Научная статья
УДК 343.98
DOI 10.33184/pravgos-2025.2.11

Original article

ХАРИСОВА Зарина Ирековна
Уфимский университет науки и технологий,
Уфа, Россия,
e-mail: zarinaid@mail.ru,
https://orcid.org/0000-0002-3902-3459

KHARISOVA Zarina Irekovna
Ufa University of Science and Technology,
Ufa, Russia.

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

CRIMINALISTIC CHARACTERISTICS OF CRIMES RELATED TO ILLEGAL ACCESS TO COMPUTER INFORMATION

Аннотация. *В статье показана необходимость рассмотрения направлений повышения эффективности расследования преступлений, связанных с неправомерным доступом к компьютерной информации, что обусловлено их широкой на сегодняшний день распространенностью. Прикладное значение исследования заключается в возможности формирования на основе криминалистической характеристики указанного вида преступлений частных криминалистических методик расследования таких преступлений, создания криминалистических учетов цифровых доказательств, разработки специализированного программного обеспечения в виде систем поддержки принятия решений, применяемых при выдвижении следственных версий. Цель исследования: описание элементов криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации, с учетом современного развития информационных технологий. В процессе исследования использовалась совокупность общих (описания, обобщения и сравнения), общенаучных (анализа, синтеза, моделирования и классификации) и частнонаучных (статистический, кибернетический) методов познания. Результаты: описаны элементы криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации, которые могут выступить основой для формирования информационной модели (цифрового двойника) преступления.*

Abstract. *The article shows the need to consider the directions of improving the effectiveness of investigation of crimes related to illegal access to computer information, which is due to their widespread today. The applied significance of the study lies in the possibility of forming on the basis of the criminalistic characteristic of this type of crime private criminalistic methods of investigation of such crimes, creating criminalistic records of digital evidence and developing specialized software in the form of decision support systems used in putting forward investigative versions. The purpose of the research is to describe the elements of the criminalistic characteristics of crimes related to illegal access to computer information, taking into account the modern development of information technology. Research methods: in the course of the study, a set of general (description, generalization and comparison), general scientific (analysis, synthesis, modeling and classification), specific scientific (statistical, cybernetic) methods of cognition is used. Research results: the article describes the elements of the criminalistic characteristics of crimes related to illegal access to computer information, which can be the basis for the formation of an information model (digital twin) of the crime.*

Ключевые слова: *преступления в сфере компьютерной информации, киберпреступность, неправомерный доступ к информации, криминалистическая характеристика преступлений, цифровая модель преступления, цифровые двойники, алгоритмы расследования, оптимизация расследования, компьютерная криминалистика, искусственный интеллект*

Keywords: *computer information crimes, cybercrime, illegal access to information, criminalistic characteristics of crimes, digital model of crime, digital twins, investigation algorithms, investigation optimization, digital criminalistics, artificial intelligence*

Для цитирования: Харисова З.И. Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации / З.И. Харисова. – DOI 10.33184/pravgos-2025.2.11 // Правовое государство: теория и практика. – 2025. – № 2. – С. 96–105.

For citation: Kharisova Z.I. Criminalistic Characteristics of Crimes Related to Illegal Access to Computer Information. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2025, no. 2, pp. 96–105. (In Russian). DOI 10.33184/pravgos-2025.2.11.

Введение

Преступления в сфере компьютерной информации – это обозначение преступных деяний, предусмотренных гл. 28 УК РФ, объединяющей ст. 272, 272.1, 273, 274, 274.1, 274.2. Стоит отметить, что в настоящее время существенно увеличилось количество преступлений, связанных с утечкой конфиденциальных данных, способных нанести ущерб объектам критической информационной инфраструктуры Российской Федерации (ст. 274.1); хищением персональных данных граждан, их неправомерным использованием и распространением (ст. 272.1) [1, с. 156]; противоправным применением информационно-телекоммуникационных технологий организованными преступными группами, которые все чаще используют вредоносное программное обеспечение (ст. 273); нарушением правил эксплуатации средств хранения, обработки и передачи компьютерной информации (ст. 274), централизованного управления средствами противодействия угрозам устойчивости и безопасности функционирования сети Интернет (ст. 274.2). Отдельно следует отметить неправомерный доступ к охраняемой законом информации (ст. 272), который составляет 99,56 % от общего числа зарегистрированных в 2024 г. преступлений в сфере компьютерной информации[1]. В связи с этим особенно важно рассмотреть возможности оптимизации процесса расследования именно преступлений, связанных с несанкционированным доступом к информации, в частности изучить элементы, входящие в их криминалистическую характеристику.

Под доступом к компьютерной информации понимается возможность ознакомиться с ней либо в дальнейшем ею воспользоваться[2] в результате применения тех или иных средств и способов, что определяет наступление одного или нескольких последствий:

– уничтожение информации (в виде приведения ее (или ее части) в непригодное для использования по назначению состояние вне зависимости от возможности дальнейшего ее восстановления);

– блокирование информации (в виде создания условий, препятствующих в течение некоторого времени или постоянно доступу к компьютерной информации субъекта, имеющему право на него, а также ограничения или прекращения доступа к персональным компьютерам, системам и находящимся в них информационным ресурсам);

– модификация информации (в виде любых изменений компьютерной информации, в том числе внесение изменений в программное обеспечение, базы данных и информационные ресурсы, размещаемые на электронных носителях информации);

1 Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития : аналитический обзор / М.В. Гончарова, М.М. Бабаев, Р.В. Черкасов и др. М. : ФГКУ «ВНИИ МВД России», 2025. С. 28.

2 Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

– копирование информации (в виде неправомерного дублирования информации на другой носитель и воспроизведения ее в любой форме).

Соответственно, неправомерным признается доступ к информации лица, которое на момент доступа не обладало соответствующими правами на работу с данной информацией, персональным компьютером или информационной системой, равно как и не имело прав на использование средств и способов для ознакомления с информацией, в отношении которой приняты специальные меры защиты[3].

Элементы криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации

Все преступления в сфере компьютерной информации имеют общую родовую криминалистическую характеристику [2, с. 585], которая включает в себя сведения о способах совершения преступлений, лицах, их совершивших, о потерпевшей стороне и обстоятельствах, способствующих и препятствующих совершению данных преступлений. Между тем лишь перечисление элементов такой системы не может в полной мере определять ее сути, требующей выявления взаимосвязей между ее составляющими. Поэтому актуальной задачей является проведение содержательного анализа элементов криминалистической характеристики преступлений, связанных с неправомерным доступом к компьютерной информации, с точки зрения системно-структурного, а также кибернетического подходов. Результаты анализа могут послужить основой для формирования информационной модели преступления в сфере компьютерной информации на основе наиболее значимых элементов сформированной криминалистической характеристики.

Анализ уголовных дел по фактам совершения рассматриваемых преступлений позволил выделить соответствующие текущему уровню состояния преступности в сфере компьютерной информации элементы их криминалистической характеристики:

– способ совершения преступления (с описанием типичных следов преступления, способов их сокрытия, вероятных мест их нахождения и распространенности (серийности) преступного деяния);

– обстановка (место (среда), время) совершения преступления;

– личность преступника;

– личность потерпевшего и (или) предмет посягательства.

Включение в «способ совершения преступления» в сфере компьютерной информации такого элемента, как «распространенность (серийность) преступного деяния», целесообразно, поскольку подтверждается на практике необходимостью проверки схожести (серийности) эпизода с ранее выявленными преступными деяниями и обязательным включением сведений о способе и иных обстоятельствах совершения преступления в подсистемы программно-технического комплекса интегрированного банка данных федерального уровня (ИБД-Ф) ГИАЦ МВД России. Кроме того, серийность преступного деяния – один из обязательных реквизитов[4] для указания в статистической карточке преступления, содержание которого может выступить основой для формирования нового криминалистического учета цифровых доказательств [3, с. 96], что сонаправлено с одной из основных задач государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий[5].

Способ совершения преступления

Среди основных преднамеренных способов осуществления неправомерного доступа к компьютерной информации можно отметить преодоление систем защиты в виде хи-

3 Комментарий к Уголовному кодексу РФ : в 4 т. Т. 3. Особенная часть. Раздел IX / В.М. Лебедев и др. ; отв. ред. В.М. Лебедев. М. : Юрайт, 2024. С. 286.

4 О едином учете преступлений : приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 // Доступ из справ.-правовой системы «КонсультантПлюс».

5 О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 25.03.2025 № 41-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс».

щения учетных данных пользователей; использование несовершенств систем защиты информации; выявление уязвимостей программного обеспечения (эксплойтов (от англ. exploit – эксплуатировать)) и операционных систем; несанкционированное подключение к техническим средствам и информационным системам, а также вспомогательному компьютерному оборудованию – внешним запоминающим устройствам и пр., в том числе удаленно или в случае системной поломки; фишинг (создание поддельных ресурсов или сообщений для несанкционированного получения данных) и т. п.

Процессы, возникшие в ходе случайных действий либо стечения обстоятельств, относят к непреднамеренным. Это может быть, например, доступ к учетной записи иного пользователя из-за автосохранения пароля в браузере; работа на ПЭВМ, доступ к которой имеется у нескольких пользователей (в офисе, коворкинге), с сохранением личных данных в системе. К программным способам можно отнести неправомерный доступ к компьютерной информации, осуществленный с использованием специализированного программного обеспечения. Доступ к информации с использованием непрограммных способов осуществляется посредством специальных технических средств, но не предполагает использование дополнительных приложений (например, установку аппаратных устройств, записывающих нажатия клавиш (кейлоггинг), и т. п.). В целом все способы неправомерного доступа к компьютерной информации можно подразделить на непосредственный, удаленный и гибридный. В большинстве случаев при совершении указанных преступлений применяются комбинации перечисленных способов, функционирующих по различным алгоритмам [4, с. 100].

Анализ уголовных дел позволил выявить основные средства совершения неправомерного доступа к компьютерной информации. При непосредственном доступе ими могут выступать носители информации, эксплуатируемые с техническими средствами, а при опосредованном – сетевое оборудование и средства доступа в информационные системы (средства вычислительной техники, мобильные средства связи и пр.). К основным средствам также относится различное программное обеспечение (например, VPN-сервисы (Virtual Private Network – виртуальная частная сеть), обеспечивающие шифрование трафика и сокрытие реального IP-адреса преступника, системы прокси-серверов, построенные на базе многослойного шифрования данных, и пр.), в том числе вредоносное, предназначенное для распространения в локальных информационных системах в целях выполнения какого-либо деструктивного действия (удаление, блокирование или изменение файлов), а также программное обеспечение, предназначенное для проведения тестов на проникновение, и пр.

Основными способами сокрытия следов неправомерного доступа к компьютерной информации являются: очищение журналов и шифрование событий в системе; удаление сведений о подключениях к ПЭВМ или информационным системам; использование программных средств анонимизации в целях подмены IP-адресов устройств (VPN-сервисы и системы прокси-серверов); несанкционированное подключение к беспроводным точкам доступа; использование беспроводных модемов с SIM-картами, оформленными на подставных лиц, с целью анонимизации абонентских номеров, а также VoIP-технологий (от англ. Voice Over Internet Protocol – протокол, обеспечивающий передачу речевого сигнала по сети Интернет или другим IP-сетям) и виртуальных (облачных) автоматических телефонных станций; использование мессенджеров, обеспечивающих усиленное шифрование данных, и пр.

Типичными следами неправомерного доступа к компьютерной информации в общем случае являются: цифровые (установленное программное обеспечение, используемое для несанкционированного доступа, изменения в конфигурации операционной системы устройства, журналы подключений к ПЭВМ или информационным системам, модифицированные или блокированные файлы данных и т. п.) и материальные следы на компьютерной периферии.

Основными следообразующими и следовоспринимающими объектами преступлений рассматриваемого вида могут выступать: системное и прикладное программное обеспечение; поименованные области записей на носителях информации; электронные файлы;

базы данных; электронные ключи (подписи); идентификаторы в сети передачи данных (например, IP-адрес устройства или MAC-адрес его сетевой карты), IMEI-коды мобильных средств связи, DNS-адреса; реестры операционных систем; файлы подкачки и временные файлы; сетевой трафик; цифровые финансовые активы и электронные кошельки; IMS-, SMS- и MMS-сообщения.

Отдельно стоит отметить факторы, связанные с развитием генеративного искусственного интеллекта, метавселенных и квантовых алгоритмов, которые порождают относительно новые виды преступных деяний, связанных с неправомерным доступом к компьютерной информации (подмена данных, кража виртуальной собственности, идентификаторов личности, взлом ключей шифрования, перехват данных и т. п.). По рассматриваемым преступным деяниям следовоспринимающими и следообразующими объектами будут, например, сфальсифицированный мультимедиаконтент [5, с. 2], метаданные [6, с. 416] и конфигурации серверов, формирующие метапространство (журналы функционирования программного обеспечения, обеспечивающего визуализацию трехмерных виртуальных пространств и работу децентрализованных сетей [7, с. 2], конфигурационные файлы с настройками дополненной (AR), виртуальной (VR) и расширенной (XR) реальностей, сетевые адреса взаимодействия цифровых аватаров и пр.), или конфигурации квантовых компьютеров (реестры эксплуатации квантовых приложений и дампов квантовых состояний, протоколы квантовых связей [8, с. 80] и пр.). Вероятными местами расположения типичных следов неправомерного доступа к компьютерной информации в цифровом виде являются носители информации, серверное оборудование и облачные хранилища, в том числе файлы и каталоги хранения данных, файлы конфигурации программ удаленного доступа и пр.

Распространенность преступного деяния выражается в установлении факта схожести эпизода на основе полученных сведений об использовании в преступной схеме способа совершения преступления. Так, например, идентифицирующими признаками схожести могут выступать идентичные реквизиты в виде MAC- или IP-адресов устройств, абонентских номеров, программируемых ботов, используемых для совершения массовых атак, IMEI-кодов задействованных мобильных средств связи, электронных адресов, банковских реквизитов и т. п.

Несмотря на имеющиеся проблемы реализации основных принципов теории криминалистической идентификации [9, с. 80] по установлению связи между двумя объектами (идентифицируемым и идентифицирующим) посредством определения их идентичности или отсутствия таковой в процессе расследования преступного деяния [10, с. 236], а также на сложности идентификации материальных процессов, явлений, состояний материальных объектов и их комплексов в соответствии с кибернетической теорией распознавания образов [11, с. 71] и теорией криминалистической диагностики, введение категории «распространенность преступного деяния» в элемент криминалистической характеристики «способ совершения преступления» в свете построения цифровых криминалистических моделей [12, с. 60] представляется актуальным. Ввиду тесной взаимосвязи с цифровыми идентифицирующими признаками преступных деяний рассматриваемого вида это позволит наиболее просто осуществить выявление задействованных в преступлении объектов либо диагностику протекающих информационных процессов, например, путем использования методов интеллектуального анализа и распознавания данных [13, с. 8]. Предлагаемый подход соответствует одному из главных направлений совершенствования криминалистического обеспечения, который заключается в интеграции в процесс расследования алгоритмов искусственного интеллекта и машинного обучения [14, с. 123].

Обстановка совершения преступления

Обстановка совершения неправомерного доступа к компьютерной информации предполагает как непосредственный доступ к объекту посягательства (преимущественно в момент отсутствия обладателя защищаемой информации), так и удаленный из любой точки мира (при наличии подключения к сети Интернет или к локальной сети предприятия) и определяется спецификой работы

с данными в электронном виде, использованием программно-аппаратных средств для их обработки, хранения и передачи.

Местами совершения рассматриваемых преступлений являются как конкретные ПЭВМ, серверы или информационные системы (зачастую значительно удаленные друг от друга), так и локальные территории, учреждения и организации, в которых эксплуатируется объект преступления. В целях сокрытия физического расположения преступника удаленный доступ нередко осуществляется из общественных мест, предоставляющих сеть Интернет в порядке пользования услугами на базе организации. В подавляющем большинстве случаев местом (средой) совершения неправомерного доступа к компьютерной информации является киберпространство ввиду его распространенности среди населения, реже – метапространство, блокчейн (распределенные реестры) либо гибридные инфраструктуры (распределенные облачные системы хранения данных и пр.). Таким образом, местом совершения рассматриваемого вида преступлений является, как правило, место реализации преступного умысла в интернет-пространстве – место, где фактически располагалось компьютерное оборудование, посредством которого реализован преступный план.

Согласно ч. 2 ст. 9 УК РФ временем совершения преступления признается время окончания преступного деяния, вне зависимости от момента наступления последствий. Время совершения рассматриваемых преступлений не всегда устанавливается точно, поскольку при их совершении часто задействуются различные ПЭВМ, программное обеспечение, информационные системы и т. д., реестры функционирования которых бывает довольно сложно сопоставить. Кроме того, работа указанных средств связана с временем, установленным в их системе, которое может быть легко изменено преступником в целях искажения типичных следов.

Таким образом, анализ обстановки совершения преступления, представленной в качестве самостоятельного элемента криминалистической характеристики, позволяет следователю получить информацию об обстоятельствах и условиях, предшествовавших преступлению, о том, что в обстановке способствовало или препятствовало его совершению, каким образом обстановка повлияла на выбор способов, орудий и средств совершения преступления, а также о личности потерпевшего и др. [15, с. 35].

Личность преступника

Сведения о преступнике, сопоставленные с данными о способе и обстановке совершения преступления, позволяют сформировать новые сведения, способствующие его поиску и изобличению [16, с. 32]. Как правило, лицо, осуществляющее неправомерный доступ к компьютерной информации, имеет высшее или среднее инженерно-техническое либо экономическое образование, обладает устойчивыми преступными навыками. Совершаемые преступления часто носят серийный, многоэпизодный характер и сопровождаются тщательными действиями по сокрытию следов преступной деятельности.

Все чаще рассматриваемые деяния совершают несовершеннолетние, действующие по заранее определенным алгоритмам, диктуемым преимущественно взрослыми, что способствует активному вовлечению этой категории лиц в преступную деятельность [17, с. 57].

Одной из особенностей личности преступника, совершающего преступление в сфере компьютерной информации в целом, является его возраст – от 16 до 45 лет [18, с. 77], около 90 % лиц, совершивших указанные деяния, мужского пола [19, с. 75]. Вместе с тем деление преступников на возрастные категории весьма условно [20, с. 44].

Как правило, преступник грамотно владеет комплексом манипулятивных приемов и техник воздействия на жертву с целью неправомерного доступа к конфиденциальной информации, методами социальной инженерии, а также совокупностью знаний в области социологии и психологии, которые позволяют управлять поведением людей, играя на их эмоциях, чувствах, страхах и рефлексах, прогнозируя их возможное поведение исходя из складывающейся обстановки. Анализ уголовных дел показывает, что преступники часто используют принцип доверия, построенного на знании, тщательно готовятся к атаке конкретного лица, собирая о нем информацию

из открытых источников, персонализируя ее под предмет неправомерного доступа.

Основными мотивами совершения неправомерного доступа к компьютерной информации выступают корыстные побуждения (получение материальной выгоды), личная неприязнь к собственнику информации, вымогательство или мошенничество, хулиганство, вандализм (разрушение информационных систем, атаки на технические средства и пр.), шпионаж (получение сведений экономической направленности, о личной жизни и пр.).

Личность потерпевшего и (или) предмет посягательства

Предметом неправомерного доступа к компьютерной информации являются охраняемые законом сведения, под которыми понимаются данные о лицах, предметах, фактах, событиях, явлениях и процессах, находящиеся на машинном носителе информации, в ЭВМ, системе ЭВМ или их сети[6] в форме электрических сигналов. Нематериальный характер компьютерной информации не может выступать веским аргументом в пользу отрицания возможности ее рассмотрения в качестве предмета неправомерного доступа по смыслу ст. 272 УК РФ [21, с. 184].

Личность потерпевшего можно связать с владельцем технического средства или информационной системы, в которые осуществлен неправомерный доступ. Потерпевших по рассматриваемым преступлениям можно также разделить на категории по принадлежности к физическим или юридическим лицам, к государственным структурам.

Исходя из анализа сложившейся за последние несколько лет следственной и судебной практики можно выделить отличительные особенности личности потерпевшего. Как правило, основными чувствами и эмоциями, которые испытывают потенциальные жертвы, являются любопытство, жадность, жалость или страх, способные отключить объективное восприятие действительности, критическое мышление и логику. Дополняет перечисленное такой фактор, как безотлагательность действий, диктуемых преступником, что усиливает манипуляционный эффект. В протоколах допроса потерпевших часто фигурируют фразы: «все было как в тумане», «сам(-а) не понял(-а), как все произошло», «сделал(-а) все на автомате» и пр. Таким образом, в ряде случаев осуществляется вовлечение потерпевшего в совершение преступления с применением психологических манипуляций с целью, например, получения уникального кода для осуществления несанкционированного доступа к ресурсу или склонения жертвы к самостоятельной загрузке программного обеспечения, позволяющего удаленно управлять ее устройством.

Характерной особенностью потерпевшей стороны является бездействие или неохотное желание сообщать о преступлении в правоохранительные органы, что обусловлено безосновательным предположением о низкой вероятности раскрытия преступления. Потерпевшие часто не могут предоставить минимально необходимые данные и доказательства для создания полноценной картины расследования (параметры входа в сеть, учетные данные и пр.) [22, с. 95], что является следствием пока еще низкого уровня просвещенности населения в области информационно-телекоммуникационных технологий. Часто потерпевший использует условно бесплатное программное обеспечение или приложения, в которых настроен обход контроля лицензий, что позволяет внедрить в устройство пользователя дополнительный функционал для несанкционированного доступа к информации.

Стоит также отметить, что исследование уголовных дел показало массовость и идентичность совершаемых преступлений рассматриваемого вида, которые редко организуются единолично. Часто правоохранительные органы имеют дело с повторяющимися, детально подготовленными деяниями со сложным и многоступенчатым механизмом, что может осуществляться только организованными преступными группами, включающими организатора; специалистов в области информационных технологий и программирования; лиц, обладающих компетенциями в области компьютерных технологий, эксплуатации ПЭВМ и иных технических средств, а также электронных кошельков с целью последующего перевода на них денежных средств; лиц,

6 Клепицкий И.А. Комментарий к Уголовному кодексу Российской Федерации (постатейный). М. : ИНФРА-М, 2019. С. 556.

осуществляющих снятие наличных денежных средств со счетов или в банкоматах[7], и пр.

Потерпевшей стороной среди юридических лиц обычно являются организации финансового сектора, преимущественно занимающиеся электронной коммерцией, оказывающие телекоммуникационные или образовательные услуги. Кроме того, крупные компании и корпорации не желают сообщать в правоохранительные органы о совершенных преступлениях в связи с действующей репутационной политикой, боязнью раскрытия механизма обеспечения информационной безопасности и функционирования систем защиты информации на предприятии.

Заключение

Выявление актуального набора элементов, входящих в состав криминалистической характеристики отдельно взятого вида преступлений – в сфере компьютерной информации, – позволит в дальнейшем формировать информационно-компьютерные модели деяний [23, с. 69] (обобщение сведений о криминалистически значимых признаках конкретного вида преступления и их закономерных связях на основе изучения больших массивов уголовных дел), а также цифровые криминалистические модели преступлений (обобщение в машиночитаемой форме, в которой сведения о значимых признаках и их взаимосвязях выражены математическими категориями) в виде основ криминалистической методики их расследования. Знание о модели в виде типовых наборов элементов криминалистической характеристики преступлений позволяет выдвигать достоверные криминалистические версии об обстоятельствах, подлежащих установлению и доказыванию в каждом конкретном случае.

Элементы криминалистической характеристики рассматриваемой категории преступлений имеют существенное значение и требуют своевременной актуализации. Стоит также отметить, что все выделенные составляющие находятся в неразрывной связи друг с другом и обретают причинно-следственные связи. Необходимость их выявления и актуализации обусловлена тем, что при наличии сформированных наборов элементов, специфичных для конкретного преступного деяния, следователь сможет выстроить криминалистические версии и подобрать наиболее подходящую методику расследования со значительно меньшими трудовыми и временны́ми затратами.

Таким образом, криминалистическая характеристика преступлений, совершаемых в сфере компьютерной информации, фактически представляет собой информационно-теоретическую базу для создания типовых алгоритмов их расследования. Изложенное позволяет сделать вывод о возможности формирования на их основе так называемого цифрового двойника [24, с. 3563] преступления в виде его цифровой копии, позволяющей оптимизировать процесс расследования. В качестве исходных дополнительных данных для построения такого рода информационно-компьютерной модели могут быть отобраны условные признаки, которые в наибольшей степени влияют на прогноз раскрываемости (взятые, например, из статистических карт по преступлениям прошлых лет) и, по сути своей, выступают значимыми элементами криминалистической характеристики преступления.

7 Обзор правоприменительной практики по противодействию киберпреступлений : аналитический обзор / Е.А. Антонян, Е.Р. Россинская, Е.Н. Клещина и др. М. : Консорциум «Инновационная юриспруденция», 2024. С. 85.

Список источников

1. Ходанов А.И. Проблемы придания статуса casus belli кибератаке на государство – члена НАТО / А.И. Ходанов. – DOI 10.33184/pravgos-2024.3.18 // Правовое государство: теория и практика. – 2024. – № 3. – С. 155–159

2. Россинская Е.Р. Избранное : монография / Е.Р. Россинская. – Москва : Норма, 2021. – 680 с.

References

1. Khodanov A.I. Challenges of Granting the Status of Casus Belli to a Cyberattack on a NATO Member State. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2024, no. 3, pp. 155–159. (In Russian). DOI 10.33184/pravgos-2024.3.18.

2. Rossinskaya E.R. Selected. Moscow, Norma Publ., 2021. 680 p.

3. Россинская Е.Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики / Е.Р. Россинская. - DOI 10.33184/pravgos-2020.4.9 // Правовое государство: теория и практика. – 2020. – № 4-1 (62). – С. 88–101.

4. Вехов В.Б. Компьютерные преступления. Способы совершения. Методики расследования : монография / В.Б. Вехов. – Москва : Право и закон, 1996. – 136 с.

5. Hashemi A. AI-generated or Ai Touch-Up. Identifying AI Contribution in Text Data / A. Hashemi, W. Shi, J. Corriveau // International journal of data science and analytics. – 2024. – № 1. – P. 1–12.

6. Pachimatla D. Advanced Algorithms to Detect and Prevent the Spread of Manipulated Images and Videos Using Deep Learning and AI / D. Pachimatla, R. Kilari, I.B. Ranitha // Proceedings of 5th International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. – 2025. – № 1182. – P. 415–427.

7. Qin H. Identity, Crimes, and Law Enforcement in the Metaverse / H. Qin, Y. Wang, P. Hui // Humanities and Social Sciences Communications. – 2025. – № 12 (194). – P. 1–15.

8. Mihailescu M. Quantum algorithms / M. Mihailescu, S. Nita, V. Marascu. – Springer, 2025. – 118 p.

9. Потапов С.М. Принципы криминалистической идентификации / С.М. Потапов // Советское государство и право. – 1940. – № 1. – С. 66–81.

10. Криминалистика. Теоретический курс : монография / А.А. Эксархопуло, И.А. Макаренко, Р.И. Зайнуллин и др. – Уфа : НИИ ППГ, 2022. – 650 с.

11. Тюхтин В.С. Отражение, системы, кибернетика. Теория отражения в свете кибернетики и системного подхода : монография / В.С. Тюхтин. – Москва : Наука, 1972. – 256 с.

12. Бессонов А.А. Цифровая криминалистическая модель преступления как основа противодействия киберпреступности / А.А. Бессонов // Академическая мысль. – 2020. – № 4 (13). – С. 58–61.

13. Татарникова Т.М. Интеллектуальный анализ данных : монография / Т.М. Татарников. – Вологда : Инфра-Инженерия, 2024. – 172 с.

14. Макаренко И.А. Содержание криминалистического обеспечения расследования преступлений / И.А. Макаренко // Криминалистика, уголовный процесс и судебная экспертология в XXI веке: векторы развития (66-е ежегодные криминалистические чтения) : сборник статей Международной научно-практической конференции, Москва 25 апреля 2025 г. : в 3 ч. – Москва : Академия управления МВД России, 2025. – Ч. 2. – С. 119–126.

15. Яблоков Н.П. Обстановка совершения преступления как элемент его криминалистической характеристики / Н.П. Яблоков // Криминалистическая характеристика преступления : сборник научных трудов научной конференции. – Москва, 1984. – С. 38–39.

16. Ахмедшин Р.Л. Криминалистическая характеристика личности преступника : автореф. дис. … д-ра юрид. наук : 12.00.09 / Р.Л. Ахмедишин. – Томск, 2006. – 54 с.

17. Макаренко И.А. Развитие идей профессора Л.Л. Каневского в современной криминалистике / И.А. Макаренко. – DOI 10.33184/pravgos-2024.2.7 // Правовое государство: теория и практика. – 2024. – № 2. – С. 56–59.

18. Зуев С.В. ИТ-справочник следователя : монография / С.В. Зуев. – Москва : Юрлитинформ, 2019. – 232 с.

19. Holt T.J. Cybercrime and Digital forensics. Introduction / T.J. Holt, A.M. Bossler, K.C. Seigfried-Spellar. – Abingdon-Routledge, 2018. – 754 p.

3. Rossinskaya E.R. The Doctrine of Forensic Activities Digitalization and the Problems of Forensic Didactics. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2020, no. 4-1 (62), pp. 88–101. (In Russian). DOI 10.33184/pravgos-2020.4.9.

4. Vekhov V.B. Computer Crimes. Means of Committing. Investigation Methods. Moscow, Pravo i zakon Publ., 1996. 136 p.

5. Hashemi A., Shi W., Corriveau J. AI-generated or AI Touch-Up. Identifying AI Contribution in Text Data. *International Journal of Data Science and Analytics,* 2024, no. 1, pp. 1–12.

6. Pachimatla D., Kilari R., Ranitha I.B. Advanced Algorithms to Detect and Prevent the Spread of Manipulated Images and Videos Using Deep Learning and AI. *Proceedings of 5th International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*, 2025, no. 1182, pp. 415–427.

7. Qin H., Wang Y., Hui P. Identity, Crimes, and Law Enforcement in the Metaverse. *Humanities and Social Sciences Communications*, 2025, no. 12 (194), pp. 1–15.

8. Mihailescu M., Nita S., Marascu V. Quantum Algorithms. Springer, 2025. 118 p.

9. Potapov S.M. Principles of Criminalistic Identification. *Sovetskoe gosudarstvo i pravo = Soviet State and Law,* 1940, no. 1, pp. 66–81. (In Russian).

10. Eksarkhopulo A.A., Makarenko I.A., Zainullin R.I. et al. Criminalistics. Theoretical Course. Ufa, 2022. 650 p.

11. Tyukhtin V.S. Reflection, Systems, Cybernetics. Reflection Theory in Light of Cybernetics and Systems Approach. Moscow, Nauka Publ., 1972. 256 p.

12. Bessonov A.A. Digital Forensic Crime Model as a Basis for Countering Cybercrime. A*kademicheskaya mysl' = Academic Thought*, 2020, no. 4 (13), pp. 58–61. (In Russian).

13. Tatarnikova T.M. Data Mining. Vologda, Infra-Engineering Publ., 2024. 172 p.

14. Makarenko I.A. Contents of Criminalistic Support for Crime Investigation. *Criminalistics, Criminal Procedure and Forensic Expertology in the 21st Century: Development Vectors (66th Annual Criminalistic Readings). Collection of Articles from the International Scientific and Practical Conference, Moscow, April 25*, 2025. Academy of Management of the Ministry of Internal Affairs of Russia Publ., 2025, pt. 2, pp. 119–126. (In Russian).

15. Yablokov N.P. The Environment of the Crime as an Element of Its Criminalistic Characteristics. *Criminalistic Characteristics of the Crime. Collection of Scientific Papers of the Scientific Conference*. Moscow, 1984, pp. 38–39. (In Russian).

16. Akhmedshin R.L. Criminalistic Characteristics of the Criminal's Personality. *Doct. Diss. Thesis*. Tomsk, 2006. 54 p.

17. Makarenko I.A. The Development of Professor L.L. Kanevsky's Ideas in Contemporary Criminalistics. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2024, no. 2, pp. 56–59. (In Russian). DOI 10.33184/pravgos-2024.2.7.

18. Zuev S.V. Investigator's IT Handbook. Moscow, Yurlitinform Publ., 2019. 232 p.

19. Holt T.J., Bossler A.M., Seigfried-Spellar K.C. Cybercrime and Digital Forensics. Introduction. Abingdon-Routledge, 2018. 754 p.

20. Хисамова З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики / З.И. Хисамова // Российский следователь. – 2018. – № 9. – С. 43–47.

21. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е.А. Русскевич. – Москва : ИНФРА-М, 2022. – 352 с.

22. Харисова З.И. Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» / З.И. Харисова // Вестник Уфимского юридического института МВД России. – 2019. – № 3 (85). – С. 92–98.

23. Россинская Е.Р. Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа») / Е.Р. Россинская, А.И. Семикаленова // Вестник Томского государственного университета. Право. – 2021. – № 42. – С. 68–80.

24. Tao F. Digital Twin-Driven Product Design, Manufacturing and Service with Big Data / F. Tao, J. Cheng, Q. Qi // International Journal of Advanced Manufacturing Technology. – 2018. – № 94. – P. 3563–3576.

20. Khisamova Z.I. On the Criminal Liability for Embezzlement Performed Using IT Technology: An Analysis of Legal Amendments and the Law Enforcement Practice. *Rossijskij sledovatel' = Russian Investigator*, 2018, no. 9, pp. 43–47. (In Russian).

21. Russkevich E.A. Criminal Law and "Digital Crime": Problems and Solutions. Moscow, INFRA-M Publ., 2022. 352 p.

22. Kharisova Z.I. Current Issues of Law Enforcement Agencies of Crime Counteraction in the Global "Network". *Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii = Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia*, 2019, no. 3 (85), pp. 92–98. (In Russian).

23. Rossinskaya E.R., Semikalenova A.I. Information-Computer Criminalistic Models of Computer Crimes as the Elements of Criminalistic Techniques (Using the Example of "Cyber Blackmail"). *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo = Tomsk State University Journal of Law,* 2021, no. 42, pp. 68–80. (In Russian).

24. Tao F., Cheng J., Qi Q. Digital Twin-Driven Product Design, Manufacturing and Service with Big Data. *International Journal of Advanced Manufacturing Technology,* 2018, no. 94, pp. 3563–3576.

Информация об авторе

Харисова Зарина Ирековна – кандидат технических наук, доцент, старший преподаватель кафедры криминалистики Института права.

Information about the Author

Kharisova Zarina Irekovna – Candidate of Technical Sciences, Associate Professor, Senior Lecturer of the Chair of Criminalistics of the Institute of Law.

Статья поступила в редакцию 19.04.2025; одобрена после рецензирования 21.05.2025; принята к публикации 21.05.2025.
The article was submitted 19.04.2025; approved after reviewing 21.05.2025; accepted for publication 21.05.2025.