Научная статья
https://doi.org/10.24412/2658-7335-2025-4-6
УДК 343.98

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОИЗВОДСТВА СЛЕДСТВЕННОГО ОСМОТРА ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Лозовский Д.Н.[1], Ульянова И.Р.[2]
Кубанский институт социэкономики и права (филиал Академии труда и социальных отношений)[1],
Краснодарский университет МВД России[2]

Аннотация. *В статье авторами рассмотрены особенности производства следственного осмотра при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий. Диапазон правонарушений простирается от сетевых домогательств до комплексных мошеннических операций и несанкционированного доступа к конфиденциальным сведениям. Специфика данных преступлений выходит за рамки традиционных криминальных схем, зачастую представляя собой сложные многоступенчатые операции, требующие особого криминалистического подхода. В рамках статьи рассмотрена классификация следственного осмотра, уголовно-процессуальные и криминалистические аспекты проведения отдельных видов данного следственного действия. В ходе изучения судебно-следственной практики выявлены проблемные аспекты и предложены пути их решения. По итогам исследования разработаны отдельные рекомендации по совершенствованию производственного следственного осмотра по делам исследуемой категории.*

Ключевые слова: *следственный осмотр, осмотр места происшествия, осмотра предметов и документов, тактика производства следственных действий, преступления в сфере информационно-коммуникационных технологий; организация производства следственных действий.*

Финансирование: *инициативная работа.*

Original article

CERTAIN ASPECTS OF THE INVESTIGATIVE INSPECTION IN CRIMINAL CASES OF CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Denis N. Lozovsky[1], Irina R. Ulyanova[2]
Kuban Institute of Socio-Economics and Law (branch of the Academy of Labor and Social Relations)[1],
Krasnodar University of the Ministry of Internal Affairs of Russia[2]

Abstract. *In the article, the authors consider the specifics of conducting an investigative inspection in the investigation of crimes committed using information and communication technologies. The range of offenses ranges from online harassment to complex fraudulent transactions and unauthorized access to confidential information. The specifics of these crimes go beyond the traditional criminal schemes, often representing complex multi-stage operations that require a special forensic approach. The article considers the classification of the investigative examination, the criminal procedural and criminalistic aspects of certain types of this investigative action. During the study of judicial and investigative practice, problematic aspects were identified and ways of solving them were proposed. Based on the results of the study, separate recommendations have been developed to improve the industrial investigative inspection in cases of the category under study.*

Keywords: *investigative inspection, inspection of the scene, inspection of objects and documents, tactics of investigative actions, crimes in the field of information and communication technologies; organization of investigative actions.*

Funding: *Independent work.*

Введение.

Преступные деяния в области информационно-коммуникационных технологий сегодня представляют собой динамично эволюционирующий сегмент криминалистической практики.

На фоне цифровой трансформации общества и экспоненциального роста обрабатываемой информации, противоправные действия в сфере информационно-коммуникационных технологий (далее – ИКТ) приобретают все более изощренный характер. Диапазон таких правонарушений простирается от сетевых домогательств до комплексных мошеннических операций и несанкционированного доступа к конфиденциальным сведениям. Специфика данных преступлений выходит за рамки традиционных криминальных схем, зачастую представляя собой сложные многоступенчатые операции, требующие особого криминалистического подхода.

Обсуждение.

Следственный осмотр является следственным действием, представляющим собой процесс прямого восприятия осматриваемых объектов с целью обнаружения и закрепления их признаков и свойств, позволяющих судить об обстоятельствах расследуемого события.

В соответствии со статьей 176 УПК РФ, осмотр места происшествия, местности, жилища, иного помещения, предметов и документов производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела.

А.А. Эксархопуло считает, что следственный осмотр следует классифицировать:

1. По объему осмотра:

– осмотр места происшествия (местности, жилища, иных помещений) (ч. 1 ст. 176 УПК РФ);

– осмотр помещений и местности, не являющихся местом происшествия (ч. 1 ст. 176 УПК РФ);

– осмотр трупа (ст. 178 УПК РФ);

– осмотр предметов и документов (ч. 1 ст. 176 УПК РФ);

– осмотр живых лиц (освидетельствование).

2. По последовательности:

– первичный;

– повторный (если первичный был проведен некачественно, без использования технических средств или ввиду объективной невозможности его качественного проведения).

3. По объему:

– основной;

– дополнительный (если требуется расширить границу ранее осмотренного участка либо осмотреть ранее не осмотренные участки в пределах границ) [1].

Следственный осмотр является важным процессуальным действием в рамках расследования преступлений в сфере ИКТ. В отличие от других дел, где в центре внимания вещественные доказательства и видимые следы, в расследовании киберпреступлений основной упор делается на анализ цифровой информации. Это влечет за собой изменения в методике самого осмотра.

Прежде всего, необходимо подчеркнуть нестандартную природу осмотра места происшествия в расследовании киберпреступлений.

С одной стороны, осмотр может охватывать физические объекты: рабочее пространство подозреваемого, офисные помещения, серверные комнаты, где физически размещена техника, предположительно хранящая информацию, релевантную для расследования.

С другой стороны, в сферу следственного интереса попадают логические структуры: жесткие диски, файловые системы, логи сетевых подключений, содержимое электронной почты, облачных хранилищ и даже данные, переданные по каналам связи в момент совершения противоправных действий.

Тактика проведения осмотра в подобных ситуациях должна быть выстроена с учетом специфики работы с цифровыми доказательствами.

Основной задачей следователя является гарантирование их целостности и подлинности. Для этого активно используется метод создания копий носителей информации с использованием специализированных технических средств и программных решений [2]. Процесс же фиксации действий протоколируется не только в официальном протоколе, но и посредством видеофиксации.

Визуальный осмотр помещения должен включать анализ следующих характеристик:

- тип помещения (административное, жилое, общественное или служебное);

- наличие систем безопасности (охрана, сигнализация, видеонаблюдение);

- состояние и надежность входных групп и оконных проемов [3].

Такой структурированный подход обеспечивает полноту и достоверность собранных доказательств.

Изучение судебно-следственной практики расследования преступлений в сфере ИКТ, наглядно демонстрирует важность качественного проведения следственных осмотров и фиксации цифровых данных. В частности, из материалов дела приговора Заводского районного суда г. Саратова (Саратовская область) № 1-538/2024 от 21 ноября 2024 г. по делу № 1-538/2024 [4], следует, что ФИО1 четырежды совершила неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование компьютерной информации, лицом с использованием своего служебного положения.

В данном приговоре описаны следующие следственные действия:

– осмотр оптических дисков с трудовыми документами подозреваемой, сканированными договорами и личными данными абонентов;

– осмотр мобильного телефона подозреваемой с записями переписок и голосовыми сообщениями, имеющими отношение к противоправным действиям;

– осмотр видеозаписей с камер наблюдения, зафиксировавших ее действия в рабочем помещении;

– изъятие мобильного телефона в рамках процессуального действия по расследованию.

Каждое из вышеуказанных действий было тщательно запротоколировано. Это позволило гарантировать допустимость полученных доказательств и полностью подтвердить факт незаконного доступа к компьютерной информации с использованием служебного положения, совершенного ФИО1, квалифицированного по ч. 3 ст. 272 УК РФ. Судебная инстанция признала полученные цифровые доказательства допустимыми и назначила наказание в виде условного лишения свободы.

Другой пример – приговор Асбестовского городского суда (Свердловская область) № 1-271/2023 1-8/2024 от 6 июня 2024 г. по делу № 1-271/2023 [5]. Из

материалов дела следует, что ФИО6 и ФИО7 совершили неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло блокирование, модификацию компьютерной информации, из корыстной заинтересованности, группой лиц по предварительному сговору.

Основное внимание было сосредоточено на офисе продаж оператора сотовой связи. Именно там была осуществлена замена SIM-карты, ставшая ключевым звеном в преступном плане.

Не менее важным стало изучение видеоматериалов. Записи с камер видеонаблюдения помогли установить маршруты передвижения подозреваемых, воссоздать хронологию событий и подтвердить их пребывание в салоне связи в конкретное время. Исследование электронных носителей информации – CD-дисков с детализацией звонков, данных переписки, мобильных телефонов и компьютеров – позволило выстроить «цифровой след». Анализ активности подозреваемых в мессенджерах, системах онлайн-платежей и социальных сетях помог получить детальное представление об их действиях. Собранные данные внесли существенный вклад в воссоздание полной картины преступления.

Дополнительным источником информации послужили результаты оперативно-разыскных мероприятий. Они также подверглись тщательному документальному осмотру. Оценка этих сведений, в комплексе с другими доказательствами, привела суд к заключению о виновности обвиняемых.

Особое внимание необходимо уделять привлечению специалиста, в качестве которого может выступать программист, инженер по средствам связи или системный аналитик. В ходе осмотра специалист оказывает содействие в обнаружении, фиксации и изъятии следов (в том числе цифровых). Роль специалиста также может заключаться в обеспечении доступа к компьютерным данным, имеющим значение для дела, которые при осмотре электронных носителей информации могут быть в зашифрованном виде. Необходимо отметить, что ввиду сложной структуры цифровых следов, данные, содержащиеся в них, могут быть получены и интерпретированы в полном объеме и без изменения содержания с использованием специальных знаний [6].

Привлечение специалистов в сфере информационных технологий представляет собой важный компонент осмотра. С учетом высокого уровня технической сложности, возникающего перед правоохранительными органами при обнаружении, извлечении и фиксации цифровых следов, участие таких экспертов помогает снизить вероятность утраты данных и увеличить точность их анализа. Это приобретает особую значимость при изучении программного обеспечения, журналов сетевой активности, криптографических методов защиты информации, инструментов удаленного доступа и иных аспектов информационной инфраструктуры преступления.

Тактика проведения следственного осмотра обязана принимать во внимание недолговечность существования цифровых следов. Данные, несущие доказательную ценность, подвержены легкому удалению, сокрытию или шифрованию, в том числе автоматическому – после заранее установленного периода времени или при отключении устройства [7]. В связи с этим. осмотр должен проводиться незамедлительно, нередко даже до официального возбуждения уголовного дела, в формате осмотра места происшествия по обнаруженным признакам преступления. Пренебрежение этим требованием увеличивает риск потери доказательств, а сами следы преступления могут быть уничтожены без возможности восстановления.

Особого рассмотрения требует процедура фиксации выполненных мероприятий. В протоколе следует с максимальной точностью указывать место обнаружения каждого изъятого предмета, его технические параметры, визуальные особенности, применяемое программное обеспечение на момент изъятия, а также прочие данные, которые могут оказаться важными для последующей экспертизы. Привлечение понятых, фото- и видеофиксация, составление описи, опечатывание носителей информации – все эти элементы обеспечивают подтверждение подлинности следственных действий.

Результаты.

В преступлениях с информационными технологиями особую роль играют именно материальные следы, ведь они имеют неординарные индивидуальные особенности. Последние могут быть присущи традиционным видам преступлений. Поэтому, проводя осмотр места происшествия, прежде чем погружаться во внутреннее содержание компьютерных устройств, следует тщательно осмотреть внешний вид предмета исследования.

В процессе работы операционной системы на ее поверхности оседает естественная и бытовая пыль (от распечатывающих устройств), которая не подлежит ежедневной уборке, накапливается в малодоступных местах (под монитором, системным блоком, клавиатурой, факсом, принтером, в местах соединения кабелей и т.п., следовательно, не исключено, что во время вероятных несанкционированных действий с компьютерными системами, преступник оставил следы [8].

Дополнительно, при осмотре электронных устройств следует учитывать аспекты, касающиеся соблюдения неприкосновенности частной жизни, тайны переписки и персональных данных. Получение доступа к зашифрованным файлам, электронной почте, облачным сервисам и мессенджерам допустимо лишь при наличии соответствующего судебного решения, либо в рамках исключений, предусмотренных уголовно-процессуальным законодательством. Так, Конституционный Суд РФ в Определении от 24 июня 2021 г. № 1364-О [9] отметил, что проведение осмотра и экспертизы с целью получения имеющей значение для

уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения.

Вместе с тем, лица, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суде в порядке, предусмотренном ст. 125 УПК РФ.

Заключение.

Таким образом, можно констатировать, что следственный осмотр по делам о преступлениях, совершенных с использованием информационно-коммуникационных технологий, является многогранным действием, которое совмещает классические тактические приемы с новыми цифровыми способами фиксации доказательств.

Данное мероприятие предполагает не просто наличие специального оборудования, но и существенную подготовку следователя, включая понимание принципов работы цифровой среды, навыки сотрудничества с профильными экспертами, а также соблюдение процессуальных норм.

Все это способствует повышению эффективности расследования и корректной юридической оценке преступных действий, имевших место в киберпространстве.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. Эксархопуло А.А. Криминалистика в схемах: учебник для вузов, 3-е изд., перераб., и доп. М., 2025. С. 366.

2. Кахрамонов А. Инструменты цифровой криминалистики // Наука, инновации и образование: ключевые векторы общественного прогресса. 2024. Т. 1. №. 1. С. 84.

3. Миронова А.В., Мандрыка Ю.С. Основания и процессуальные условия проведения осмотра места происшествия // Юристъ-Правоведъ. 2020. №. 1 (92). С. 106-110. EDN: VJLZOR

4. Приговор Заводского районного суда г. Саратова (Саратовская область) № 1-538/2024 от 21 ноября 2024 г. по делу № 1-538/2024 // https://sudact.ru/regular/doc/.

5. Приговор Асбестовского городского суда (Свердловская область) № 1-271/2023 1-8/2024 от 6 июня 2024 г. по делу № 1-271/2023 // https://sudact.ru/regular/doc/.

6. Лебедев, В. С. Чугунова К.С. Тактические особенности осмотра места происшествия при расследовании компьютерных преступлений // International & Domestic Law: Материалы XVII Ежегодной международной научной конференции по национальному и международному праву. - Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2023. - С. 1065-1071.

7. Петрова А.О., Жукова М.Н. О возможности внедрения вспомогательной методики сбора доказательств для повышения эффективности расследования киберпреступлений //Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации. 2020. С. 347. EDN: IBVNQQ

8. Поваляев, Э. А. Особенности осмотра места происшествия по преступлениям в сфере компьютерной информации // Антикриминальная политика: актуальные проблемы регионов: сборник статей по материалам всероссийской научно-практической конференции. Самара. 2024. - С. 294-305. EDN: GCIOAL

9. Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации: Определение Конституционного Суда РФ от 24 июня 2021 г. № 1364-О // ИПС "Гарант". - URL: https://www.garant.ru/products/ipo/prime/doc/401428484/.

Reference:

1. Exarchopulo A.A. Criminalistics in schemes: textbook for universities, 3rd ed., revised and supplemented by M., 2025. p. 366.

2. Kakhramonov A. Tools of digital criminalistics // Science, innovation and education: key vectors of social progress. 2024. Vol. 1. No. 1. P. 84.

3. Mironova A.V., Mandryka Yu.S. The grounds and procedural conditions for conducting an inspection of the scene // Jurist-Pravoved. 2020. No. 1 (92). pp. 106-110. EDN: VJLZOR

4. Verdict of the Zavodskoy District Court of Saratov (Saratov region) No. 1-538/2024 dated November 21, 2024 in case No. 1-538/2024 // https://sudact.ru/regular/doc /.

5. Verdict of the Asbestovsky City Court (Sverdlovsk region) no. 1-271/2023 1-8/2024 dated June 6, 2024 in case no. 1-271/2023 // https://sudact.ru/regular/doc /.

6. Lebedev, V. S. Chugunova K.S. Tactical features of incident site inspection in the investigation of computer crimes // International & Domestic Law: Proceedings of the XVII Annual International Scientific Conference on National and International Law. Yekaterinburg: Ural State Law University named after V.F. Yakovlev, 2023, pp. 1065-1071.

7. Petrova A.O., Zhukova M.N. On the possibility of introducing an auxiliary evidence collection methodology to improve the effectiveness of cybercrime investigations //Fundamental problems of information security in the context of digital transformation. 2020. P. 347. EDN: IBVNQQ

8. Povalyaev, E. A. Features of the inspection of the scene of crimes in the field of computer information // Anti-criminal policy: actual problems of the regions: a collection of articles based on the materials of the All-Russian scientific and practical conference. Samara. 2024. - pp. 294-305. EDN: GCIOAL

9. On the refusal to accept for consideration the complaint of citizen Fomin Evgeny Petrovich for violation of his constitutional rights by Articles 93, 176, 177 and part two of Article 184 of the Criminal Procedure Code of the Russian Federation: Ruling of the Constitutional Court of the Russian Federation dated June 24, 2021 No. 1364-O // IPS "Garant". - URL: https://www.garant.ru/products/ipo/prime/doc/401428484/.

Информация об авторах:
Лозовский Денис Николаевич, доктор юридических наук, профессор, профессор кафедры общетеоретических дисциплин Кубанского института социоэкономики и права (филиал Академии труда и социальных отношений), dlozovsky@mail.ru
Ульянова Ирина Рачиковна, кандидат юридических наук, доцент, заместитель начальника кафедры уголовного процесса Краснодарского университета МВД России. amfora-74@mail.ru
Denis N. Lozovsky, Doctor of Law, Professor, Professor of the Department of General Theoretical Disciplines at the Kuban Institute of Socio-Economics and Law (branch of the Academy of Labor and Social Relations).
Irina R. Ulyanova, PhD in Law, Associate Professor, Deputy Head of the Department of Criminal Procedure at the Krasnodar University of the Ministry of Internal Affairs of Russia.

Вклад авторов:
все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors:
All authors contributed equally to this article.

Статья поступила в редакцию / The article was submitted 27.11.2025;
Одобрена после рецензирования / Approved after reviewing 13.12.2025;
Принята к публикации / Accepted for publication 20.12.2025.
Авторами окончательный вариант рукописи одобрен.