УДК 343

Сухоставский Артём Игоревич, магистрант ,
Дальневосточный ФГКОУ ВО ДВЮИ
МВД России имени И.Ф. Шилова

Жердев Павел Александрович,
профессор кафедры криминалистики,
ФГКОУ ВО ДВЮИ МВД России имени И.Ф. Шилова

НАУЧНЫЕ И ПРАВОВЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ ОТДЕЛЬНЫХ ВИДОВ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ
SCIENTIFIC AND LEGAL ISSUES IN INVESTIGATING SPECIFIC TYPES OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Аннотация. В статье анализируется криминалистическая характеристика преступлений, совершённых с использованием информационно-телекоммуникационных технологий. Раскрываются её ключевые элементы – способ совершения преступления, обстановка, личность и мотивация преступника, а также следовая картина, включающая физические и цифровые следы. Подчёркивается необходимость разработки специализированных методик расследования и повышения квалификации следователей для эффективного противодействия киберпреступности.

Abstract. This article examines the forensic characteristics of crimes committed through the use of information and telecommunication technologies. It elucidates the key components of such characteristics – namely, the modus operandi, the circumstances of the offense, the offender's profile and motivation, as well as the trace evidence encompassing both physical and digital traces. The study emphasizes the necessity of developing specialized investigative methodologies and enhancing the professional competence of investigators to effectively counter cybercrime.

Ключевые слова: Криминалистическая характеристика, киберпреступления, информационно-телекоммуникационные технологии, способ совершения преступления, следовая картина, личность преступника, цифровые следы, методика расследования, криминалистика, информационная безопасность.

Keywords: Forensic characteristics, cybercrime, information and telecommunication technologies, modus operandi, trace evidence, offender profile, digital traces, investigative methodology, forensic science, information security.

В науке понятие «криминалистическая характеристика» прочно утвердилась в качестве базового концептуального элемента, раскрывающего специфику действий лиц в рамках конкретного преступления. Считается, что любое противоправное деяние представляет собой действие, имеющее уникальный набор атрибутов и особых черт, имеющих значение для обнаружения, раскрытия и расследования преступлений.

Выделение наиболее часто встречающихся, характерных черт определенного типа преступлений находит отражение в концепции «криминалистической характеристики преступления». В отличие от уголовно-правовой и криминологической характеристик, используемых для оценки масштаба распространения, динамики отдельных видов преступлений и определения степени общественной опасности конкретного деяния,

криминалистическая характеристика способствует повышению результативности расследования преступного события [1].

Несмотря на продолжающиеся научные споры, криминалистическая характеристика является основополагающим структурным элементов частных криминалистических методик. В теории криминалистики она признается научной абстракцией, представляющей собой систему знаний о типичных признаках преступлений и закономерностях их взаимосвязи, служащей основой для методики расследования преступлений против личности, против собственности, против информационной безопасности (Р.С.Белкин, А.Н. Васильев, Л. Г. Видонов, И. А. Возгрин, В. К. Гавло, В. А. Образцов, И. Ф. Пантелеев, В. Г. Танасевич, В. И. Шиканов, Н. П. Яблоков). На базе этих научных знаний разрабатываются конкретные практические рекомендации, направленные на раскрытие, расследование и предотвращение преступной деятельности.

Сюда можно отнести и преступления, совершенные с использованием компьютерных технологий. К этой группе относятся общественно опасные деяния, совершённые с применением информационных технологий и сетей в виртуальном мире. Такие преступления могут быть связаны с использованием сети «Интернет», средств мобильной связи, компьютерных техники и программ, пластиковых карт и иных технологий.

В юридической науке наблюдается разнообразие трактовок дефиниции преступлений, совершаемых с использованием информационных технологий, включая сеть «Интернет». Первая категория исследователей склонна к отождествлению данных правонарушений с «компьютерными преступлениями», «киберпреступлениями» или преступлениями, совершаемыми в киберпространстве. Другая группа специалистов описывает их как деяния в области высоких технологий или информационные преступления [2].

Использование телекоммуникационных сетей в преступных целях создает значительную угрозу общественной безопасности в силу специфических характеристик сетевой инфраструктуры и широкого спектра возможностей, которые она предоставляет. Потенциал сетевого пространства служит стимулирующим фактором для совершения противоправных действий, значительно упрощая их реализацию. Инструменты сокрытия следов преступлений, такие как специализированное программное обеспечение и технологии «луковой маршрутизации» (например, Tor), позволяют маскировать IP-адрес соединения и повышать анонимность сетевой активности. Подобные методы затрудняют идентификацию преступников и сбор доказательств, что способствует росту киберпреступности и требует разработки новых подходов к расследованию и предотвращению правонарушений в цифровой среде.

Для противодействия данному виду преступлений требуется особая методика расследования. В ее основе должны лежать задачи раскрытия и расследования преступлений в цифровой сфере. На научной основе сегодня формируется система криминалистических знаний об обнаружении, закреплении и конфискации электронных следов. Методы работы с этим типом улик должны опираться на научные принципы. Следствие по данной группе дел отличается повышенной сложностью и сопряжено с организационными проблемами, вытекающими из международного характера преступлений.

Для обеспечения системной работы в этой области в центральном аппарате Следственного комитета функционирует специализированное подразделение, занимающееся расследованием киберпреступлений и преступлений в сфере высоких технологий, а также подразделение компьютерно-технических и инженерно-технических исследований. Сотрудники этих подразделений проводят предварительное следствие и осуществляют экспертизы по делам, касающимся анализируемых преступлений. Ведется подготовка следователей, готовых работать в этой области [3].

В теории криминалистики активно обсуждается вопрос структуры, а именно, элементов, позволяющих описать событие преступления. Большинство исследователей придерживаются мнения о необходимости включения в криминалистическую характеристику закономерно повторяющихся (устойчивых) признаков, характеризующих сущность преступной деятельности. Чаще всего авторы в структуру криминалистической характеристики преступления включают способ и взаимосвязанные с ним элементы. Это могут быть сведения о методах подготовки, совершения и сокрытия противоправного деяния, характерные материальные следы и наиболее вероятные места их нахождения, данные о типичных личностных чертах преступников и потерпевших, обстановка совершения преступлений определенного типа, информация о распространенных мотивах, а также причины и условия, способствующие совершению преступлений.

Некоторые эксперты расширяют этот перечень, добавляя уголовно-правовую квалификацию деяния и типичные следственные ситуации. Несмотря на различия в составе элементов криминалистической характеристики, существует единогласие в отношении того, что её содержание должно включать только имеющие криминалистическое значение признаки, изучение которых способствует решению задач, стоящих перед следствием.

Важным является вопрос об элементах криминалистической характеристики преступлений в сфере компьютерной информации. По нашему мнению, криминалистическую характеристику следует рассматривать в качестве информационной модели, представляющей описание существенных признаков противоправного деяния, важных с точки зрения его раскрытия и расследования. В состав элементов, характеризующих преступления, совершенные с использованием информационно-телекоммуникационных технологий, следует включить:

1) способ совершения преступления, раскрывающий воплощенный в действиях и используемых средствах алгоритм преступления, позволяет установить иные элементы деяния. В результате можно установить логическую последовательность действий, выражающуюся в формуле «действия подозреваемого и средства преступления – способ совершения преступления»;

2) обстановка совершения преступления представляет собой совокупность взаимосвязанных объектов, явлений, процессов, действующих до и в момент совершения противоправного деяния. Эта категория охватывает временные, пространственные, материальные и иные условия окружающей среды, а также характер поведения лиц, косвенно причастных к преступлению, связанному с использованием компьютерной техники. Указанные факторы в совокупности определяют вероятность, условия и обстоятельства совершения преступного деяния. Консолидированные знания об обстановке преступления, рассматриваемые во взаимосвязи с другими компонентами криминалистической характеристики, позволяют следователю сфокусировать внимание на наиболее продуктивном поиске и установлении обстоятельств, имеющих доказательственное значение.

3) личность и мотивация преступника. Анализ особенностей личности киберпреступника обусловлен значимостью преступных действий и его ориентаций. Такие характеристики позволяют понять каков механизм совершения преступления, план преступника и его потенциальный интерес в уголовном деле. В условиях повсеместной цифровизации общественных отношений, исследование психологических особенностей киберпреступников приобретает особую значимость. В системе ценностей этих лиц преобладают эгоцентрические установки, выражающиеся в стремлении к личному обогащению и самовыражению. Бесконтрольность в совершении киберпреступлений и доступность информационных технологий способствуют объединению хакеров в организованные преступные группы с общими интересами в сфере компьютерной

информации. Анализируя личность преступника, совершившего преступление с использованием информационно-телекоммуникационных технологий, необходимо выделить основные мотивы, которыми руководствуются киберпреступники: развлечение, стремление к мести, цифровой вандализм, получение материальной выгоды, корыстные побуждения, самоутверждение и поиск признания.

4) следовая картина преступления содержит данные о расположении и виде обнаруженных следов, а также об их специфических особенностях, выраженных в качественных и количественных показателях. Очевидно, что увеличение количества объектов, содержащих следовую информацию, расширяет возможности следователя в успешном раскрытии преступления. В процессе формирования механизма образования следов при преступлениях, связанных с информационными технологиями, выделяют два типа следов: физические (следы-отпечатки, следы-частицы, следы-объекты) и электронно-цифровые [4]. Эти два вида следов важны для детального анализа и раскрытия преступлений в сфере информационных технологий. Каждый из этих типов следов предоставляет уникальную информацию, которая может быть использована для восстановления хода событий и установления виновных лиц. Комбинированное использование анализа материальных и электронно-цифровых следов повышает эффективность расследования преступлений, совершенных с применением информационных технологий [5].

Таким образом, криминалистическая характеристика преступлений в сфере компьютерной информации представляет собой сбор информации о личности преступника, способе, месте и времени, мотивах и целях, технологиях и программах, которые использовались для совершения преступления. Особую роль играют знания и навыки следователей в сфере информационно-коммуникационных технологий, поскольку от их корректных и своевременных действий зависит весь процесс расследования. Значимость и прикладная польза криминалистической характеристики любого рода тесно связаны с тем, насколько полно и систематизировано представлены сведения в её составных частях. Крайне необходимо уделять максимальное внимание деталям каждого из этих элементов.

Список литературы:

1. Дубынин Е. А. Криминалистическая характеристика преступления как фактор, влияющий на принятие решения в процессе расследования // Вестник Сибирского юридического института МВД России. 2024. № 3 (56). С. 52-57.
2. Алферова Е.В., Алешкова И.А. Электронные (цифровые) коммуникации: путь к прогрессу или регрессу // Образование и право. 2020. № 6. С. 232-237.
3. Бастрыкин А.И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник РПА. 2022. № 4. С. 88-94.
4. Жердев П.А. Электронно-цифровые следы как элемент криминалистической характеристики преступлений в сфере компьютерной информации // Вестник Дальневосточного юридического института МВД России. 2020. № 2 (51). С. 94-101.
5. Жердев П.А., Бондарчук А.С. Механизм следообразования при совершении преступлений в сфере компьютерной информации // В сборнике: Актуальные проблемы науки и практики. Сборник научных трудов. Хабаровск, 2018. С. 118-121.