УДК 34 **Юридические науки**

Стулина Екатерина Александровна, *студентка 2 курса магистратуры*
Московский университет Министерства внутренних дел Российской Федерации им В. Я. Кикотя

РАССМОТРЕНИЕ СООБЩЕНИЙ О ПРЕСТУПЛЕНИЯХ, СВЯЗАННЫХ С ДИСТАНЦИОННЫМ ХИЩЕНИЕМ ДЕНЕЖНЫХ СРЕДСТВ

Аннотация: в данной статье представлена точка зрения на вопросы, связанные с практикой применения закона в аспекте установления территориальной юрисдикции в ходе предварительной проверки сообщений о киберпреступлениях, которые включают удаленное присвоение финансовых средств, а также последующее ведение расследования в рамках уголовных дел данной категории.

Ключевые слова: IT-преступления, способ совершения преступления, дистанционное хищение денежных средств, место совершения преступления, процессуальная проверка, подследственность, неотвратимости уголовного наказания.

Abstract: This article presents a point of view on issues related to the practice of applying the law in terms of establishing territorial jurisdiction during the preliminary verification of reports of cybercrime, which include the remote appropriation of funds, as well as subsequent investigation in criminal cases of this category.

Key words: IT crimes, the method of committing a crime, remote theft of funds, the place of commission of the crime, procedural verification, investigation, the inevitability of criminal punishment.

Современные достижения науки внимательно затрагивают каждый аспект общественной жизни, стимулируя появление всё более новых и усовершенствованных методов информационного обмена.

В эпоху глобальной цифровизации становится очевидной тенденция к формированию устойчивой связи между растущим многообразием информационных и телекоммуникационных технологий и качественными преобразованиями в структуре преступности в современной России. Обширное распространение и стремительное развитие средств удаленной коммуникации открывают практически неограниченные возможности для организации, осуществления и скрытия преступлений с использованием совершенно новых методов и инструментов. Вирусные программы, мошенничество с использованием платежных карт, удаленное присвоение средств с банковских счетов, нарушения в эксплуатации автоматизированных информационных систем представляют собой лишь часть широкого спектра таких преступных действий [1].

Это явление в профессиональной среде имеет несколько названий: киберпреступность, компьютерные преступления, преступления, связанные с компьютерными технологиями, IT-преступления и так далее. В криминалистической науке последних десяти лет особенно часто употребляются два термина: "киберпреступление" и "компьютерное преступление". Считается, что эти термины взаимозаменяемы, так как они относятся к одной и той же категории общественно опасных действий, которые готовятся и совершаются с помощью различных компьютерных технологий и инструментов, а также с использованием возможностей всемирной сети Интернет.

Мы полагаем, что ключевая криминалистическая характеристика киберпреступлений состоит в необходимости глубокого понимания механизмов современных информационных технологий для их эффективного предупреждения, обнаружения, раскрытия и расследования. Как правильно отмечает А.С. Шаталов, это обстоятельство определяет необходимость разработки и улучшения методических подходов к расследованию преступлений

в цифровой среде. Тем не менее, эти процессы часто протекают медленно и несистематизированно по различным причинам [2].

В результате, наблюдается годовой рост числа таких преступлений, и в среднем они составляют почти четверть от общего числа уголовных преступлений. Более того, свыше половины уголовных дел по этим преступлениям приостанавливаются из-за невозможности установить личность обвиняемого. Например, согласно официальной статистике МВД России, из 517722 преступлений, совершенных в 2021 году в сфере информационных технологий, не были раскрыты 388607 случаев, включая 201974 преступления, квалифицируемые как «тяжкие и особо тяжкие» [3].

Против этого фона растет недоверие населения к деятельности правоохранительных структур, а также снижается шанс восстановления нарушенных прав с помощью уголовно-правовых механизмов. Это утверждение подкрепляется результатами проверок, проведенных ведомствами, которые показали, что каждый третий клиент банков, ставший жертвой кражи со счетов, не обращался за помощью в правоохранительные органы [4].

В условиях отсутствия эффективных криминалистических методик, процесс выявления и расследования киберпреступлений сталкивается с необходимостью самостоятельно находить решения возникающих юридических, организационных, технических, информационных и методологических проблем. В процессе этого правоохранительные органы накапливают опыт, который применяется в соответствии с современными требованиями их работы. Тем не менее, часто им приходится действовать, опираясь на принципы, которые заставляют их постоянно «догонять» развитие событий.

В числе ключевых проблем, отражающих текущее положение дел, необходимо особо отметить неправильное установление территориальной юрисдикции при рассмотрении дел о киберпреступлениях, которые включают в себя удаленное присвоение финансовых средств.

Некорректная правовая квалификация в таких делах, а также отсутствие стандартизированного подхода к принятию решений по этим вопросам приводят

к повторной отправке документов проверок и уголовных дел на основании формальностей, связанных с территориальной и ведомственной подсудностью. Это не только способствует скрытности таких преступлений, но и нарушает конституционные права граждан на своевременное уголовное разбирательство, приводит к потере важных доказательств и снижает шансы на выявление всех фактов и лиц, совершивших преступление.

В соответствии с частью 1 статьи 145 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) по результатам рассмотрения сообщения о преступлении должно быть принято одно из следующих решений: о возбуждении уголовного дела, о передаче сообщения по подследственности или об отказе в возбуждении уголовного дела [5].

На начальном этапе расследования киберпреступлений, связанных с удаленным присвоением финансов, проверка обычно ограничивается доступными дознавателю объяснениями потерпевшего или свидетелей, документацией из банков (как чеками, так и выписками по счетам), а также данными, имеющими криминалистическое значение, которые сохранены в устройствах связи и компьютерах. Это ограничение информации часто не позволяет полностью понять все детали происшествия и может привести к разногласиям относительно юрисдикции дела.

В соответствии с нормами действующего уголовно-процессуального кодекса, место проведения предварительного следствия устанавливается по месту совершения акта, который имеет признаки уголовного преступления, и это не зависит от времени, когда произошли общественно опасные последствия. В условиях, когда нет четкого определения «места совершения преступления», и учитывая, что действия, формирующие объективную сторону дистанционного преступления, могут происходить в различных местах, любая из этих географических точек может быть признана местом совершения преступления.

Киберпреступления, связанные с несанкционированным удаленным доступом к финансам, часто выходят за рамки одного региона или страны и осуществляются без физического контакта, при этом сохраняется анонимность

преступника. Это создает трудности для оперативного выявления как уже известных, так и других важных фактов, связанных с делом.

Важно подчеркнуть, что сегодня не все банковские и финансовые учреждения имеют филиалы, где можно открыть счет или вести учет электронных активов. Это создает сложности в точном определении места преступления, если руководствоваться только расположением филиала, где жертва открыла счет, учитывались ее электронные средства, или где был зарегистрирован счет подозреваемого, а также местом снятия наличных или регистрации пользователя мобильной или интернет-связи.

Результаты анализа нормативных правовых актов позволяют сделать вывод о том, что разъяснения по данным вопросам отсутствуют и в постановлениях Пленума Верховного Суда Российской Федерации от 27.12.2002 №29 «О судебной практике по делам о краже, грабеже и разбое» [6] и от 30.11.2017 №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [7], касающихся места окончания дистанционных краж и мошенничеств.

Указанные факторы в целом препятствуют созданию консистентной судебной практики по криминальным кейсам данного типа и подчеркивают необходимость разработки криминалистических методик, которые будут способствовать гарантированному исполнению уголовных санкций за преступления.

Мы убеждены, что при рассмотрении дел о кражах финансовых средств через IT-технологии и оценке оснований таких обвинений, прежде всего, необходимо придерживаться принципов своевременности уголовного процесса и справедливого баланса интересов всех его сторон.

Для этого в статье 152 УПК РФ предусмотрена возможность альтернативного определения подследственности, а именно: по месту совершения большинства преступных деяний; по наиболее тяжкому из преступлений; по месту нахождения обвиняемого; по месту нахождения большинства свидетелей; по месту жительства или пребывания потерпевшего.

Таким образом, проведение предварительной проверки по сообщениям о киберпреступлениях, предусмотренных статьями 158, 159-159.3, 159.5, 159.6, 163 Уголовного кодекса Российской Федерации [7], совершенных с использованием платежных карт, информационно-телекоммуникационной сети «Интернет», средств мобильной связи и иными бесконтактными способами, следует осуществлять территориально по месту их первичной регистрации. При этом решение о возбуждении уголовного дела, в случае наличия повода и достаточных оснований, целесообразно принимать в территориальном органе внутренних дел, в который поступило соответствующее сообщение.

Дальнейшая передача уголовного дела в соответствии с частью 5 статьи 152 УПК РФ для направления по подследственности, по сути, возможна лишь после производства неотложных следственных действий.

Порядок осуществления расследования уголовных дел рассматриваемой категории также должен исходить из установленных частью 4 статьи 152 УПК РФ правил территориальной подследственности, которые, в отсутствие специальных на то указаний в уголовно-процессуальном законодательстве, не требуют принятия специального решения о производстве предварительного расследования по месту нахождения обвиняемого, большинства свидетелей или потерпевших.

Следователю, завершающему предварительное расследование, надлежит учитывать положения пункта 5.1 уже упомянутого постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 No 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которому территориальная подсудность уголовного дела о хищениях, предметом которых являются безналичные денежные средства, определяется с учетом сведений о месте совершения преступления, а также других указанных в законе обстоятельств (а именно части 1–3 и 5.1 статьи 32 УПК РФ). При этом территориальная подсудность уголовного дела может быть изменена в соответствии с частью 4 статьи 32, а также статьей 35 УПК РФ.

Кажется, что особое внимание в данном контексте заслуживает недостаточная и запаздывающая реакция следственных органов на сбор дополнительной информации, имеющей криминалистическую ценность, такой как сведения о владельцах и операциях по банковским счетам, принадлежности телефонных номеров, электронных кошельков, почтовых адресов, аккаунтов, IP-адресов и записей с камер видеонаблюдения. Это часто приводит к потере важных доказательств.

Исследование практики ведения следствия по делам данного типа показывает[8], что иногда, вопреки положениям пятой части статьи 208 УПК РФ, предварительное расследование останавливается без проведения тех следственных действий, которые могут быть выполнены даже при отсутствии подозреваемого или обвиняемого. Часто задания, возложенные на органы, ответственные за оперативно-розыскную деятельность, выполняются неполностью, и результаты не фиксируются должным образом. Не всегда предварительное следствие корректно оценивает действия всех лиц, причастных к преступлениям (например, сотрудников колл-центров, лиц, занимающихся выводом средств, поддерживающих работу веб-сайтов и т.д.). В то же время, для привлечения последних к ответственности важно грамотное планирование действий в этом направлении, и координация с органами оперативно-розыскной деятельности для установления методов вывода украденного, а также порядка создания, регистрации и управления интернет-ресурсами.

Учитывая особенности механизма киберпреступлений, которые выделяют необходимость незамедлительных действий для их предотвращения, предложенные рекомендации способствуют гарантированию принципа неизбежности наказания. Это будет эффективным при условии, что такие меры не повлияют на соответствие, достоверность, законность и полноту доказательств, собранных в рамках уголовного процесса, и не приведут к нарушению прав подозреваемых, обвиняемых и потерпевших.

Библиографический список:

1. Давыдов В.О. Несколько тезисов к вопросу о проблематике практики рассмотрения сообщений и расследования уголовных дел о преступлениях, связанных с дистанционным хищением денежных средств.
2. Шаталов А.С. Феноменология преступлений, совершенных с использованием современных информационных технологий // Право: Журнал Высшей школы экономики. 2018. № 2. С. 68–83.
3. Статистический сборник «Состояние преступности в России» (январь-декабрь 2021 года). М.: ГИАЦ МВД России, 2022. 51 с.
4. Информационное письмо Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации от 08.02.2022 №36-49-22/1/1329 «О практике рассмотрения сообщений о преступлениях, совершаемых с использованием информационно-коммуникационных технологий, и об иных проблемных вопросах» [Электронный ресурс] // СПС «Консультант-Плюс» (дата обращения 22.06.2024).
5. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. От 29.05.2024) // «Российская газета» от 22 декабря 2001 г. №249.
6. Постановление Пленума Верховного Суда Российской Федерации от 27.12.2002 №29 «О судебной практике по делам о краже, грабеже и разбое» // Бюллетень Верховного Суда Российской Федерации. 2003. No 2.
7. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]// Информационно-правовой портал «Гарант» (Дата обращения 22.06.2024).
8. Обзор практики расследования уголовных дел о хищения денежных средств, совершаемых бесконтактными способами (январь–декабрь 2021 года). Тула: Следственное управление УМВД России по Тульской области, 2022.