

Дарья Алексеевна ГРИНЁВА,

кандидат юридических наук

Санкт-Петербургский университет МВД России (г. Калининград)

начальник кафедры оперативно-разыскной деятельности

органов внутренних дел Калининградского филиала

995095@mail.ru

Данияр Вулкайрович КАЙРГАЛИЕВ,

кандидат биологических наук, доцент

ООО «Экспертные технологии и сертификация продукции» (г. Саратов)

эксперт

danchem@mail.ru

Научная статья

УДК 343.985

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ НЕСОВЕРШЕННОЛЕТНИМИ: ОТ ТЕОРЕТИЧЕСКОЙ ОСНОВЫ К ПРАКТИЧЕСКОЙ ЗНАЧИМОСТИ

КЛЮЧЕВЫЕ СЛОВА. Цифровое преступление, несовершеннолетний цифровой преступник, жертва несовершеннолетнего цифрового преступника, типичная личность, способы подготовки преступления, способы совершения преступления, способы сокрытия преступления, время и место совершения преступления, мотивация, форма вины.

АННОТАЦИЯ. *Введение.* В статье представлены результаты исследования, цель которого заключалась в системном описании типовых признаков криминалистической характеристики цифровых преступлений, совершаемых несовершеннолетними. Актуальность темы обусловлена значительной распространенностью таких преступлений, особенностями онлайн-среды, психологией несовершеннолетних и широкой доступностью интернета. Изучение практики расследования преступлений позволило выявить важнейшую роль цифровых следов (записей входов в соцсети, данных подключений, банковских переводов) в доказывании вины преступника. Данное обстоятельство находит подтверждение в обвинительных приговорах судов. **Методы.** В основу исследования был положен диалектический метод познания. Кроме того, комплексно применялись общенаучные, специально-юридические и эмпирические методы: анализ и синтез, формально-юридический, сравнительный, статистический, документальный, метод обобщения приговоров. **Результаты.** По итогам изучения научной литературы, официальной статистики и судебной практики были определены шесть ключевых элементов криминалистической характеристики цифровых преступлений несовершеннолетних. В совокупности они представляют собой систематизированное описание типичных признаков преступной деятельности. Это обуславливает возможность, исходя из анализа цифровых следов, проводить предварительную диагностику, связывая зафиксированные в уголовном деле следы с конкретной личностью преступника, прогнозировать наличие неустановленных в ходе расследования преступления обстоятельств, планировать розыск подозреваемых, осуществлять оценку полноты расследования и подготовку к суду.

ВВЕДЕНИЕ

Криминалистическая характеристика преступления определяется как систематизированное, научно обоснованное описание типичных, криминалистически значимых признаков конкретного вида преступной деятельности, позволяющее прогнозировать неустановленные в ходе расследования преступления обстоятельства

на основе анализа типовых следов и иной информации. В контексте современных цифровых преступлений (киберпреступлений), совершаемых несовершеннолетними, данная характеристика приобретает особую актуальность, обусловленную спецификой виртуальной среды (анонимность, глобальность доступа), особенностями подростковой психологии (импульсивность, недооценка

Darya A. GRINYOVA,
Cand. Sci. (Jurisprudence)
Saint Petersburg University of the Ministry
of the Interior of Russia (Kaliningrad, Russia)
Head of the Department of Operational Investigative
Activities of Internal Affairs Bodies of the Kaliningrad Branch
995095@mail.ru

Daniyar V. KAIRGALIEV,
Cand. Sci. (Biology)
LLC «Expert technologies and product certification» (Saratov, Russia)
Expert
danchem@mail.ru

CRIMINALISTIC CHARACTERISTICS OF DIGITAL CRIMES COMMITTED BY MINORS: FROM THEORETICAL BASIS TO PRACTICAL SIGNIFICANCE

KEYWORDS. Digital crime, juvenile digital offender, victim of juvenile digital offender, typical personality, methods of crime preparation, methods of crime commission, methods of crime concealment, time and place of digital crime, motivation, type of guilt.

ANNOTATION. Introduction. This article presents the results of a study aimed at providing a systematic description of typical forensic characteristics of digital crimes committed by minors. The relevance of this topic is determined by the significant prevalence of such crimes, the specifics of the online environment, the psychology of minors, and the widespread availability of the internet. A study of crime investigation practices revealed the crucial role of digital traces (social media login records, connection data, bank transfers) in proving the guilt of the offender. This fact is confirmed by the guilty verdicts of the courts. **Methods.** The study is based on the dialectical method of cognition. In addition, general scientific, specialized legal, and empirical methods were comprehensively applied: analysis and synthesis, formal legal, comparative, statistical, documentary, and summary of verdicts. **Results.** Based on the study of scientific literature, official statistics, and judicial practice, six key elements of the forensic characteristics of digital crimes committed by minors were identified. Together, they represent a systematized description of typical features of criminal activity. This makes it possible, based on the analysis of digital traces, to conduct preliminary diagnostics, linking traces recorded in a criminal case to the specific identity of the perpetrator, to predict the presence of circumstances not established during the investigation of the crime, to plan the search for suspects, to assess the completeness of the investigation and prepare for trial.

рисков) и повсеместной доступностью технологий (смартфоны, мессенджеры, облачные сервисы). По данным МВД России, каждое двадцать девятое преступление (3,4%) в 2025 году было совершено несовершеннолетними или при их соучастии, причем каждое пятое из них являлось киберпреступлением¹, что подчеркивает необходимость адаптации криминалистической характеристики к цифровым следам.

Результаты анализа практики расследования преступлений, предусмотренных п. «Г» ч. 3 ст. 158, ст. 159.3, ст. 159.6, п. «В» ч. 3 и п. «В» ч. 5 ст. 222, п. «В» ч. 3 и п. «В» ч. 5 ст. 222.1, п. «В» ч. 3 и п. «В» ч. 5 ст. 222.2, п. «Д» ч. 2 ст. 230, п. «Г» ч. 2 ст. 242.2, ст.ст. 272, 272.1, 273, 274, 274.1, 274.2², позволяют выделить ключевые цифровые следы, которые требуют установления и фиксации: логи авторизации³ в социальных сетях и мессенджерах («ВКон-

такте», «Telegram» – 81% случаев), метаданные устройств (IP-адреса, MAC), транзакционные записи (банковские переводы), поведенческие модели (поисковые запросы, переписка в чатах). Статистика свидетельствует о росте количества направленных в суд дел по киберпреступлениям (в 2025 году их было 164038, +1,1% по сравнению с показателем 2024 года, удельный вес в общем массиве раскрытых преступлений – 91,6%), возмещение ущерба достигло 1,2 млрд рублей, что иллюстрирует востребованность знаний о цифровых следах и криминалистической характеристике в целом в расследовании киберпреступлений несовершеннолетних [1, с. 212].

Судебная практика подтверждает необходимость установления цифровых следов по каждому преступлению, совершенному с использованием (применением) информационно-телекоммуника-

¹ Состояние преступности: статистика и аналитика // МВД России: сайт // URL: <https://мвд.рф/folder/101762> (дата обращения: 30.01.2026).

² Перечень № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации // Указание Генпрокуратуры России № 503/11, МВД России № 1 от 28.07.2025 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности».

³ Лог авторизации в соцсетях (логи аккаунтов) – это файлы, которые хранят информацию о действиях пользователя на платформе.

ционных технологий или в сфере компьютерной информации. Так, в июне 2025 года Семилукский районный суд Воронежской области вынес приговор 17-летнему местному жителю, деяния которого были квалифицированы по ч. 2 ст. 272, ч. 1 ст. 159 и ч. 3 ст. 30, ч. 1 ст. 159 УК РФ. Молодой человек обвинялся в мошенничестве и неправомерном доступе к компьютерной информации посредством купленных им обезличенных SIM-карт. Их он использовал для восстановления телефонных номеров. Идентифицировать преступника помогли цифровые следы (логи операторов, банковские переводы)¹. Их фиксация в этом случае сыграла решающую роль для установления события преступления, его исполнителя и формирования доказательственной базы. Логи операторов связи зафиксировали последовательность восстановления телефонных номеров с использованием обезличенных SIM-карт. Эти записи (дата, время, IP-адреса подключений, IMEI устройств) однозначно связали совершенные действия с конкретным лицом и его техническими средствами, что опровергло возможность случайного совпадения и подтвердило умысел на несанкционированный доступ. Банковские переводы отразили движение похищенных средств, связав мошеннические операции с реквизитами, использованными злоумышленником. Метаданные транзакций (суммы, получатели, временные метки) подтвердили причинно-следственную связь между взломом и попыткой обогащения, что имело ключевое значение для квалификации преступления по ст. 159 УК РФ. Поскольку киберпреступление совершалось удаленно, без очевидцев, цифровые следы заменили традиционные показания, обеспечив реализацию принципа непосредственности исследования доказательств (ст. 274 УПК РФ) и исключив сомнения в подлоге.

В июне 2022 года Северодвинский городской суд Архангельской области вынес обвинительный приговор пятерым несовершеннолетним, осужденным по п. «г» ч. 3 ст. 158 УК РФ за хищение 35 тысяч рублей посредством банковских переводов². В данном случае в доказательственной базе по уголовному делу имелись электронно-цифровые следы нескольких видов. Транзакционные записи банковских систем (логи переводов, содержащие сведения о датах, суммах и реквизитах счетов отправителей и получателей) позволили установить неразрывную связь между финансовыми операциями и конкретными устройствами, идентифицированными по IP-адресам, принадлежащим осужденным, а также зафиксировать временные параметры их активности. Сведения, полученные от интернет-провайдеров (IP-логи домашних Wi-Fi-сетей и мобильного интернета), обеспечили возможность геолокационной привязки преступных действий к месту нахождения исполнителей

и их персонификации. Цифровые следы коммуникативного характера (сообщения в мессенджере «Telegram» и социальной сети «ВКонтакте») помогли раскрыть содержание переписки, касавшейся распределения похищенных средств и координации совместных действий, что послужило подтверждением наличия такого квалифицирующего признака, как совершение преступления группой лиц по предварительному сговору. На основе результатов анализа остаточных данных, обнаруженных на электронных устройствах (кэш браузера, сведения об удаленных учетных записях), была восстановлена полная картина механизма преступления, включая этапы сбора информации о потенциальных жертвах, получения неправомерного доступа к счетам и последующего осуществления переводов. Принципиальное значение цифровых следов в этом уголовном деле обусловлено спецификой предмета доказывания: в отсутствие традиционных материальных следов на физическом месте происшествия именно виртуальная следовая картина оказалась основным средством установления события преступления, виновности конкретных лиц и механизма хищения. Благодаря совокупности перечисленных доказательств удалось неопровержимо подтвердить причинно-следственную связь между действиями осужденных и наступившими последствиями.

Рассмотренные примеры свидетельствуют о высокой криминалистической значимости системного подхода к собиранию, фиксации и анализу цифровой информации для формирования полноценной доказательственной базы. Надлежащее процессуальное закрепление электронно-цифровых следов обеспечило возможность вынесения обвинительных приговоров, последующего возмещения имущественного ущерба и реализации превентивного потенциала уголовного судопроизводства. Всё это позволяет говорить о последовательной адаптации криминалистической науки и практики к условиям цифровой трансформации современной преступности.

МЕТОДЫ

Методологическую основу исследования, результаты которого представлены в статье, составил диалектический подход к научному познанию. Он был использован для всестороннего изучения интересующей авторов тематики. При формировании криминалистической характеристики цифровых преступлений, совершаемых подростками, мы опирались на общенаучные, специально-юридические и эмпирические методы.

В процессе исследования анализировалась официальная статистика МВД России, формально-юридический метод оказался востребован при рассмотрении норм УК РФ. Это помогло выделить ключевые признаки криминалистической характеристики цифровых преступлений несовершенно-

¹ В Семилукском районе вынесен приговор несовершеннолетнему за мошенничество и неправомерный доступ к охраняемой законом компьютерной информации // Администрация Губарёвского сельского поселения Семилукского муниципального района Воронежской области: сайт // URL: https://gubarevskoe-r20.gosweb.gosuslugi.ru/dlya-zhiteley/novosti-i-reportazhi/novosti_470.html (дата обращения: 01.02.2026).

² Уголовное дело № 1-602/2024 // Северодвинский городской суд Архангельской области: сайт // URL: https://seversud-arh.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=222648606&case_uid=4ee99dbc-8d2f-47ec-9d47-9ae7a7740a85&delo_id=1540006&new=# (дата обращения: 01.02.2026).

нолетних и составить ее шестиэлементную структуру. Главным эмпирическим инструментом стал сравнительный анализ судебной практики: изучено 58 приговоров районных и городских судов Российской Федерации, вынесенных за 2021-2025 годы, где цифровые следы играли роль ключевых доказательств. На основе этих материалов были сформулированы представления о характерных чертах несовершеннолетних преступников, их типичных мотивах и способах совершения ими киберпреступлений.

Общенаучные методы анализа и синтеза связали разрозненные данные – от умысла до обстоятельств совершения преступления, – что имеет прогностическую ценность для практики расследования преступлений рассматриваемого вида. Отсутствие в исследовании экспериментальной части компенсируется репрезентативной документальной базой, что полностью соответствует методологическим основам криминалистики как прикладной науки.

РЕЗУЛЬТАТЫ

В криминалистической доктрине устоявшейся является позиция, согласно которой структура криминалистической характеристики преступлений представляет собой совокупность взаимосвязанных типичных элементов. К числу таковых традиционно относят:

- типичные свойства личности преступника, включая социально-демографические данные (пол, возраст, уровень образования, профессиональная принадлежность), наличие криминального опыта и степень организованности преступной деятельности;
- типичные свойства личности потерпевшего, связанные с его социально-демографическим статусом (возраст, род занятий, образ жизни), а также особенностями поведения, способствующими виктимизации;
- типичные способы совершения преступления, охватывающие систему действий виновного на этапах подготовки, непосредственного совершения противоправного деяния и сокрытия его следов;
- типичные временные и пространственные характеристики (хронология преступления): время суток, дни недели, сезонность, территориальная локализация события (жилое помещение, общественное место, офис, объект транспортной инфраструктуры и пр.);
- обстановку и иные обстоятельства совершения преступления, под которыми понимается совокупность условий окружающей среды (степень многолюдности, открытость или закрытость пространства), влияющих на механизм преступления и процесс его расследования;
- типичную мотивацию, целеполагание и форму вины, раскрывающие внутреннее содержание

деяния (доминирующие мотивы – корыстные, хулиганские и пр., конкретные цели – неправомерное обогащение, самоутверждение, форма вины – прямой или косвенный умысел, неосторожность).

В научных трудах неоднократно подчеркивалось, что содержание криминалистической характеристики базируется на изучении материальных и идеальных следов преступления. Они фиксируются на месте происшествия, в документах, в поведенческих актах участников события и становятся информационной основой, отражающей содержание перечисленных выше элементов [2, с. 112]. Рассматривать специфику криминалистической характеристики цифровых преступлений, совершаемых несовершеннолетними, целесообразно с учетом изложенных теоретических положений.

1. Типичная личность несовершеннолетнего киберпреступника

Обобщение результатов изучения судебной практики позволяет выделить устойчивые социально-демографические, психологические и профессиональные признаки, образующие типичный криминалистический портрет несовершеннолетнего, совершающего преступления в цифровой сфере.

В структуре данной категории преступников доминируют лица мужского пола (в пределах от 80% до 90%), преимущественно в возрасте 16-17 лет. Для них характерно городское происхождение, принадлежность к семьям со средним уровнем дохода, что обеспечивает беспрепятственный доступ к интернету и современным цифровым устройствам. Как свидетельствуют изученные приговоры, более чем в 60% случаев преступления совершались с использованием собственных персональных компьютеров, смартфонов или планшетных устройств¹.

Образовательный статус несовершеннолетних киберпреступников, как правило, связан с обучением в общеобразовательных организациях либо в учреждениях среднего профессионального образования технической направленности (специализация в области информатики и программирования). Отличительной чертой лиц данной категории является повышенный уровень компьютерной грамотности, включая владение базовыми навыками программирования (например на языке «Python») и осведомленность о методах эксплуатации уязвимостей информационных систем (осуществление SQL-инъекций² и др.). Формирование указанных компетенций происходит в основном в ходе самостоятельной деятельности: посредством изучения специализированных онлайн-ресурсов либо в рамках участия в гейминг-сообществах (в том числе на платформах «Discord»), где проводится коллективный обмен опытом и осуществляются экспериментальные действия.

¹ Здесь и далее наши выводы основаны на результатах изучения в 2026 году 58 приговоров районных и городских судов, вынесенных за 2021-2025 годы на территории России, в которых цифровые следы рассматривались в качестве доказательств.

² Эксплуатация уязвимостей посредством SQL-инъекции – это способ манипуляции SQL-запросами, используемый для получения несанкционированного доступа к конфиденциальной информации, хранящейся в базе данных. Основной механизм – вставка вредоносного кода через поля пользовательского ввода: текстовые поля в цифровых формах, параметры URL, значения cookie. Если приложение не проверяет или не очищает пользовательский ввод перед его включением в SQL-запрос, вредоносные элементы могут изменить структуру запроса.

Психологический профиль лиц рассматриваемой категории характеризуется наличием устойчивой киберзависимости (ежедневное пребывание в виртуальной среде продолжительностью свыше шести часов), заниженной самооценкой, а также конфликтными отношениями в офлайн-среде (школьная дезадаптация, буллинг, асоциальные связи). Отсутствие либо незначительность предшествующего криминального опыта обуславливает импульсивный характер первичных преступных посягательств [3, с. 64].

Механизм индивидуального преступного поведения несовершеннолетних киберпреступников включает в себя корыстные побуждения, выражающиеся в стремлении к получению материальной выгоды для приобретения внутриигровых предметов, «скинов»¹ либо криптовалюты [4, с. 63]; статусные стремления, связанные с потребностью в самопрезентации и укреплении авторитета в виртуальной субкультуре (посредством демонстрации успешных взломов в чатах мессенджеров «Discord», «Telegram») [5, с. 138]; идеологическую основу, обусловленную влиянием деструктивных сообществ и распространением противоправного контента в социальных сетях [6, с. 101].

Результаты анализа уровня организованности преступной деятельности свидетельствуют о преобладании одиночных форм совершения преступлений, реже это происходит в составе малочисленных групп (от 3 до 5 участников), взаимодействие в которых осуществляется посредством мессенджеров и не сопровождается созданием сложных иерархических структур.

Выявленные закономерности находят подтверждение в материалах изученных нами приговоров. Так, Омским районным судом в октябре 2025 года был осужден 17-летний Д., совершивший неправомерный доступ к учетным записям пользователей портала «Госуслуги» с последующим оформлением микрозаймов². В данном случае отчетливо проявились корыстная основа криминальной деятельности (целенаправленное стремление к незаконному обогащению) и самостоятельность приобретения навыков, позволивших реализовать объективную сторону преступления без соучастников. Обнаруженные в ходе расследования цифровые следы (поисковые запросы, логи скачивания базы данных утерянных SIM-карт) помогли раскрыть механизм подготовки и совершения противоправного деяния.

Другой характерный пример обнаружен нами в материалах рассмотренного Верховным судом Республики Калмыкия уголовного дела, возбужденного по ст. 272 УК РФ. В январе 2023 года несовершеннолетний калининградец осуществил не-

правомерный доступ к аккаунту жителя Элисты в социальной сети «ВКонтакте», после чего направил знакомой потерпевшего сообщение с просьбой о переводе денежных средств в размере одной тысячи рублей³. Изучение обстоятельств преступления позволяет говорить об импульсивности осуществления деяния (отсутствие тщательной подготовки, выбор удаленной цели, незначительность ущерба) и доминировании у несовершеннолетнего желания повысить свой статус. Использование взломанного аккаунта для получения денежных средств под видом законного обращения демонстрирует стремление к социальному признанию в подростковой среде, тогда как незначительность затребованной суммы указывает на второстепенный характер корыстной составляющей по отношению к потребности в самоутверждении.

2. Типичная личность жертвы цифровых преступлений несовершеннолетних

На основе изучения судебной практики нами определены устойчивые признаки, свойственные типичной жертве цифровых преступлений, совершаемых подростками. В возрастной структуре потерпевших преобладают (более 70%) сверстники преступников – лица в возрасте от 12 до 17 лет. В 20% случаев потерпевшими оказываются родители или иные родственники самого преступника. Оставшаяся доля приходится на случайных пользователей. Это преимущественно взрослые, имеющие банковские карты, с недостаточно высоким уровнем цифровой компетентности.

Результаты виктимологического анализа свидетельствуют о том, что повышенная уязвимость потенциальных жертв киберпреступлений обусловлена следующими обстоятельствами: наивностью и недостаточной критичностью при оценке онлайн-контента (переход по фишинговым ссылкам, распространяемым через социальные сети «ВКонтакте» и мессенджер «Telegram»); неосмотрительным раскрытием учетных данных в многопользовательских онлайн-играх («Roblox», «Brawl Stars» и аналогичных); участием в мошеннических сделках на электронных торговых площадках («Avito» и др.). К числу характерных признаков типичной жертвы преступлений рассматриваемой категории относятся: активное использование социальных сетей при отсутствии двухфакторной аутентификации, высокая степень вовлеченности в игровую онлайн-среду, избыточная доверчивость при коммуникации с незнакомыми пользователями.

В рамках совершения цифровых преступлений несовершеннолетними выбор жертвы представляет собой целенаправленный процесс, сочетающий

¹ «Скины» являются символом социального статуса в геймерской субкультуре, где обладание редкими экземплярами внутриигровых предметов (например ножами стоимостью от 100 до 1000 долларов США в «Counter-Strike 2») сигнализирует об игровом успехе и привлекает внимание участников состязаний. Приобретение «скинов» осуществляется за реальные деньги (через платформу «Steam») на специализированных торговых площадках («CS.MONEY», «Skinout»), а обмен – в рамках внутриигровой экосистемы, что формирует полноценный виртуальный рынок с оборотом в миллиарды долларов США.

² Вынесен приговор Д. за 23 удачных взлома «Госуслуг» через «брошенные» телефонные номера // Коммерческие вести: сайт. 16.10.2025 // URL: <https://kvnews.ru/news-feed/200440> (дата обращения: 01.02.2026).

³ Суд назначил год исправительных работ за взлом чужого аккаунта // РАПСИ: сайт. 11.03.2024 // URL: https://rapsinews.ru/judicial_news/20240311/309688537.html (дата обращения: 01.02.2026).

использование технических методов геолокации и приемов психологического воздействия в виртуальной среде [7, с. 145]. Такой механизм позволяет повысить эффективность преступной деятельности за счет локализации целей одновременно в географическом и социальном измерениях. Это обстоятельство находит подтверждение в материалах судебной практики. На первоначальном этапе преступник устанавливает местонахождение потенциальных жертв посредством анализа IP-адресов и иных сетевых идентификаторов, доступных в открытых профилях социальных сетей и игровых платформ [8, с. 66]. Данный подход позволяет преступнику ограничить круг поиска лицами, проживающими в одном с ним регионе или населенном пункте, что упрощает реализацию психологического давления и снижает риски изобличения. Это особенно характерно для преступлений, совершаемых в условиях локальных подростковых сообществ, где территориальная общность усиливает эффект воздействия на психику [9, с. 60].

После определения жертвы преступник инициирует общение через региональные чаты или тематические группы сверстников, позиционируя себя как представителя той же социальной среды – ровесника либо обладателя схожих интересов. Формирование доверительных отношений достигается путем демонстрации общих ценностей, обсуждения тем, значимых для подростковой аудитории, и предложений о взаимовыгодном сотрудничестве [10, с. 217]. Результатом становится раскрытие жертвой конфиденциальной информации либо совершение действий, объективно способствующих реализации преступного замысла, что обусловлено эксплуатацией свойственной подросткам в условиях виртуальной общности открытости.

В криминалистическом аспекте принципиальное значение имеет то обстоятельство, что описанные действия, связанные с поиском жертвы и общением с ней, оставляют устойчивые цифровые следы в истории коммуникаций на виртуальных платформах и в данных о сетевых подключениях. Фиксация и последующий анализ таких следов создают основу для идентификации лица, совершившего преступление, и восстановления полной картины противоправного деяния.

3. Типичные способы совершения и сокрытия преступления

В структуре криминалистической характеристики преступлений рассматриваемого нами вида центральное место занимают типичные способы подготовки, совершения и сокрытия противоправных деяний. Эти элементы образуют систему взаимосвязанных действий, составляющих характерные цифровые следы и предопределяющих особенности расследования.

Подготовка несовершеннолетних к совершению киберпреступлений начинается, как правило, с создания условий для последующей реализации преступного замысла. К числу наиболее распространенных подготовительных мероприятий относятся: сбор общедоступных сведений о потенциальной жертве посредством мониторинга

профилей в социальных сетях и анализа информации, утекшей из баз данных; изучение уязвимостей учетных записей с целью определения возможных способов неправомерного доступа; создание поддельных веб-страниц, имитирующих интерфейсы легальных онлайн-сервисов (банковских учреждений, платежных систем, игровых платформ) [11, с. 42]. Перечисленные действия характеризуются относительно низкой степенью технической сложности, инструкции по их осуществлению доступны в открытых источниках, можно использовать автоматизированные инструменты, не требующие наличия глубоких знаний в сфере программирования.

Изучение эмпирического материала позволило нам выделить следующие основные способы совершения преступлений рассматриваемого вида:

- фишинг – побуждение потерпевшего к переходу по гиперссылкам, ведущим на поддельные веб-страницы, с последующим вводом конфиденциальных данных (логинов, паролей, реквизитов банковских карт); реализация данного способа предполагает использование методов социальной инженерии, адаптированных к подростковой аудитории;

- неправомерный доступ к учетным записям (аккаунтам) в социальных сетях, игровых сервисах и на порталах государственных услуг; техническая реализация требует подбора паролей, использования украденных баз данных, эксплуатации уязвимостей процедур восстановления доступа;

- мошенничество под видом торговых операций – размещение заведомо ложных объявлений о продаже товаров (цифровых товаров, игровых ценностей, аккаунтов) на электронных площадках («Avito» и аналогичных) с последующим получением предоплаты и неисполнением обязательств.

Противодействие расследованию и сокрытие следов киберпреступлений осуществляется несовершеннолетними преступниками посредством применения следующих способов:

- использование средств анонимизации сетевых подключений (VPN-сервисы, прокси-серверы, браузер «Tor»), затрудняющих идентификацию реального IP-адреса;

- удаление истории действий на используемых устройствах (очистка кэша браузеров, журналов сообщений, файлов подкачки);

- создание подставных (фейковых) учетных записей для коммуникации с жертвами и получения похищенного [12].

Вместе с тем необходимо обратить внимание на типичные ошибки, допускаемые несовершеннолетними при сокрытии следов преступления. Исходя из результатов проведенного нами анализа правоприменительной практики, к числу таковых следует отнести: использование одних и тех же идентификаторов (никнов, адресов электронной почты) в различных эпизодах преступной деятельности; раскрытие геолокационной информации через метаданные публикуемых изображений; сохранение остаточных данных в облачных хранилищах, синхронизированных с мобильными устройствами.

Криминалистически значимым обстоятельством является то, что в ряде случаев несовершеннолетние действуют не как самостоятельные субъекты преступной деятельности, а играют роль исполнителей общественно опасных деяний под руководством взрослых организаторов. Вознаграждением за совершение такого рода деяний становится доля от похищенного имущества либо заранее оговоренная выплата. Эти обстоятельства обуславливают дополнительную квалификацию по ст. 150 УК РФ (вовлечение несовершеннолетнего в совершение преступления), что должно учитываться при планировании расследования для достижения цели установления всех участников преступной деятельности.

4. Типичное время и место совершения преступления

Изучение материалов судебной практики позволило выявить устойчивые закономерности, характеризующие временные параметры и пространственную локализацию цифровых преступлений несовершеннолетних. Эти элементы криминалистической характеристики имеют существенное значение для организации расследования, построения версий и планирования оперативно-разыскных мероприятий.

Результаты анализа эмпирических данных свидетельствуют об отсутствии строгой корреляции преступной активности и какого-либо определенного времени суток. При этом очевидно, что есть выраженные пиковые периоды. Наибольшая интенсивность противоправных действий рассматриваемого вида фиксируется в ночное время – в интервале с 22:00 до 4:00, на него приходится около 70% от общего числа зарегистрированных деяний. Второй по значимости пик активности наблюдается в вечерние часы после окончания учебных занятий (с 15:00 до 20:00), что обусловлено наличием у подростков свободного времени и отсутствием родительского контроля.

Отчетливо прослеживается зависимость интенсивности преступной деятельности от календаря: значительный рост числа киберпреступлений отмечается в выходные дни, а также в периоды школьных каникул. Сезонный анализ позволяет констатировать, что максимальные показатели преступной активности приходятся на летние месяцы, что объясняется увеличением времени пребывания несовершеннолетних в цифровой среде в связи с отсутствием учебной нагрузки.

Специфичным признаком преступлений рассматриваемого вида является исключительно виртуальный характер места их совершения. Противоправные деяния осуществляются посредством использования различных цифровых устройств, чаще всего это: персональные компьютеры – в 65% случаев; смартфоны (преимущественно на платформах «Android» и «iOS») – в 55% случаев. Возможно использование для достижения криминальной цели нескольких устройств.

К числу основных площадок (виртуальных пространств), в рамках которых разворачивается преступная деятельность, относятся: социальная сеть «ВКонтакте» (фигурирует в 60% изученных приговоров); мессенджер «Telegram» (в 30% случа-

ев); платформы «Discord», многопользовательские онлайн-игры и электронные доски объявлений (в 10% случаев в совокупности).

Принципиальным для расследования обстоятельством выступает то, что при всей виртуальности места совершения преступления физическая локализация цифровых следов осуществляется через привязку к конкретным сетевым адресам. В подавляющем большинстве случаев используются IP-адреса домашних Wi-Fi-сетей либо мобильного интернет-подключения. Такая особенность, с одной стороны, обуславливает возможность идентификации абонентского устройства и его владельца, а с другой – способствует формированию доказательственной базы, приобщаемой к материалам уголовного дела в установленном законом процессуальном порядке. Наличие устойчивой связи между виртуальным действием и физическим сетевым адресом существенно облегчает процесс расследования преступления и изобличения виновных [13, с. 45].

5. Обстановка и иные обстоятельства совершения преступления

Специфика цифровой среды придает обстановке, в которой осуществляется общественно опасное деяние рассматриваемого вида, ряд специфических черт, имеющих существенное значение для понимания механизма преступления и организации его расследования.

Обстановка преступной деятельности детерминируется свойствами анонимности виртуального пространства, реализуемой посредством функционирования тематических чатов и закрытых онлайн-форумов. Анонимность выполняет криминогенную функцию, значительно ослабляя морально-психологические барьеры и создавая предпосылки для эскалации противоправного поведения. В такой ситуации актуализируется феномен группового давления, проявляющийся в форме публичных вызовов (челленджей) и провокационных действий, демонстрируемых в социальных сетях [14, с. 387; 15, с. 160].

Результаты анализа организационных форм преступной деятельности свидетельствуют о доминировании двух моделей:

- совершение преступлений в одиночку в условиях изолированного домашнего пространства, обеспечивающего конфиденциальность действий и отсутствие внешнего контроля;

- координация преступных действий в малых группах сверстников с использованием средств видеосвязи и мессенджеров, позволяющих синхронизировать усилия участников без необходимости физического присутствия в одном месте [16, с. 741].

К числу криминалистически значимых обстоятельств, объективно облегчающих реализацию несовершеннолетними преступных замыслов, относятся: недостаточный уровень защищенности учетных записей потенциальных жертв (отказ от двухфакторной аутентификации, установка простых паролей, игнорирование настроек приватности); отсутствие надлежащего родительского контроля за деятельностью несовершеннолетних в цифровой среде, в частности за использованием банковских карт и иных платежных инструмен-

тов; криминогенное влияние популярных видеоблогеров, контент-мейкеров и других авторитетных в онлайн-пространстве лиц, транслирующих в сети модели поведения, сопряженные с нарушением законодательства либо провоцирующие противоправные действия [4, с. 63].

Наряду с обстоятельствами, облегчающими деятельность криминального характера, в обстановке совершения киберпреступлений есть элементы, объективно затрудняющие реализацию умысла и повышающие риск изобличения преступников. Прежде всего это оперативное реагирование жертв преступлений, выражающееся в направлении жалоб в службы поддержки соответствующих цифровых платформ и сервисов; сохранение интернет-провайдером журналов (логов) сетевых подключений, обеспечивающее возможность последующего установления реальных IP-адресов и идентификации абонентских устройств.

Характерной чертой преступлений рассматриваемого вида является их кратковременность. Результаты анализа эмпирического материала позволяют констатировать, что продолжительность активной фазы противоправных действий, как правило, не превышает 30 минут. Такая особенность обусловлена спецификой механизма преступления: получение неправомерного доступа, совершение необходимых операций (например перевода денежных средств) и немедленный вывод похищенного на электронные кошельки либо в иные платежные системы, не требующие длительной идентификации получателя.

6. Типичные мотивация, цели и форма вины выступают необходимыми элементами криминалистической характеристики преступлений, поскольку позволяют раскрывать внутреннее содержание противоправного деяния, устанавливать механизм формирования преступного умысла и определять обстоятельства, подлежащие доказыванию в ходе расследования.

Вина в составе цифровых преступлений исследуемого нами вида представлена в форме прямого умысла: несовершеннолетний осознает общественную опасность совершаемых им действий (неправомерного доступа к компьютерной информации, модификации данных, нарушения целостности учетных записей), предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления (получения доступа к чужим денежным средствам, завладения конфиденциальной информацией, достижения иного преступного результата). Осознание противоправности деяния у несовершеннолетних, как правило, носит абстрактный характер и не сопровождается полноценным пониманием степени общественной опасности содеянного и возможных правовых последствий.

Что касается мотивов совершения преступлений рассматриваемого вида, то результаты анализа судебной практики показывают, что корыстные побуждения доминируют в 50% случаев. Они выражаются в стремлении к получению материальной выгоды (завладению денежными средствами, цифровыми активами, внутриигровыми ценностями). Хулиганские и статусные мотивы,

связанные с потребностью в самоутверждении, демонстрации превосходства, завоевании авторитета в подростковой субкультуре, отмечены в 40% случаев. Идеологические установки, обусловленные влиянием деструктивных сообществ, распространением экстремистской или иной запрещенной информации [7, с. 145], зафиксированы в 10% случаев. Выявленное распределение мотивов коррелирует с возрастными психологическими особенностями подростков, к числу которых относятся повышенная потребность в признании, склонность к рискованному поведению и подверженность групповому влиянию.

Анализ целеполагания несовершеннолетних киберпреступников позволяет констатировать краткосрочный характер преследуемых целей. Получаемая материальная выгода, как правило, ограничена незначительными суммами – от ста до пяти тысяч рублей. Данная особенность имеет принципиальное значение для квалификации деяния и понимания его причин. В связи с этим необходимо отметить, что классической корыстной мотивации, предполагающей осознанное стремление к обогащению с учетом долгосрочного эффекта, не усматривается у подростков в полной мере. Похищенные денежные средства расходуются ими импульсивно, без планирования и понимания отдаленных правовых и социальных последствий. Такое поведение объясняется комплексом факторов: это и свойственная подростковому возрасту незрелость мышления, проявляющаяся в затруднениях с прогнозированием результатов собственных действий; и восприятие киберпространства как условной, игровой среды, в которой можно игнорировать опасность наступления ответственности; и размывание границ между виртуальным экспериментированием и реальным противоправным поведением. Перечисленные особенности восприятия должны учитываться при планировании расследования, построении следственных версий, а также при решении вопросов, связанных с индивидуализацией ответственности и назначением наказания несовершеннолетним киберпреступникам.

ЗАКЛЮЧЕНИЕ

Криминалистическая характеристика цифровых преступлений, совершаемых несовершеннолетними, представляет собой систематизированное описание типичных признаков их преступной деятельности. Она позволяет на основе анализа цифровых следов проводить предварительную диагностику, связывая зафиксированные в деле следы с конкретной личностью преступника, прогнозировать наличие неустановленных обстоятельств, планировать розыск подозреваемых, осуществлять оценку полноты расследования и подготовку к суду. Роль криминалистической характеристики цифровых преступлений заключается в обеспечении методологической основы для оперативно-разыскных мероприятий и доказывания вины. Это особенно актуально в условиях распространенности киберпреступности в подростковой среде.

Изучение элементов криминалистической характеристики цифровых преступлений несовер-

шеннолетних способствует разработке мер предупреждения, включая родительский контроль и повышение цифровой грамотности потенциальных жертв. В экспертной практике криминалистическая характеристика предоставляет вспомогательную информацию для составления заключений, повышая убедительность доказательной базы в контексте виртуальности пространства, в котором

совершаются преступления и где некоторые традиционные методы сбора доказательств неприменимы. Сформированная нами криминалистическая характеристика цифровых преступлений несовершеннолетних трансформирует фрагментарные данные в целостную картину, что может способствовать повышению раскрываемости и реализации принципа неотвратимости ответственности. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Поляков А.В., Гринева Д.А. О возможностях использования информационных технологий в решении задач оперативно-розыскной деятельности // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 211-215.
2. Алексеева А.П., Анисимова Т.В. Законодательные инициативы в части усиления защиты несовершеннолетних от преступных посягательств: проблемы и перспективы // Уголовная политика и правоприменительная практика: Сборник статей по материалам международной научно-практической конференции. СПб: Астерион, 2023. С. 110-115.
3. Горковенко И.А. Отдельные аспекты противодействия преступности несовершеннолетних оперативно-розыскными мерами // Актуальные проблемы теории и практики оперативно-розыскной деятельности: Материалы Всероссийской научно-практической конференции. Краснодар: КрУ МВД России, 2025. С. 63-66.
4. Попов С.В. К вопросу о нормативно-правовом регулировании в сфере противодействия экстремизму // X Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2022. С. 63-64.
5. Желудков М.А., Алексеева А.П. Кризис семейных отношений в современном обществе как одно из условий низкой эффективности профилактики преступности несовершеннолетних // Вестник Санкт-Петербургского университета МВД России. 2023. № 2 (98). С. 131-139.
6. Попов С.В. О некоторых вопросах бифуркации дефиниции «экстремистская деятельность» в российском законодательстве // XII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2024. С. 100-102.
7. Герасимов А.В., Поляков А.В. Психологические особенности оперативно-розыскного обеспечения проведения отдельных следственных действий // VIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2020. С. 144-146.
8. Горковенко И.А. Оперативно-розыскное противодействие преступным проявлениям среди несовершеннолетних: проблемы и подходы к их решению // Криминалистика – наука без границ: традиции и новации: Материалы международной научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 66-68.
9. Герасимов А.В., Поляков А.В. К вопросу информационного воздействия на объекты оперативной заинтересованности // X Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2022. С. 60-61.
10. Попов С.В. К вопросу об особенностях обнаружения признаков мошеннических действий в сети Интернет // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 216-219.
11. Горковенко И.А. Некоторые проблемы оперативно-розыскного противодействия преступности несовершеннолетних // Актуальные вопросы теории и практики оперативно-розыскной деятельности: Сборник научных трудов межведомственной научно-практической конференции. М.: МосУ МВД России, 2024. С. 41-44.
12. Глубоковских Р.В. Розыскная работа подразделений уголовного розыска (ситуационный подход): Монография. М., 2025. 207 с.
13. Горковенко И.А. Перспективы оперативно-розыскного предупреждения преступлений, совершаемых несовершеннолетними // Оперативно-розыскная деятельность: актуальные вопросы теории и практики: Сборник научных трудов всероссийской научно-практической конференции. Ростов-на-Дону: Ростовский ЮИ МВД России, 2025. С. 41-47.
14. Попов С.В. О некоторых вопросах привлечения граждан к гласному содействию оперативными аппаратами ОВД // Актуальные проблемы права и пути их решения: Материалы международной научно-практической конференции. Донецк: Академия МВД ДНР, 2022. С. 385-388.

15. Попов С.В. Хавала на службе террористических организаций как современная угроза безопасности государства // VIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2020. С. 159-161.

16. Попов С.В. Конфиденциальное содействие: проблемы реализации и перспективы трансформации // Санкт-Петербургские встречи молодых ученых: Материалы всероссийского конгресса. СПб: СПбУ МВД России, 2024. С. 740-745.

REFERENCES

1. Polyakov A.V., Grineva D.A. O vozmozhnyakh ispol'zovaniya informatsionnykh tekhnologiy v reshenii zadach operativno-rozysknoy deyatel'nosti // Mezhdedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 211-215.

2. Alekseyeva A.P., Anisimova T.V. Zakonodatel'nyye initsiativy v chasti usileniya zashchity nesovershennoletnikh ot prestupnykh posyagatel'stv: problemy i perspektivy // Ugolovnaya politika i pravoprimeritel'naya praktika: Sbornik statey po materialam mezhdunarodnoy nauchno-prakticheskoy konferentsii. SPb: Asterion, 2023. S. 110-115.

3. Gorkovenko I.A. Otdel'nyye aspekty protivodeystviya prestupnosti nesovershennoletnikh operativno-rozysknymi merami // Aktual'nyye problemy teorii i praktiki operativno-rozysknoy deyatel'nosti: Materialy Vserossiyskoy nauchno-prakticheskoy konferentsii. Krasnodar: KrU MVD Rossii, 2025. S. 63-66.

4. Popov S.V. K voprosu o normativno-pravovom regulirovanii v sfere protivodeystviya ekstremizmu // X Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: Kf SPbU MVD Rossii, 2022. S. 63-64.

5. Zheludkov M.A., Alekseyeva A.P. Krizis semeynykh otnosheniy v sovremennom obshchestve kak odno iz usloviy nizkoy effektivnosti profilaktiki prestupnosti nesovershennoletnikh // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2023. № 2 (98). S. 131-139.

6. Popov S.V. O nekotorykh voprosakh bifurkatsii definitsii «ekstremistskaya deyatel'nost'» v rossiyskom zakonodatel'stve // XII Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: Kf SPbU MVD Rossii, 2024. S. 100-102.

7. Gerasimov A.V., Polyakov A.V. Psikhologicheskiye osobennosti operativno-rozysknogo obespecheniya provedeniya otdel'nykh sledstvennykh deystviy // VIII Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: Kf SPbU MVD Rossii, 2020. S. 144-146.

8. Gorkovenko I.A. Operativno-rozysknoye protivodeystviye prestupnym proyavleniyam sredi nesovershennoletnikh: problemy i podkhody k ikh resheniyu // Kriminalistika – nauka bez granits: traditsii i novatsii: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 66-68.

9. Gerasimov A.V., Polyakov A.V. K voprosu informatsionnogo vozdeystviya na ob'yekty operativnoy zainteressovannosti // X Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: Kf SPbU MVD Rossii, 2022. S. 60-61.

10. Popov S.V. K voprosu ob osobennostyakh obnaruzheniya priznakov moshennicheskikh deystviy v seti Internet // Mezhdedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 216-219.

11. Gorkovenko I.A. Nekotoryye problemy operativno-rozysknogo protivodeystviya prestupnosti nesovershennoletnikh // Aktual'nyye voprosy teorii i praktiki operativno-rozysknoy deyatel'nosti: Sbornik nauchnykh trudov mezhdedomstvennoy nauchno-prakticheskoy konferentsii. M.: MosU MVD Rossii, 2024. S. 41-44.

12. Glubokovskikh R.V. Rozysknaya rabota podrazdeleniy ugolovnogo rozyska (situatsionnyy podkhod): Monografiya. M., 2025. 207 s.

13. Gorkovenko I.A. Perspektivy operativno-rozysknogo preduprezhdeniya prestupleniy, sovershayemykh nesovershennoletnimi // Operativno-rozysknaya deyatel'nost': aktual'nyye voprosy teorii i praktiki: Sbornik nauchnykh trudov vserossiyskoy nauchno-prakticheskoy konferentsii. Rostov-na-Donu: Rostovskiy YuI MVD Rossii, 2025. S. 41-47.

14. Popov S.V. O nekotorykh voprosakh privlecheniya grazhdan k glasnomu sodeystviyu operativnymi apparatami OVD // Aktual'nyye problemy prava i puti ikh resheniya: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Donetsk: Akademiya MVD DNR, 2022. S. 385-388.

15. Popov S.V. Khavala na sluzhbe terroristicheskikh organizatsiy kak sovremennaya ugroza bezopasnosti gosudarstva // VIII Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: Kf SPbU MVD Rossii, 2020. S. 159-161.

16. Popov S.V. Konfidentsial'noye sodeystviye: problemy realizatsii i perspektivy transformatsii // Sankt-Peterburgskiye vstrechi molodykh uchenykh: Materialy vserossiyskogo kongressa. SPb: SPbU MVD Rossii, 2024. S. 740-745.

Авторы заявляют об отсутствии конфликта интересов.

Авторами внесён равный вклад в написание статьи.

The authors declare no conflicts of interests.

The authors have made an equal contribution to the writing of the article.

© **Гринёва Д.А., Кайргалиев Д.В., 2026.**

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Гринёва Д.А., Кайргалиев Д.В. Криминалистическая характеристика цифровых преступлений, совершаемых несовершеннолетними: от теоретической основы к практической значимости // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2026. № 1 (83). С. 71-81.