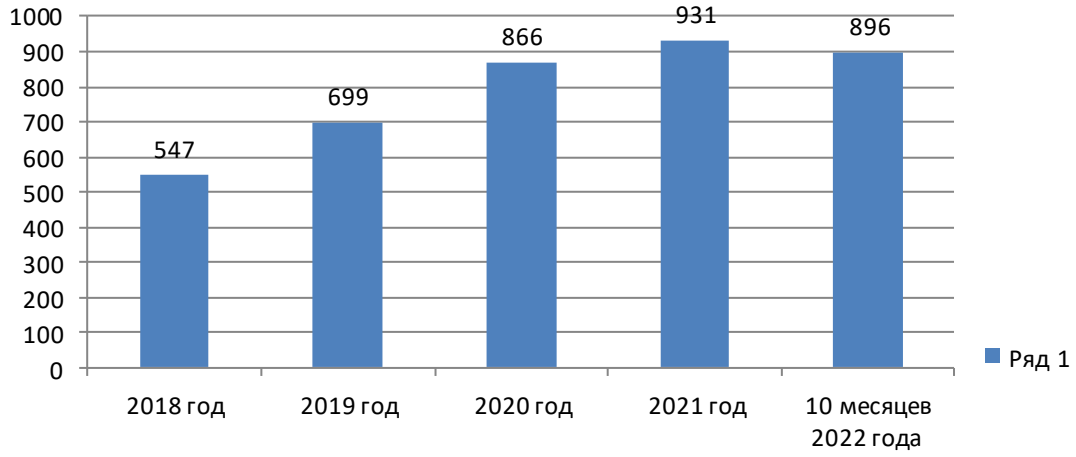

Рисунок №1.5. Количество зарегистрированных преступлений по п. «г» ч. 2 ст. 307, ч. 2 ст. 307 (1), ч. 2 ст. 307 (3) УК РТ

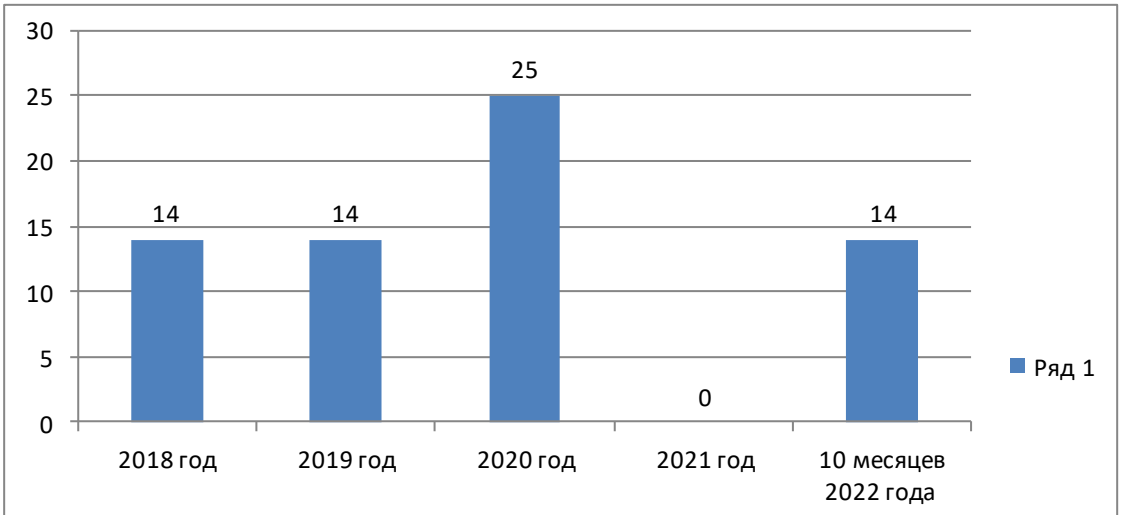

Рисунок №1.6. Количество зарегистрированных преступлений по ст.ст. 298, 299, 301 УК РТ

ПРИЛОЖЕНИЕ 2

ОПРОСНЫЙ ЛИСТ

для сотрудников следственных подразделений Государственного комитета национальной безопасности Республики Таджикистан

В рамках проведения научно-исследовательской работы на тему «Особенности обнаружения и фиксации доказательственной электронно-цифровой информации», Высшая школа ГКНБ Республики Таджикистан проводит анкетирование следователей в целях изучения опыта расследования преступлений, совершаемых с использованием информационных технологий, а также выявления недостаток при фиксации электронных доказательств.

Просим вас ответить на приведенные ниже вопросы, проявив предельную внимательность и объективность. Анкетирование проводится анонимно.

Мы признательны вам за оказанную помощь в проводимом исследовании.

1. Стаж работы в должности следователя:

a) от 1 года до 3 лет;

b) от 3 до 5 лет;

c) от 5 до 10 лет;

d) более 10 лет.

2.Участвовали ли Вы в расследовании преступлений, совершенных с использованием информационных технологий или ресурсов глобальной сети Интернет?

a) да;

b) нет.

3.В расследовании каких преступлений, совершенных с использованием информационных технологий или ресурсов глобальной сети Интернет, вам приходилось участвовать?

a) преступлений террористического характера;

b) преступлений экстремистского характера;

c) проникновение в телекоммуникационные сети банковских структур с целью хищения денежных средств клиентов;

d) размещение интернет-сайтов азартных игр;

e) преступлений против информационной безопасности;

f) изготовление и распространение порнографических материалов;

g) иных преступлений (указать, какое) _____

4. Основанием для возбуждения уголовного дела являлось:

a) заявление потерпевшей стороны о преступлении;

b) явка с повинной;

c) сообщение должностного лица предприятия, учреждения и организации;

d) непосредственное обнаружение дознавателем, следователем или прокурором сведений, указывающих на признаки преступления;

e) выявление признаков преступлений данной категории при расследовании других преступлений;

f) сообщение в средствах массовой информации.

5. Привлекали ли вы при проведении следственных действий в рамках расследования преступлений, совершенных с использованием информационных технологий, специалиста соответствующего профиля? Если да, то в каких?

a) нет, специалист не был привлечён;

b) да, при осмотре места происшествия;

c) да, при осмотре предметов;

d) да, при осмотре электронных документов;

e) да, при осмотре информации, содержащейся на ресурсах сети Интернет, а также выемке данной информации;

f) да, при назначении судебно-компьютерной экспертизы;

g) да, при производстве иных процессуальных действий (указать каких) _____.

6. При осмотре места происшествия по делам рассматриваемой категории, сотрудники каких подразделений были включены в состав следственно-оперативной группы?

a) только следователь;

b) следователь и сотрудник-специалист органов национальной безопасности;

c) следователь и специалист IT-технологий;

d) иные лица.

7.Какие объекты изымались наиболее часто в ходе осмотра места происшествия?

a) технические средства;

b) электронный носитель;

c) программные средства;

d) электронный документ;

e) файлы с информацией;

f) пластиковая карта;

g) иные предметы (указать, какие) _____

8.Назначали ли вы по уголовным делам судебно-компьютерную экспертизу (СКЭ), если да, то кому было поручено её производство?

a) нет, не было необходимости в проведении СКЭ;

b) нет, в связи с отсутствием соответствующего экспертного учреждения;

c) да, её производство было возложено на Республиканский центр судебных и криминалистических экспертиз Министерства юстиции Республики Таджикистан;

d) да, её производство было возложено на Республиканский центр судебных и криминалистических экспертиз Министерства внутренних дел Республики Таджикистан;

e) да, её производство было возложено на иное экспертное учреждение (укажите, какое) _____

9. Какие объекты чаще всего направлялись для проведения СКЭ по преступлениям, совершённым с использованием информационных технологий?

a) технические средства;

b) электронный носитель;

c) программные средства;

d) электронный документ;

e) файлы с информацией;

f) пластиковые карты;

g) иные объекты (указать, какие) _____

10. В ходе расследования преступлений названной категории получали ли вы доказательства с электронных носителей информации?

a) да, часто;

b) да, но не часто;

c) нет, не получал.

11. В какой процессуальной форме изымались объекты-носители электронно-цифровых следов?

a) в ходе обыска;

b) в ходе выемки;

c) при осмотре места происшествия;

d) при осмотре предметов;

e) при личном обыске;

f) при наложении ареста на почтово-телеграфные отправления согласно ст.195 УПК РТ;

g) в ходе ареста имущества;

h) представление с результатами оперативно-розыскной деятельности;

i) иным образом (указать, каким) _____.

12. В каких направлениях расследования уголовных дел были использованы данные, полученные с объектов-носителей электронно-цифровой информации?

a) при определении направления расследования и выдвижении версий по уголовному делу;

b) для установления события преступления;

c) при розыскной работе следователя;

d) для установления лица, совершившего преступление;

e) при доказывании виновности лица в совершении преступления;

f) в других направлениях (указать, каких) _____.

13. В современном обществе электронно-цифровая информация играет большую роль в процессе доказывания по уголовным делам. На ваш взгляд, стоит

ли признавать электронно-цифровую информацию как отдельный вид доказательств и включить её в ст. 72 УПК Республики Таджикистан?

a) да, в связи с тем, что_____.

b) нет, поскольку_____.

14. В Уголовно-процессуальном кодексе Республики Таджикистан не предусмотрены процессуальные средства собирания доказательственной информации из информационно-телекоммуникационных сетей. Считаете ли вы необходимым дополнить настоящий Кодекс новой статьёй 183 (1) «Дистанционный осмотр электронно-цифровых информационных ресурсов»?

a) Да: _____

b) Нет: _____

15. С какими проблемами вы встречались при собирании доказательственной информации в компьютерных сетях, устройствах мобильной связи и других электронных носителях, укажите?

_____

_____

_____

ПРИЛОЖЕНИЕ 3

Справка
по результатам анкетирования сотрудников следственных подразделений ГКНБ Республики Таджикистан

В ходе анкетирования было опрошено 38 следователей центрального аппарата и территориальных подразделений Государственного комитета национальной безопасности Республики Таджикистан.

Опрошенные респонденты имели следующий стаж работы в должности следователя:

от 1 года до 3 лет – 39,5%;

от 3 до 5 лет – 13%;

от 5 до 10 лет – 18,5%;

более 10 лет – 29%.

Подавляющее большинство опрошенных (92,3%) заявили, что в процессе расследования преступлений, совершённых с использованием информационных технологий, им приходилось получать доказательства с электронных носителей информации, 7,7% ответили отрицательно.

На вопрос, в расследовании каких преступлений, совершённых с использованием информационных технологий или ресурсов глобальной сети Интернет, им приходилось участвовать, респонденты ответили, что в 58,8% случаев при расследовании преступлений экстремистского характера, в 35,3% случаев – преступлений террористической направленности и в 5,9% случаев – преступлений против информационной безопасности.

Основанием для возбуждения уголовного дела по преступлениям рассматриваемой категории в 44,9% случаев являлось непосредственное обнаружение дознавателем, следователем или прокурором сведений, указывающих на признаки состава преступления, в 15,4% случаев – выявление признаков преступлений данного вида при расследовании других преступлений, в 12,8% случаев – сообщение в средствах массовой информации, в 10,25% случаев – заявление потерпевшей стороны о преступлении, столько же – сообщение

должностного лица предприятия, учреждения и организации и в 6,4% случаев – явка с повинной.

Опрос респондентов показал, что в рамках расследования преступлений, совершённых с использованием информационных технологий, специалисты соответствующего профиля чаще всего привлекались при осмотре информации, содержащейся на ресурсах сети Интернет (36,7%), назначении судебно-компьютерной экспертизы (33,3%), осмотре места происшествия (10%), осмотре электронных документов (8,3%), осмотре предметов (6,7%). При этом 5% опрошенных отметили, что специалистов вообще не привлекали.

В ходе анкетирования удалось выяснить, в каких процессуальных формах производилось изъятие объектов-носителей электронно-цифровых следов. Ответы были следующие: в 33,3% случаев в ходе осмотра места происшествия, в 15,5% случаев представлены с результатами оперативно-розыскной деятельности, в 14,4% случаев в ходе обыска, в 13,4% случаев в ходе осмотра предметов, в 13,4% случаев в ходе личного обыска, в 6,6% случаев в ходе выемки и в 3,4% случаев при наложении ареста на почтово-телеграфные отправления**.**

Респонденты указали, что в ходе осмотра места происшествия по делам о преступлениях, совершённых с использованием информационных технологий, они изымали следующие предметы в процентном отношении:

технические средства – 28,4%;

электронные носители информации – 17,5%;

программные средства – 5,4%;

электронные документы – 23%;

файлы с информацией – 23%;

пластиковые карты – 2,7%.

На поставленный вопрос о том, в каких направлениях расследования уголовных дел были использованы данные, полученные с объектов-носителей электронно-цифровой информации, опрошенные ответили, что собранные сведения использовались при определении направления расследования и выдвижении версий по уголовному делу (6%), для установления события

преступления (23,2%), при розыскной работе следователя (12,2%), для установления лица, совершившего преступление (23,2%) и при доказывании виновности лица в совершении преступления (35,4%).

Относительно признания электронно-цифровой информации как отдельный вид доказательств и включения её в ст. 72 УПК Республики Таджикистан, положительно ответили 87,2% анкетированных и 12,8% опрошенных не видят в этом необходимости.

84,6% респондентов считают необходимым введения в Уголовно-процессуальный кодекс Республики Таджикистан новых процессуальных средств собирания доказательственной информации из информационно-телекоммуникационных сетей («Дистанционный осмотр электронно-цифровых информационных ресурсов» и «Дистанционный обыск»). Вместе с тем, 15,4% ответило отрицательно.

Среди существующих проблем собирания доказательственной информации в компьютерных сетях, устройствах мобильной связи и других электронных носителях, с которыми им приходилось столкнуться, респонденты отметили: недостаточное количество IT-специалистов, отсутствие технических средств вскрытия заблокированных устройств, невозможность восстановления удалённых данных в компьютерных сетях, анонимность и использование чужих данных при регистрации аккаунтов.