Научная статья
УДК 343.14
doi: 10.35750/2071-8284-2024-1-103-110

Михаил Александрович Бугера
кандидат юридических наук, доцент
https://orcid.org/0000-0003-4752-0620, ma.bugera@mail.ru

Волгоградская академия МВД России
Российская Федерация, 400075, Волгоград, ул. Историческая, д. 130

Информационные особенности типичных следственных ситуаций, возникающих при расследовании хищений мобильных средств связи

Аннотация: **Введение.** Хищения мобильных средств связи – часто совершаемое преступление, регулярность которого обусловлена, в том числе, ростом количества средств связи у граждан, их популярностью и удобством в использовании, а также иными факторами. **Методы.** Работая над статьей, автор использовал различные методы, среди которых общенаучные методы познания, частнонаучные методы и междисциплинарный метод формализации. К материалам же относятся данные из реальной юридической практики, материалы уголовных дел, судебные акты. **Результаты.** В статье были проанализированы современное состояние и трансформация механизма хищений мобильных средств связи. Изучены и типизированы основные способы совершения хищений, применяемые при этом приёмы и технологии. Автором исследованы информационные особенности наиболее типичных следственных ситуаций, возникающих при расследовании хищений мобильных средств связи и сделан вывод о том, что чаще всего хищения мобильных средств связи совершаются путём краж (в том числе карманных; краж в общественных местах; краж с проникновением), грабежей, мошенничества. Система формирования наиболее типичных следственных ситуаций построена на сочетании аналитики следственной практики и теоретического исследования. Сама типичная следственная ситуация в расследовании хищений мобильных телефонов включает в себя различные аспекты, среди которых автор выделяет совокупность всех сведений и данных о хищении; сбор доказательств, связанных с преступлением; их комплексный системный анализ; основы взаимодействия с операторами мобильной (сотовой) связи и т. д.

Ключевые слова: типичные следственные ситуации, мобильные телефоны, мобильные средства связи, хищения, взаимодействие с оператором мобильной (сотовой) связи, онлайн-платформы, кибербезопасность

Для цитирования: Бугера М. А. Информационные особенности типичных следственных ситуаций, возникающих при расследовании хищений мобильных средств связи // Вестник Санкт-Петербургского университета МВД России. – 2024. – № 1 (101). – С. 103–110; doi: 10.35750/2071-8284-2024-1-103-110.

Mikhail A. Bugera
Cand. Sci. (Jurid.), Docent
https://orcid.org/0000-0003-4752-0620, ma.bugera@mail.ru

Volgograd Academy of the MIA of Russia
130, Istoricheskaya str., Volgograd, 400075, Russian Federation

The most typical investigative situations that arise during the investigation of theft of mobile communication devices

Abstract: **Introduction.** Theft of mobile communication devices is a frequently committed crime, the regularity of which is due to the increase in the number of communication devices among citizens, its popularity and ease of use, as well as other factors. **Methods.** While working on the article, the author used various methods, including general scientific methods of cognition, private scientific methods and an interdisciplinary method of formalization. The data of real legal practice, materials of criminal cases and judicial acts were also used. **Results.** The current state and transformation of the mechanism of theft of mobile communication devices is analyzed in the article. The main methods of committing theft, the techniques and technologies used in this process are studied and typified. The author considered the most typical investigative situations that arise duringthe investigation of theft of mobile communication devices. The conclusion was drawn that the most common loss of mobile communication devices is committed by theft (including pickpocketing; theft in public places; burglary), robbery, fraud. The system of formation of the most typical investigative situations is based on a combination of analysis of investigative practice and theoretical research. The typical investigative situation in the investigation of mobile phone theft includes various aspects, among which the author emphasizes the totality of all information and data regarding theft; collecting evidence related to the crime; its comprehensive system analysis; the basics of interaction with mobile operators, etc.

Keywords: typical investigative situations, mobile phones, mobile communication devices, theft, interaction with a mobile operator, online platforms, cybersecurity

For citation: Bugera M. A. The most typical investigative situations that arise during the investigation of theft of mobile communication devices // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2024. – № 1 (101). – P. 103–110; doi: 10.35750/2071-8284-2024-1-103-110.

Введение

Как и всякое электронное устройство, мобильные средства связи могут стать объектами различных хищений. Самый распространенный способ хищения мобильного устройства – кража. Один из наиболее типичных способов хищения мобильных телефонов — это карманные кражи. Преступники могут подойти к жертве незаметно и быстро вытащить телефон из кармана, сумки, а затем мгновенно скрыться. Это часто происходит в местах плотного скопления людей, таких как общественный транспорт, уличные мероприятия (митинги, праздники и т. д.) или торговые центры.

Киберпреступники могут пытаться копировать или перехватывать данные SIM-карты. Они могут воспользоваться различными мошенническими методами и приёмами, чтобы получить информацию о SIM-карте от оператора связи или использовать специализированное оборудование для копирования данных.

Мобильные телефоны являются ценными предметами, востребованными на рынке. Их высокая стоимость и популярность делают их привлекательными для потенциальных похитителей.

Некоторые мобильные средства связи могут быть легко подвержены хищениям из-за отсутствия должной безопасности и защиты. Низкая эффективность или слабость установленных механизмов блокировки, паролей или биометрической идентификации может способствовать хищениям.

Недостаточное внимание или беспечность со стороны владельцев мобильных телефонов также может способствовать кражам. Оставление устройств без присмотра или небрежное обращение с ними в общественных местах может предоставить возможность похитителям совершить кражу.

Отсутствие эффективной системы реагирования со стороны правоохранительных органов, операторов мобильной (сотовой) связи и других заинтересованных сторон может способствовать безнаказанности преступников и, следовательно, поощрять хищения мобильных телефонов.

Организованные преступные группы могут разрабатывать и распространять схемы хищений мобильных средств связи, такие как уличные грабежи, карманные кражи, разбойные нападения на магазины или курьеров, чтобы осуществлять хищения мобильных устройств.

Создание незаконного рынка для похищенных мобильных устройств и отсутствие эффективных контрмер провоцируют хищения. Преступники могут перепродавать похищенные телефоны через интернет или другие каналы и получать незаконную прибыль.

В целом, факторы, способствующие хищениям мобильных телефонов в России, объединяются вокруг ценности устройств, возможностей для хищения, отсутствия эффективной системы предотвращения и реагирования, а также востребованности незаконного рынка для перепродажи.

Актуальность темы безусловна. Исследования в данной сфере проводили различные авторы, многие из которых по-разному трактуют отдельные аспекты процесса расследования хищений мобильных средств связи. Так, А. В. Шебалин характеризовал наиболее типичные следственные ситуации первоначального этапа расследования хищений сотовых телефонов [14]; этот же анализ осуществлял и А. С. Харлов[11], предлагая определённые программы действий следователя на первоначальном этапе расследования по делам о хищении сотовых телефонов, Е. Е. Шавкарова изучала деятельность следователя на первоначальном этапе расследования хищений сотовых телефонов [12], А. Б. Максимович давал авторскую характеристику хищений средств сотовой связи [8]; И. В. Макогон [6], Л. В. Косарева [7] и Б. Б. Шойжилцыренов [15] детализировали проблемы, возникающие при расследовании хищений мобильных средств связи; К. Е. Демин и А. А. Васильев раскрыли криминалистические аспекты получения доказательственной информации с электронных носителей данных [5], А. А. Голубчиков в целом характеризовал криминалистическое обеспечение раскрытия и расследования грабежей и разбойных нападений [4].

Методы

Работая над статьей, мы использовали различные методы, среди которых общенаучные методы познания (сравнение, восхождение от абстрактного к конкретному, анализ, синтез, индукция, дедукция, обобщение, классификация, абстрагирование), частнонаучные методы (формально-юридический, сравнительно-правовой, метод толкования норм права, догматический), междисциплинарный метод формализации. К материалам же относятся данные из реальной юридической практики, материалы уголовных дел, судебные акты.

Результаты

Некоторые учёные группируют данные факторы по основаниям технических особенностей средств мобильной связи, виктимного поведения потерпевших и деятельности правоохранительных органов, направленной на установление лиц, совершивших рассматриваемые хищения средств мобильной связи [1, с. 14].

В. К. Гавло, который пишет, что «типичные ситуации являются своеобразными теоретическими моделями, ориентироваться на которые полезно с точки зрения отыскания в них недостающих признаков сложившейся конкретной ситуации. Поэтому следователь всегда должен сопоставить конкретную ситуацию с типичной, известной ему ранее. Если они оказываются сопоставимыми по своим криминалистическим характеристикам, то основной алгоритм типичной ситуации по расследованию преступления может быть приемлемым и для конкретной ситуации»[2, с. 163].

А. В. Шебалин [13, с. 100] в основу деления типичных следственных ситуаций по рассматриваемой категории уголовных дел положил способ сокрытия виртуальных следов преступления. Он предлагал следующие типичные следственные ситуации:

1. Неустановленный преступник не предпринимал мер к сокрытию виртуальных следов преступления и звонил с похищенного телефона, в котором находилась SIM-карта потерпевшего.

2. Неустановленный преступник удалил SIM-карту потерпевшего из похищенного телефона, однако телефон подключен к сети одного из операторов мобильной (сотовой) связи с другой SIM-картой.

В зависимости от сведений о лице, совершившем хищение средства сотовой связи, и факта обнаружения мобильного телефона выделены типичные следственные ситуации первоначального этапа расследования [10, с. 41]:

1) имеются признаки совершения хищения средства сотовой связи, лицо (подозреваемый) задержано, сотовый телефон изъят;

2) имеются признаки совершения хищения средства сотовой связи, лицо (подозреваемый) задержано, сотовый телефон не изъят;

3) имеются признаки совершения хищения средства сотовой связи, лицо (подозреваемый) не установлено и не задержано, сотовый телефон не изъят.

К сожалению, невозможно в рамках одной статьи проанализировать все типичные версии, мы рассмотрим их в зависимости от объёма данных, характеризующих непосредственно само мобильное средство связи, и выделим в соответствии с этим три типичные ситуации, возникающие при расследовании хищений мобильных средств связи:

в распоряжении следователя имеется полная информация о признаках средства мобильной связи, IMEI-номере, номере SIM-карты [9, с. 221];

в распоряжении следователя имеется неполная информация о признаках средства мобильной связи, т. е. отсутствует информация о номере SIM-карты и (или) отсутствует информация об IMEI-номере. Чтобы расследовать такое хищение, следователь может использовать данные с системы видеонаблюдения в общественных местах или свидетельские показания. Если преступник пытается использовать похищенный телефон или продать его, следы могут обнаружиться при проверке данных провайдера или баз данных похищенных устройств;

в ходе раскрытия и расследования преступлений было обнаружено и изъято средство мобильной связи, в котором отсутствовала SIM-карта, и нет данных о владельце.

Охарактеризуем алгоритм действий следователя в указанных типичных следственных ситуациях, анализируя отдельные нюансы его действий.

Действия следователя в первой типичной следственной ситуации, следующие:

Проводится осмотр места происшествия, причём следователь обязан фиксировать все имеющиеся данные, включая признаки средства мобильной связи, IMEI-номер и номер SIM-карты. Эти данные могут быть важными для проведения следующих этапов расследования. Важно проследить возможные пути отхода преступника.

Нужно обратиться к оператору, предоставляющему услуги мобильной связи для получения от него установочных данных абонента (ФИО, паспортных данных, адреса регистрации и места жительства) по абонентскому номеру, чтобы получить информацию о последних вызовах, отправленных и полученных сообщениях, а также о расходе данных на телефоне. Если мобильный телефон включен, следователь может направить оператору запрос на определение местоположения устройства с использованием сети сотовой связи.

Нужно запросить у оператора мобильной (сотовой) связи информацию о последних вызовах, отправленных и полученных сообщениях, длительности разговоров, а также о расходе данных на телефоне. Это позволяет определить активность телефона и возможные контакты.

IMEI-номер является уникальным идентификатором каждого мобильного устройства. Следователи могут использовать этот номер для отслеживания телефона и определения его статуса (например, заблокирован ли он). Если средство мобильной связи было заблокировано или у него был включен режим поиска, следователь может обратиться в службу поддержки производителя телефона для получения дополнительной информации или помощи в отслеживании и восстановлении телефона.

Следователи могут обращаться к различным интернет-платформам и социальным сетям для получения информации об активности на похищенном телефоне, например входе (или попытках входа) в учетные записи или сообщениях, которые могут быть полезными для расследования.

Конечно же, следователем должен быть осуществлён максимально подробный и детализированный допрос потерпевшего лица, у которого похитили мобильное средство связи. В ходе допроса нужно выяснить для последующей перепроверки все обстоятельства хищения.

Далее необходимо произвести выемку документов, имеющих непосредственное отношение к похищенному мобильному средству связи (упаковки, гарантийного талона, руководства по эксплуатации смартфона, инструкции, чеки и т. д.) при их наличии.

Нужно также помнить, что в России централизованный учет похищенных и изъятых номерных вещей и документов используется для облегчения и улучшения расследования различных преступлений, в том числе хищений, включая хищение мобильных телефонов. Система учета содержит информацию о похищенных и изъятых номерных вещах и документах, включая мобильные телефоны.

При осуществлении контрольных мероприятий, например, при проверке документов задержанных лиц или при проверке места жительства подозреваемых, правоохранительные органы могут запросить информацию из базы данных и установить, является ли мобильный телефон связанным с преступлением и принадлежащим определенному лицу.

Если мобильный телефон уже был зарегистрирован как похищенный в базе данных, это позволяет оперативным службам быстро установить статус устройства и принять соответствующие меры в случае обнаружения или покупки такого устройства.

Централизованная система учета позволяет отслеживать повторные случаи хищений мобильных телефонов и устанавливать связи между различными криминальными активностями. Это может помочь выявить сети организованной преступности, занимающиеся кражами и сбытом украденных телефонов.

Централизованный учет похищенных и изъятых номерных вещей и документов предоставляет правоохранительным органам значительную информацию и инструменты для расследования преступлений, включая хищение мобильных телефонов. Это способствует повышению эффективности в борьбе с преступностью и может сыграть важную роль в раскрытии, расследовании предотвращении подобных преступлений.

При расследовании хищений мобильных телефонов по поручению следователя могут проводиться различные оперативно-разыскные мероприятия. Если хищение мобильного телефона произошло в общественном месте, нужно запросить видеозаписи с камер видеонаблюдения, чтобы идентифицировать подозреваемых или направление движения злоумышленника.

Важно поддерживать контакт с информаторами или соучастниками, чтобы получить сведения о преступлениях, связанных с хищениями мобильных телефонов. Преступники, пытающиеся сбыть похищенные мобильные телефоны, могут использовать различные способы и площадки для продажи похищенных устройств. Это могут быть онлайн-платформы и торговые сайты, такие как объявления о продаже, интернет-аукционы или социальные сети, чтобы нелегально продавать похищенные мобильные телефоны. Возможно создание фиктивных профилей или использование анонимных каналов связи для совершения сделок.

В некоторых случаях преступники предпочитают торговлю на рынках, где продажа и покупка товаров может осуществляться вне законного контроля. К примеру уличные рынки, расположенные на открытом воздухе, или специализированные торговые точки, которые могут быть временными или передвижными. Нужно учитывать и возможность сбыта похищенных мобильных средств связи через ломбарды и скупки.

Анализ данных (информация из баз данных) о кражах мобильных телефонов, может помочь выявить алгоритмы действий похитителей, а также определить возможные места сбыта.

Правоохранительные органы для раскрытия хищения мобильных телефонов могут проводить оперативные мероприятия с помощью сотрудников, работающих под прикрытием, которые пытаются выявить точки сбыта похищенного с использованием контактов с потенциальными преступниками.

Действия следователя во второй типичной следственной ситуации:

Если следователю неизвестны IMEI-номер и номер SIM-карты, это может сильно затруднить процесс раскрытия хищения. Однако могут быть предприняты следующие шаги: установить IMEI-код в случае, если хозяин мобильного телефона его не знает или отсутствует упаковка. При этом возможно обратиться в адрес оператора, предоставлявшего услуги сотовой связи, с заявлением о предоставлении IMEI-кода, т. к. при переговорах фиксируется не только статус звонка (input – входящий / output – исходящий), телефонный номер абонента, с которым велись переговоры, их длительность, но и IMEI-код [3, с. 66].

Следует немедленно связаться с оператором мобильной (сотовой) связи и сообщить о произошедшем. Они могут принять меры, чтобы заблокировать SIM-карту и предоставить дополнительную помощь.

Если устройство находится включенным и подключено к мобильной сети, операторы мобильной (сотовой) связи и правоохранительные органы могут в сотрудничестве отследить его местоположение. Однако такие меры требуют соответствующих юридических действий и составления процессуальных документов совместно с провайдерами услуг связи.

В случае хищения некоторые современные мобильные устройства имеют дополнительную функциональность для отслеживания, такую как «Find My iPhone» в устройствах Apple или подобные функции для устройств на базе Android. Если такая функция была предварительно настроена и активирована на устройстве, это может помочь в его поиске.

Далее следователь должен подготовить и направить поручение сотрудникам уголовного розыска о проведении оперативно-разыскных мероприятий, указанных нами выше.

В случае обнаружения и изъятия похищенного имущества необходимо представить средство мобильной связи для опознания потерпевшему.

Действия следователя при третьей следственной ситуации:

Следователь должен осмотреть средство мобильной связи и установить IMEI-номер, который указан на ярлыке, расположенном на корпусе мобильного телефона под аккумуляторной батареей. Для проверки IMEI-номера необходимо на мобиль-

ном телефоне набрать на телефоне комбинацию цифр и символов: *#06#, на экране высветится IMEI телефона – 15-значный номер. Далее следователю следует провести проверку данного средства мобильной связи по учету, используя IMEI-номер, чтобы определить, не значится ли данный мобильный телефон среди похищенных вещей. Есть и несколько иных способов отслеживания похищенного или утерянного мобильного телефона. Если владелец установил на устройстве специальное программное обеспечение для отслеживания, такое как приложение для удаленного доступа или служебные функции операционной системы (например, Find My iPhone в iOS или Find My Device в Android), можно попытаться найти местоположение телефона через интернет или GPS.

При наличии релевантной информации, такой как IMEI-номер, оператор может предоставить данные, связанные с учетной записью владельца. Следует направить запрос оператору связи об определении по IMEI-номеру номера SIM-карты, которая использовалась в мобильном телефоне последнее время, и сведения о владельце данной SIM-карты [3, с. 66]. Оператор предоставляет данные об активности SIM-карты, которая была установлена на устройство, а также могут быть доступны записи о входящих и исходящих звонках или сообщениях.

Необходимо внимательно изучить содержимое телефона, включая контакты, сообщения, фотографии, социальные сети и другие данные, которые могут помочь определить владельца или предоставить индивидуализирующую информацию.

Следователь может проанализировать метаданные, такие как дата и время звонков, отправленных сообщений или активности в интернете, чтобы установить связи и возможные пути идентификации владельца. Также можно исследовать историю посещений веб-сайтов или активность в приложениях, что может помочь в определении личности владельца.

Если следователю не удается самостоятельно установить владельца, возможно потребуется сотрудничество с техническими экспертами в области цифровой криминалистики или кибербезопасности. Эти специалисты могут помочь извлечь более глубокую информацию из телефона, включая сведения, которые могут привести к идентификации владельца.

Когда личность владельца установят, его (при возможности) нужно допросить, уточнить все обстоятельства хищения мобильного средства связи.

Итак, мы видим, что типичные следственные ситуации, связанные с хищением мобильных телефонов, могут варьироваться в зависимости от обстоятельств и деталей конкретного случая.

При получении информации о краже мобильного телефона следственные органы проводят осмотр места преступления, чтобы собрать максимальное количество информации и выявить следы, которые могут помочь в установлении личности преступника. Это может включать фотографирование места происшествия, обнаружение и изъятие следов пальцев рук или ДНК, а также поиск объектов и предметов, не принадлежащих хозяину, таких как оставленные инструменты или следы проникновения.

Многие общественные места (магазины, кафе, остановки общественного транспорта и торговые центры) оборудованы системой видеонаблюдения.

Правоохранительные органы могут проверить местные базы данных, в которых хранится информация о похищенных мобильных телефонах. Если похищенный телефон попадает в обращение снова (например, продается или его пытаются разблокировать), это может помочь следствию в обнаружении и задержании подозреваемого.

Следователи также могут запросить данные о вызовах, сообщениях и интернет-активности на похищенном телефоне. Анализ этих данных может помочь в установлении связей или контактов, а также идентификации подозреваемых.

В каждом конкретном случае расследования хищения мобильных телефонов следователи полагаются на свои навыки, технические ресурсы и сотрудничество с различными лицами и организациями, чтобы выявить преступника и вернуть похищенное имущество. Существует несколько распространенных версий хищения мобильных телефонов, и каждая из них требует своего подхода для расследования и выявления преступников.

Важно помнить, что каждый случай хищения мобильного средства связи может отличаться, и расследование может зависеть от доступной информации и сотрудничества между пострадавшим, полицией и другими организациями.

Заключение

Таким образом, типичная следственная ситуация в расследовании хищений мобильных телефонов обычно включает следующие аспекты: совокупность всех сведений и дан-

ных о хищении; сбор доказательств, связанных с преступлением, включая показания свидетелей, видеозаписи с камер наблюдения, отпечатки пальцев, информацию от операторов мобильной (сотовой) связи и другие факты, которые могут помочь в расследовании; анализ собранных доказательств; основы взаимодействия с операторами мобильной (сотовой) связи для получения информации о местоположении похищенного телефона, истории звонков или текстовых сообщений, что может помочь в определении подозреваемых или маршрута движения телефона и т. д.

Роль типичной следственной ситуации в расследовании хищений мобильных телефонов заключается в том, чтобы создать базу фактов и доказательств, которая позволяет правоохранительным органам и следователям установить подозреваемых, предъявить обвинения и передать дело в суд. Расследование таких преступлений помогает восстановить справедливость, обеспечить возмещение вреда и предупредить дальнейшие случаи хищений мобильных телефонов.

Список литературы

1. *Архипова Н. А.* Типичные следственные ситуации и алгоритм расследования хищений средств мобильной связи // Сборник материалов криминалистических чтений. – 2010. – № 6. – С. 13–18.

2. *Гавло В. К.* Методика расследования как особая теоретико-методическая модель – информационный аналог расследования криминальных событий / Избранные труды. – Барнаул: Издательство Алтайского университета, 2011. – С. 230–242.

3. *Ганина А. А.* Актуальные проблемы получения информации у операторов мобильной связи при расследовании хищений средств мобильной связи / Актуальные проблемы уголовного права и процесса, уголовно-исполнительного права и криминалистики : материалы VIII научно-практической конференции / редкол.: Г. П. Кулешова [и др.]. – Саранск, 29 марта 2019 г. – Саранск: Всероссийский государственный университет юстиции (РПА Минюста России), 2019. – С. 65–69.

4. *Голубчиков А. А.* Криминалистическое обеспечение раскрытия и расследования грабежей и разбойных нападений // Научный дайджест Восточно-Сибирского института МВД России. – 2023. – № 4 (22). – С. 16–21.

5. *Демин К. Е., Васильев А. А.* Криминалистические аспекты получения доказательственной информации с электронных носителей данных // Публичное и частное право. – 2011. – № 3 (11). – С. 147–161.

6. *Макогон И. В., Косарева Л. В.* Особенности расследования преступлений, связанных с хищением средств сотовой связи (первоначальный этап) // Расследование преступлений: проблемы и пути их решения. – 2017. – № 1 (15). – С. 138–143.

7. *Макогон И. В., Косарева Л. В.* Проблемы, возникающие при расследовании хищении средств сотовой связи, и пути их решения // Современные проблемы права, экономики и управления. – 2016. – № 2 (3). – С. 176–180.

8. *Максимович А. Б.* Криминалистическая характеристика хищений средств сотовой связи и частное криминалистическое учение // Библиотека криминалиста. Научный журнал. – 2016. – № 6 (29). – С. 251–255.

9. *Моргунов А. Е.* Проблемы расследования хищений средств мобильной связи на современном этапе / Юридическая наука: теоретические и практические аспекты : сборник тезисов и статей Всероссийской научно-практической конференции. – Волгоград: Издательский дом «Сириус», 2019. – С. 220–223.

10. *Шебалин А. В.* Расследование хищений средств сотовой связи : монография. – Барнаул: ИНиРИО БЮИ МВД России, 2013. – 192 с.

11. *Харлов А. С.* Типичные следственные ситуации и программы действий следователя на первоначальном этапе расследования по делам о хищении сотовых телефонов // Актуальные вопросы образования и науки. – 2011. – № 5-6. – С. 40–44.

12. *Шавкарова Е. Е.* Деятельность следователя на первоначальном этапе расследования хищений сотовых телефонов / Вопросы эволюции правовой мысли человечества : сборник статей Международной научно-практической конференции. – Уфа: Аэтерно, 2015. – С. 148–152.

13. *Шебалин А. В.* О некоторых вопросах криминалистической классификации хищений средств сотовой связи // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2008. – № 8. – С. 118–120.

14. *Шебалин А. В.* Типичные следственные ситуации первоначального этапа расследования хищений сотовых телефонов / Вестник криминалистики / отв. ред. А. Г. Филиппов. – Москва: Спарк, 2008. – Вып. 3 (27). – С. 98–102.

15. *Шойжилцыренов Б. Б.* О некоторых проблемах противодействия хищениям средств сотовой связи и факторах, их детерминирующих: (по материалам Байкальского региона) // Российский следователь. – 2009. – № 12. – С. 24–27.

References

1. *Arkhipova N. A.* Tipichnyye sledstvennyye situatsii i algoritm rassledovaniya khishcheniy sredstv mobil'noy svyazi // Sbornik materialov kriminalisticheskikh chteniy. – 2010. – № 6. – S. 13–18.

2. *Gavlo V. K.* Metodika rassledovaniya kak osobaya teoretiko-metodicheskaya model' – informatsionnyy analog rassledovaniya kriminal'nykh sobytiy // Izbrannyye trudy. – Barnaul: Izd-vo Alt. un-ta, 2011. – S. 230–242.

3. *Ganina A. A.* Aktual'nyye problemy polucheniya informatsii u operatorov mobil'noy svyazi pri rassledovanii khishcheniy sredstv mobil'noy svyazi / Aktual'nyye problemy ugolovnogo prava i protsessa, ugolovno-ispolnitel'nogo prava i kriminalistiki: materialy VIII nauchno-prakticheskoy konferentsii. Redkollegiya: G. P. Kuleshova [i dr.]. Saransk, 29 marta 2019 g. – Saransk: Vserossiyskiy gosudarstvennyy universitet yustitsii (RPA Minyusta Rossii). – 2019. – S. 65–69.

4. *Golubchikov A. A.* Kriminalisticheskoye obespecheniye raskrytiya i rassledovaniya grabezhey i razboynykh napadeniy // Nauchnyy daydzhest Vostochno-Sibirskogo instituta MVD Rossii. – 2023. – № 4 (22). – S. 16–21.

5. *Demin K. Ye., Vasil'yev A. A.* Kriminalisticheskiye aspekty polucheniya dokazatel'stvennoy informatsii s elektronnykh nositeley dannykh // Publichnoye i chastnoye pravo. – 2011. – № 3 (11). – S. 147–161.

6. *Makogon I. V., Kosareva L. V.* Osobennosti rassledovaniya prestupleniy, svyazannykh s khishcheniyem sredstv sotovoy svyazi (pervonachal'nyy etap) // Rassledovaniye prestupleniy: problemy i puti ikh resheniya. – 2017. – № 1 (15). – S. 138–143.

7. *Makogon I. V., Kosareva L. V.* Problemy, voznikayushchiye pri rassledovanii khishchenii sredstv sotovoy svyazi, i puti ikh resheniya // Sovremennyye problemy prava, ekonomiki i upravleniya. – 2016. – № 2 (3). – S. 176–180.

8. *Maksimovich A. B.* Kriminalisticheskaya kharakteristika khishcheniy sredstv sotovoy svyazi i chastnoye kriminalisticheskoye ucheniye // Biblioteka kriminalista. Nauchnyy zhurnal. – 2016. – № 6 (29). – S. 251–255.

9. *Morgunov A. Ye.* Problemy rassledovaniya khishcheniy sredstv mobil'noy svyazi na sovremennom etape // Yuridicheskaya nauka: teoreticheskiye i prakticheskiye aspekty: sbornik tezisov i statey Vserossiyskoy nauchno-prakticheskoy konferentsii. – 2019. – S. 220–223.

10. *Shebalin A. V.* Rassledovaniye khishcheniy sredstv sotovoy svyazi : monografiya. – Barnaul: INiRIO BYuI MVD Rossii, 2013. – 192 s.

11. *Kharlov A. S.* Tipichnyye sledstvennyye situatsii i programmy deystviy sledovatelya na pervonachal'nom etape rassledovaniya po delam o khishchenii sotovykh telefonov // Aktual'nyye voprosy obrazovaniya i nauki. – 2011. – № 5-6. – S. 40–44.

12. *Shavkarova Ye. Ye.* Deyatel'nost' sledovatelya na pervonachal'nom etape rassledovaniya khishcheniy sotovykh telefonov // Voprosy evolyutsii pravovoy mysli chelovechestva: sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii. – Volgograd: ID «Sirius», 2015. – S. 148–152.

13. *Shebalin A. V.* O nekotorykh voprosakh kriminalisticheskoy klassifikatsii khishcheniy sredstv sotovoy svyazi // Aktual'nyye problemy bor'by s prestupleniyami i inymi pravonarusheniyami. – 2008. – № 8. – S. 118–120.

14. *Shebalin A. V.* Tipichnyye sledstvennyye situatsii pervonachal'nogo etapa rassledovaniya khishcheniy sotovykh telefonov // Vestnik kriminalistiki / otv. red. A. G. Filippov. – Moskva: Spark, 2008. – Vyp. 3 (27). – S. 98–102.

15. *Shoyzhiltsyrenov B. B.* O nekotorykh problemakh protivodeystviya khishcheniyam sredstv sotovoy svyazi i faktorakh, ikh determiniruyushchikh: (po materialam Baykal'skogo regiona) // Rossiyskiy sledovatel'. – Ufa: Aeterna, 2009. – № 12. – S. 24–27.

Статья поступила в редакцию 17.06.2023; одобрена после рецензирования 12.11.2023; принята к публикации 15.01.2024.

The article was submitted June 17, 2023; approved after reviewing November 12, 2023; accepted for publication January 15, 2024.