Дата поступления рукописи в редакцию: 03.03.2026 г.
Дата принятия рукописи в печать: 12.03.2026 г.
DOI: 10.24412/2782-3849-2026-2-99-103

ИЛЬИН Александр Юрьевич,
кандидат юридических наук, доцент,
доцент кафедры государственно-правовых и уголовно-правовых дисциплин
Российского экономического университета имени Г.В. Плеханова,
доцент кафедры юриспруденции,
Херсонского государственного педагогического университета,
e-mail: Aleksandr_kun@mail.ru

КИБЕРПРЕСТУПНОСТЬ КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

Аннотация. *Вопросы компьютерной криминалистики и борьбы с киберпреступлениями обусловлены острой практической востребованностью в разработке и совершенствовании криминалистических методик и средств, адекватных вызовам цифровой эпохи. Рост числа инцидентов, связанных с компьютерными атаками, мошенничеством с использованием IT-технологий, утечкой конфиденциальных данных, а также появление новых сложных угроз, таких как целевые атаки на критическую информационную инфраструктуру, требуют от следственных и экспертных подразделений постоянного повышения уровня технической и тактической подготовленности. В статье рассматривается этап становления и развития компьютерной криминалистики, и использования компьютерной криминалистики в борьбе с киберпреступностью.*

Ключевые слова: *криминалистика, криминология, киберпреступность, компьютер, научная доктрина.*

ILYIN Alexander Yuryevich,
Candidate of Law, Associate Professor,
Associate Professor of the Department
of State Law and Criminal Law Disciplines
of the Russian University of Economics named after G.V. Plekhanov,
Associate Professor of the Department of Jurisprudence,
Kherson State Pedagogical University

CYBERCRIME AS AN OBJECT OF FORENSIC RESEARCH

Annotation. *Computer forensics and cybercrime prevention are driven by a pressing practical need to develop and refine forensic methods and tools adequate to the challenges of the digital age. The growing number of incidents involving computer attacks, IT-enabled fraud, and confidential data leaks, as well as the emergence of new complex threats such as targeted attacks on critical information infrastructure, require investigative and forensic teams to continually enhance their technical and tactical preparedness. This article examines the development of computer forensics and its use in combating cybercrime.*

Key words: *forensic science, criminology, cybercrime, computer, scientific doctrine.*

Компьютерная криминалистика, также широко известная как цифровая криминалистика, и представляет собой динамично развивающуюся отрасль криминалистического знания, которая сформировалась в ответ на вызовы, порожденные глобальной информатизацией общества и стремительным ростом киберпреступности. Ее становление и развитие является закономерным следствием необходимости адаптации традиционного криминалистического инструментария к реалиям цифровой эпохи, где значительная часть преступной деятельности, а также следы такой деятельности, существуют в нематериальной, электронной форме. В данной статье постараемся раскрыть сущность данного феномена путем анализа существующих в научной среде дефиниций, определить системообразующие цели и задачи.

Современный этап развития общества, характеризуемый стремительной цифровизацией

всех сфер жизнедеятельности, наряду с неоспоримыми преимуществами породил новую, высоколатентную и динамично эволюционирующую угрозу – киберпреступность. Транснациональный характер, изощренность методов и постоянно растущий материальный и репутационный ущерб от противоправных деяний, совершаемых в информационно-телекоммуникационном пространстве, выводят проблему противодействия им в разряд первоочередных задач для национальных правоохранительных систем и международного сообщества в целом. В этих условиях ключевая роль в раскрытии и расследовании таких преступлений принадлежит компьютерной криминалистике (цифровой криминалистике), представляющей собой прикладную научную дисциплину и практическую деятельность по обнаружению, изъятию, фиксации и анализу цифровых доказательств.

Феномен киберпреступности стал одной из ключевых угроз глобальной безопасности XXI века, что обуславливает необходимость ее глубокого и всестороннего криминалистического осмысления. Как объект криминалистического исследования, киберпреступность представляет собой сложное, многогранное явление, требующее анализа не только с правовой, но и с криминалистической точки зрения, целью которой является разработка эффективных средств, приемов и способов раскрытия, расследования и предупреждения данного вида преступной деятельности. Успешное противодействие киберпреступности невозможно без теоретического обоснования, четкого понимания ее сущностных характеристик, внутренней структуры и системных свойств [6].

В современной научной доктрине отсутствует единое, универсальное определение киберпреступности, это связано с динамичным характером самого явления, транснациональностью его проявлений и различиями в национальных уголовно-правовых системах. Можно выделить два основных подхода к определению киберпреступности: узкий (уголовно-правовой) и широкий (криминологический и криминалистический). Узкий подход, характерный для многих международных документов, таких как Конвенция Совета Европы о киберпреступности (Будапештская конвенция), фокусируется на преступлениях, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, а также на использовании компьютерных систем в преступных целях. В этом контексте киберпреступность отождествляется с преступлениями в сфере компьютерной информации. Широкий подход, которого придерживается большинство отечественных криминологов и криминалистов, трактует киберпреступность более объемно [7].

Так, В.В. Крылов понимал под ней «совокупность преступлений, совершаемых с использованием компьютерной информации или против нее, а также преступлений, в которых компьютер является предметом посягательства». Этот подход позволяет включить в сферу изучения не только «чистые» компьютерные преступления (например, неправомерный доступ к информации), но и традиционные преступления, совершаемые с помощью цифровых технологий (кибермошенничество, распространение запрещенного контента и т.д.). А.М. Зинин акцентирует внимание на операционно-технологическом аспекте, определяя киберпреступность как «общественно опасную деятельность, осуществляемую в информационном пространстве с использованием специальных знаний о свойствах и особенностях функционирования компьютерных устройств, систем и сетей, направленную на достижение преступного результата». Здесь подчеркивается интеллектуальная составляющая и необходимость специальных знаний для совершения и расследования таких деяний. Синтезируя существующие точки зрения, для целей криминалистического исследования наиболее продуктивным представляется следующее определение: «Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве (информационно-телекоммуникационной среде) с использованием или в отношении информационно-коммуникационных технологий, где эти технологии выступают либо основным инструментом, либо основной целью преступного посягательства, либо критически важной средой его совершения» [8].

Важными признаками киберпреступности являются:

1) транснациональный (глобальный) характер: преступник, жертва и инфраструктура могут находиться в разных странах, что создает серьезные препятствия для юрисдикции и международного правового сотрудничества;
2) высокая латентность: многие киберпреступления остаются невыявленными в силу их технической сложности, неосведомленности жертв или нежелания сообщать о них;
3) интеллектуальность и техническая оснащенность: для совершения преступлений требуются специальные знания в области программирования, сетевых технологий и информационной безопасности;
4) дистанционность способа совершения: преступник и жертва не находятся в физическом контакте, что усложняет установление личности виновного;
5) высокая скорость совершения и динамизм: преступное деяние может быть осущест-

влено за доли секунды, а методы атак постоянно эволюционируют;

6) значительный материальный и социальный ущерб: убытки исчисляются миллиардами долларов, а подрыв доверия к цифровым системам наносит урон всей экономике и обществу [9].

Эффективная борьба с киберпреступностью требует ее систематизации. Наиболее распространенной в криминалистической практике является классификация, основанная на роли компьютера и информационных технологий в преступном деянии. В ее рамках выделяют следующие основные группы: преступления, где компьютер или информационная система является основной целью посягательства («чистые» киберпреступления), данные деяния направлены непосредственно на конфиденциальность, целостность и доступность компьютерных данных и систем. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ): взлом систем, несанкционированный доступ к данным. Создание, использование и распространение вредоносных программ (ст. 273 УК РФ): разработка вирусов, троянов. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ): действия, приведшие к уничтожению, блокированию или модификации информации [10].

Компьютер здесь, является основным инструментом совершения преступления. В эту группу входят традиционные составы преступлений, которые приобретают новые качественные характеристики за счет использования цифровых технологий. Мошенничество с использованием компьютерных технологий (ст. 159.6 УК РФ): фишинг, кардинг, мошенничества в онлайн-банкинге и на аукционах. Преступления против конституционных прав и свобод человека и гражданина: кибersталкинг, нарушение тайны переписки, распространение клеветы в сети. Преступления в сфере экономической деятельности: незаконное предпринимательство, легализация (отмывание) доходов, полученных преступным путем, с использованием электронных платежных систем и криптовалют. Преступления против общественной безопасности и общественного порядка: распространение экстремистских материалов, публичные призывы к террористической деятельности, организация деятельности запрещенных группировок через интернет. Преступления, где компьютер является вспомогательным средством или средством хранения доказательств. Сюда относятся любые преступления, в ходе которых цифровые устройства используются для планирования, связи или хранения информации о преступной деятельности (например, хранение планов ограбления на ноутбуке, переписка соучастников в мессенджере). Хотя компьютер не является ни целью, ни основным инструментом, изъятие и исследование таких устройств становится критически важным для доказывания [11].

Криминалистическая характеристика представляет собой систему обобщенных данных о групповых признаках определенной категории преступлений, имеющих значение для их раскрытия и расследования. Для киберпреступлений она включает следующие основные элементы. Способ совершения преступления - центральный, наиболее информативный элемент. Способы киберпреступлений отличаются большим разнообразием и технической сложностью, среди них можно выделить: кибер-вторжения: несанкционированный доступ через уязвимости в ПО, подбор паролей, использование вредоносного ПО. Социальная инженерия: манипулирование людьми для получения конфиденциальной информации (фишинг, претекстинг). Атаки типа «отказ в обслуживании» (DDoS): направлены на вывод из строя интернет-ресурсов путем перегрузки сетевого трафика. Криптографические атаки: взлом систем шифрования. Веб-атаки: SQL-инъекции, XSS-атаки, направленные на уязвимости веб-приложений.

Обстановка совершения преступления, это киберпространство – виртуальная среда, не имеющая физических границ. Ее элементами являются: компьютерные сети (Интернет, интранет), аппаратное обеспечение (серверы, маршрутизаторы), программное обеспечение (операционные системы, приложения), данные. Особенностью обстановки является ее изменчивость и эфемерность цифровых следов, которые могут быть легко модифицированы или уничтожены [12].

Субъект преступления (киберпреступник) характеризуется высоким уровнем интеллекта, технической грамотности, часто – специализированными знаниями в области IT. Среди киберпреступников выделяют: одиночек («хакеров-одиночек»), организованные преступные группы с четким разделением ролей (программист, аналитик, «дроп»), и даже киберподразделения, спонсируемые государствами. Мотивация может быть различной: корыстная, идеологическая (хактивизм), стремление к самоутверждению, шпионаж.

Предмет преступного посягательства и механизм следообразования. Предметом посягательства являются компьютерная информация, информационные ресурсы, системы и сети, а также материальные и нематериальные блага, на которые осуществляется воздействие через IT (деньги, репутация, авторские права). Механизм следообразования в киберпространстве сложен и многоуровнев. Личность потерпевшего. Потерпевшими могут быть как физические лица, так и юридические лица (банки, корпорации, государственные учреждения), а в случае с DDoS-ата-

ками или распространением вредоносного ПО – и общество в целом. Часто потерпевшие не сразу обнаруживают факт совершения против них преступления [13].

Таким образом, проведённый анализ киберпреступности как объекта криминалистического исследования позволяет сформулировать комплексный вывод, раскрывающий её сущность, структуру и значение для разработки эффективных средств противодействия. Киберпреступность предстает не просто как совокупность отдельных противоправных деяний, а как сложное системное явление, порождённое глобальной цифровизацией и обладающее качественно новыми характеристиками, которые коренным образом отличают её от традиционных форм преступности. Её определение, синтезированное на основе широкого подхода, охватывает преступления, совершаемые в киберпространстве с использованием или в отношении информационно-коммуникационных технологий, где эти технологии выступают либо основным инструментом, либо основной целью, либо критически важной средой преступного посягательства. Такой подход позволяет включить в сферу криминалистического изучения не только «чистые» компьютерные преступления, но и модифицированные цифровыми средствами традиционные составы, что отражает реальную картину современной преступной деятельности. Ключевые признаки киберпреступности – транснациональность, высокая латентность, интеллектуальность и техническая оснащённость субъекта, дистанционность и скорость совершения, а также значительный материальный и социальный ущерб – формируют уникальный и крайне сложный для противодействия феномен. Эти признаки обусловливают необходимость разработки специализированных криминалистических методик, выходящих за рамки классических схем расследования. Ядром криминалистического осмысления киберпреступности стала её развёрнутая характеристика, представляющая собой систему взаимосвязанных элементов, знание которых является фундаментом для построения эффективной тактики расследования. Центральное место здесь занимает способ совершения преступления, отличающийся невероятным разнообразием и постоянной эволюцией – от технических взломов и внедрения вредоносного кода до изощрённых методов социальной инженерии. Понимание конкретного способа позволяет выдвигать обоснованные версии о личности преступника и определять направления поиска цифровых следов. Не менее важна характеристика обстановки – киберпространства, виртуальной, динамичной и безграничной среды, где материальные следы заменяются электронными артефактами, легко изменяемыми и уничтожаемыми. Эта особенность предъявляет исключительные требования к оперативности и технической корректности действий на начальном этапе расследования. Субъект преступления (киберпреступник) характеризуется высоким уровнем специальных знаний, что превращает противостояние с ним в интеллектуальное противоборство, а зачастую и в технологическую гонку. Мотивация таких субъектов может варьироваться от корысти до идеологии, что также влияет на выбор ими методов и цели атаки. Механизм следообразования в киберпространстве отличается многоуровневостью и сложностью, следы могут одновременно фиксироваться на атакуемом компьютере, промежуточных серверах, сетевом оборудовании и устройствах злоумышленника, создавая комплексную, но часто фрагментарную картину события. Личность потерпевшего (будь то частное лицо, корпорация или государственный орган) и характер причинённого ущерба определяют общественную опасность деяния и приоритетность расследования.

Таким образом, киберпреступность как объект криминалистического исследования представляет собой многомерную, динамичную и высокотехнологичную систему. Её успешное раскрытие и расследование невозможны без глубокого понимания присущих ей специфических признаков, чёткой классификации видов и, что наиболее важно, всестороннего анализа криминалистической характеристики. Полученные данные о способе, обстановке, субъекте и механизме следообразования служат основой для разработки специализированных тактических приёмов проведения следственных действий (особенно осмотра и изъятия электронных носителей), формирования частных методик расследования отдельных видов киберпреступлений и создания эффективной системы профилактики. Следовательно, сделанные выводы, закладывают необходимый теоретический фундамент для последующего анализа практических проблем, подчеркивая, что противодействие киберпреступности должно строиться на адекватном научном понимании её природы и постоянной адаптации криминалистического инструментария к меняющимся технологическим реалиям цифрового мира и развитии компьютерной криминалистики.

Список литературы:

[1] Аверьянова Т. В. Криминалистика. М.: Норма, 2023. 928 с.

[2] Аспект компьютерной криминалистики / А. Э. Федосеев, С. Б. Гладкова, И. С. Назаренко, А. В. Борисенко // Право и государство: теория и практика. – 2024. – № 12(240). – С. 726-729.

[3] Бастрыкин, А.И. Цифровые технологии современной криминалистики // Вестник Москов-

ской академии Следственного комитета Российской Федерации. -2021. - № 2, - С. 11-17.

[4] Быстрицкая, К. А. Использование методов компьютерной криминалистики в ходе проверок кредитной организации / К. А. Быстрицкая, И. В. Костенко // Научный аспект. – 2024. – Т. 41, № 6. – С. 5179-5183.

[5] Волынский А.Ф. Научно-техническое обеспечение судопроизводства: привычные проблемы и программно-целевой подход к их решению // Известия Тульского государственного университета. Экономические и юридические науки. 2023. № 2. С. 3-12.

[6] Ильин Н.Н. Транспортные экспертизы в уголовном судопроизводстве России: монография. Москва: ИНФРА-М, 2025. 379 с.

[7] Карагодин, В. Н. Современный этап эволюции российской криминалистики: оценки, траектории, качество / В. Н. Карагодин // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – № 1(35). – С. 118-126.

[8] Козлов А. Е., Макарова Е. Н., Романова О. Л. Современные технико-криминалистические средства, применяемые в ходе осмотра места происшествия. Санкт-Петербург: СПбУ МВД России, 2024. 64 с.

[9] Комплексный анализ состояния преступности в Российской Федерации и ожидаемые тенденции ее развития: аналитический обзор / М. В. Гончарова, М. М. Бабаев, Р. В. Черкасов и др. Москва: ФГКУ «ВНИИ МВД России», 2024. 87 с.

[10] Компьютерная криминалистика. Анализ механизмов сбора информации в Windows-системах / С. В. Артемова, А. А. Бакаев, Ж. Г. Вегера [и др.] // Защита информации. Инсайд. – 2024. – № 6(120). – С. 45-49.

[11] Кучин О.С. К вопросу о дефиниции «цифровая криминалистика» // Современные технологии и подходы в юридической науке и образовании: Сборник 157 материалов международного научно - практического форума, Калининград, 2021. С. 195-200.

[12] Лозинский, О. И. Компьютерная (цифровая) криминалистика (форензика) в эпоху цифровой трансформации экосистемы уголовного процесса / О. И. Лозинский // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2023. – № 12(163). – С. 115-120.

[13] Островский, О. А. Киберкриминалистика в цифровую эпоху: вызовы и перспективы развития / О. А. Островский // Юридическая гносеология. – 2024. – № 5. – С. 106-114.

References:

[1] T. Averyanova. Forensics. M.: Norma, 2023. 928 pp.

[2] Aspect of computer forensics/A. E. Fedoseev, S. B. Gladkova, I. S. Nazarenko, A. V. Borisenko// Law and State: Theory and Practice. – 2024. – № 12(240). - S. 726-729.

[3] Bastrykin, A.I. Digital technologies of modern forensics//Bulletin of the Moscow Academy of the Investigative Committee of the Russian Federation. -2021. - NO. 2, - S. 11-17.

[4] Bystritskaya, K. A. The use of computer forensics methods during inspections of a credit institution/K. A. Bystritskaya, I. V. Kostenko//Scientific aspect. – 2024. - T. 41, NO. 6. - S. 5179-5183.

[5] Volynsky A.F. Scientific and technical support of legal proceedings: familiar problems and a software-targeted approach to solving them//Izvestia of Tula State University. Economic and legal sciences. 2023. № 2. S. 3-12.

[6] Ilyin N.N. Transport expertise in criminal proceedings of Russia: monograph. Moscow: INFRA-M, 2025. 379 pp.

[7] Karagodin, V. N. The modern stage of the evolution of Russian forensics: assessments, trajectories, quality/V. N. Karagodin//Siberian criminal procedural and forensic readings. – 2022. – № 1(35). - S. 118-126.

[8] Kozlov A.E., Makarova E.N., Romanova O.L. Modern technical and forensic means used during the inspection of the scene. St. Petersburg: St. Petersburg Ministry of Internal Affairs of Russia, 2024. 64 pp.

[9] A comprehensive analysis of the state of crime in the Russian Federation and the expected trends in its development: an analytical review/M.V. Goncharova, M.M. Babaev, R.V. Cherkasov and others. Moscow: FGKU “All-Russian Research Institute of the Ministry of Internal Affairs of Russia,” 2024. 87 pp.

[10] Computer forensics. Analysis of information collection mechanisms in Windows systems/S. V. Artemova, A. A. Bakaev, J. G. Weger [et al.]//Information protection. Inside. – 2024. – № 6(120). - S. 45-49.

[11] Kuchin O.S. On the definition of “digital forensics “//Modern technologies and approaches in legal science and education: Collection of 157 materials of the international scientific and practical forum, Kaliningrad, 2021. S. 195-200.

[12] Lozinsky, O. I. Computer (digital) forensics (forensics) in the era of digital transformation of the ecosystem of criminal proceedings/O. I. Lozinsky// Science and education: economy and economics; entrepreneurship; law and governance. – 2023. – № 12(163). - S. 115-120.

[13] Ostrovsky, O. A. Cybercriminalism in the digital age: challenges and development prospects/O. A. Ostrovsky//Legal epistemology. – 2024. – № 5. - S. 106-114.