Научная статья
УДК 343.9

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ В СЕТИ ИНТЕРНЕТ

Шумилин Владимир Петрович[1], Шумилина Надежда Геннадьевна[2]
[1]Орловский юридический институт МВД России имени В.В. Лукьянова, Орел, Россия
[2]Орловский государственный университет имени И.С. Тургенева, Орел, Россия

[1]itdovd@gmail.com
[2]ngshumilina@gmail.com

Аннотация. В России проблема расследования мошеннических действий в сети Интернет и наказания за них становится всё более важной. Законодатели уделяют значительное внимание борьбе с интернет-мошенничеством, так как оно напрямую угрожает безопасности граждан и организаций. Актуальность исследования связана с быстрым ростом числа случаев интернет-мошенничеств, сложностью их раскрытия, а также необходимостью создания более эффективных методов борьбы с киберпреступлениями в условиях цифровизации и активного развития электронной коммерции.

Ключевые слова: киберпреступления, киберпреступность, интернет, мошенничество, интернет-преступления, криптовалюта.

Для цитирования: Шумилин В. П., Шумилина Н. Г. Особенности расследования преступлений, связанных с мошенничеством в сети Интернет // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2025. № 2(103). С. 350–359.

FEATURES OF INVESTIGATION OF CRIMES RELATED TO FRAUD ON THE INTERNET

Vladimir P. Shumilin[1], Nadezda G. Shumilina[2]
[1]Lukyanov Orel Law Institute of the Ministry of the Interior of Russia, Orel, Russia
[2]Oryol State University, Oryol, Russia

[1]itdovd@gmail.com
[2]ngshumilina@gmail.com

Annotation. In Russia, the problem of investigating and punishing fraudulent activities on the Internet is becoming increasingly important. Legislators pay significant attention to combating Internet fraud, as it directly threatens the security of citizens and organizations. The relevance of the study is due to the rapid growth in the number of Internet fraud cases, the difficulty of their detection, as well as the need to create more effective methods of combating cybercrime in the context of digitalization and the active development of e-commerce.

Keywords: cybercrime, cybercrime, internet, fraud, internet crimes, cryptocurrency.

For citation: Shumilin V. P., Shumilina N. G. Features of investigation of crimes related to fraud on the internet // Scientific Bulletin of the Orel Law Institute of the Ministry of the Interior of the Russian Federation named after V.V. Lukyanov. 2025. № 2(103). P. 350–359.

В ходе расследования мошеннических действий перед следователями возникает задача установить как невидимые, так и физически осязаемые следы преступления. Невидимые следы включают сведения, которые запомнили потерпевшие и свидетели: внешний вид злоумышленников, их манера общения или специфические детали мошеннической схемы. На первый взгляд такие детали могут казаться незначительными, но зачастую они играют ключевую роль в раскрытии преступления. Физически осязаемые следы, напротив, фиксируются в виде документации, электронных переписок, банковских транзакций или иных материалов, которые служат основой для построения доказательной базы. Для начала любого расследования необходимо заявление от пострадавшего, после чего правоохранительные органы проводят предварительную проверку. Данный этап становится отправной точкой для оценки достоверности указанных сведений и определения дальнейших процессуальных шагов. В ходе этой проверки могут вскрыться разные обстоятельства: от явного факта мошенничества до недоразумений, в которых заявитель ошибочно трактовал происходящее, либо же ситуация может оказаться попыткой целенаправленного ложного обвинения в личных интересах.

Следователи, обладая необходимыми правами и инструментами, опрашивают всех участников инцидента, а также анализируют предоставленную свидетелями информацию. При необходимости используется привлечение аудиторов или проведение экспертиз, чтобы сформировать объективное заключение. Если собранные данные позволяют, возбуждается уголовное дело для дальнейшего разбирательства. Иногда информация о мошенничествах поступает к правоохранительным органам без официального обращения, например в результате оперативной деятельности. Такие случаи требуют особенно внимательной фиксации обнаруженных доказательств, чтобы обеспечить их приемлемость и убедительность в суде или других процессах [1, с. 88].

Основным принципом деятельности полиции, утверждённым Федеральным законом Российской Федерации «О полиции» от 07.02.2011 № 3-ФЗ[1], является использование новейших научных и технических достижений, современных технологий и информационных систем. В законе закреплено использование автоматизированных систем обработки информации, программно-аппаратных комплексов, систем связи и передачи данных. Это вполне обосновано в связи с влиянием современного прогресса в области информационных и коммуникационных технологий, а также нарастающих киберугроз на различные сферы деятельности человека, включая правоохранительную систему. Сотрудники правоохранительных органов играют всё более важную роль в предотвращении киберпреступлений и обеспечении кибербезопасности в современном мире. Развитие технологий и интернета привело к увеличению числа киберпреступлений, что требует от правоохранительных органов оперативного реагирования на угрозы в киберпространстве. Таким образом, киберпреступность стала широко распространённым видом преступления в последние годы. Основными причинами такой тенденции являются [2, с. 216]:

– нехватка квалифицированных сотрудников правоохранительных органов;
– несовершенство законодательства;
– отсутствие согласительных процедур международного сотрудничества между правоохранительными органами разных стран.

Наиболее затруднительной становится работа следователей на первоначальном этапе расследования, что заключается в нехватке времени и недостаточной

[1] О полиции [Электронный ресурс]: Федер. закон Рос. Федерации от 7 февраля 2011 № 3-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

информации, неумении раскрывать киберпреступления, недостатке знаний и невозможности использовать определённые технические средства.

Оперативное расследование киберпреступлений существенно затруднено из-за потенциальной задержки банковских транзакций и скрытности преступников. Особую роль в таких расследованиях играет использование специальных знаний, предусмотренных Уголовно-процессуальным кодексом Российской Федерации (далее – УПК РФ)[1]. Законодательством установлены требования к изъятию и копированию информации с электронных носителей. Статья 164.1 УПК РФ регламентирует процедуру копирования с участием специалистов и понятых. Также в Кодексе отражено, что копирование возможно с разрешения владельца, за исключением определённых ситуаций. Правоохранители получают техническое образование для правильного реагирования на киберпреступления, но ошибки всё ещё происходят. Дополнительные меры безопасности включают документирование изъятий и запрет на использование изъятой техники, чтобы избежать уничтожения улик. Профессиональная проверка устройств на вирусы и закладки проводится на специальных стендах, что предотвращает потерю ценной информации. Но не всё ещё легко контролируется в результате оперативных действий. Например, особую сложность представляет изъятие компьютерных систем, которые имеют встроенную автономную аппаратную систему уничтожения информации при смене места расположения устройства или отключения его от других устройств компьютерного комплекса. Многообразие способов совершения рассматриваемой нами категории преступления, специфика механизма следообразования, безусловно, не могут не отразиться на особом характере производства отдельных следственных действий при расследовании киберпреступления с использованием сети Интернет.

Следует обратиться к взаимосвязи наук криминалистики и криминологии, поскольку благодаря совокупности двух наук можно наиболее точно описать личность преступника данной категории преступления. Наука криминология при изучении личности преступника предполагает раскрытие структуры этой личности, представляющей собой упорядоченное соотношение свойств (признаков), характеризующих преступника. Такая структура включает в себя шесть групп признаков:

1) социально-демографические признаки;

2) социальные признаки, проявляющиеся в различных сферах жизнедеятельности (например, профессия или семейное положение);

3) нравственные признаки;

4) уголовно-правовые признаки;

5) физические признаки;

6) психологические признаки.

Отметим и влияние общественной обстановки.

В России на фоне пандемии COVID-19 выросло количество интернет-преступлений. По некоторым данным, за время коронавируса количество мошеннических ресурсов увеличилось в два раза и ожидается дальнейший рост.

По статистике МВД России, с января по декабрь 2024 года было зафиксировано 765,4 тысячи киберпреступлений, что на 13,1 % больше, чем за аналогичный период 2023 года. Характерно, что личность преступника для данного вида преступления требует наличия специальных знаний. В связи с этим появляются несколько версий: лицо всегда увлекалось IT-технологиями, проходило определённые курсы либо обучалось в университете. Люди, совершающие преступления в интернете, очень

[1] Уголовно-процессуальный кодекс Рос. Федерации [Электронный ресурс]: Федер. закон Рос. Федерации от 18 декабря 2001 г. № 174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

скрытны и имеют маленький круг друзей, причём их друзья или знакомые зачастую много об их жизни не знают. Большинство подозреваемых – трудоспособное население от восемнадцати до пятидесяти лет, которые не имеют постоянного источника дохода. Практически каждое второе мошенничество в сети Интернет совершается в отношении женщин. Зачастую преступники отличаются высоким интеллектом, обладают знаниями в разных областях науки и техники. Как правило, основная часть таких преступных посягательств совершается после обеда и вечером. Таким образом, детальное изучение элементов криминалистической характеристики мошенничеств в сети Интернет позволило прийти к выводу о том, что способ преступления является центральным элементом в структуре криминалистической характеристики преступлений как информационного фундамента частных криминалистических методик расследования. Тем не менее важным является изучение всех элементов криминалистической характеристики рассматриваемого преступления в их взаимосвязи для получения полной информационной базы, необходимой для выбора эффективной тактики производства отдельных следственных действий. Если лицо, совершившее преступление, известно – проводится обыск. Информационные следы существуют на электронных и других материальных носителях, наделены физическими свойствами виртуальных следов, но, в отличие от них, и конкретным информационным содержанием, и поэтому не могут быть отнесены ни к одному из элементов традиционной классификации следов преступлений.

Осмотр компьютерной системы должен быть неожиданным, что исключает быстрое уничтожение содержащейся в ней информации. Объектами осмотра являются все компоненты: компьютеры, принтеры, сканеры и другие устройства, входящие в локальную или глобальную сеть. Осмотр работающего компьютера предполагает контроль за работой программного обеспечения, фиксацию изменений, происходящих в процессе работы программ, копирование всей информации, хранящейся на носителях. При осмотре неработающего компьютера устанавливают местонахождение компьютера и его периферийных устройств, способ соединения между собой этих устройств, проверяют соединение с локальной сетью и сетями телекоммуникации [3, с. 34]. Тактика осмотра средств мобильной связи и иных мобильных устройств, которые обладают многофункциональностью особенности, имеет свои особенности. Здесь следователь имеет дело с так называемыми виртуальными (идеальными), содержащимися в мобильном телефоне и в других аппаратах в виде компьютерной информации [4]:

1. О последних входящих и исходящих вызовах, времени начала, продолжительности соединения пользователя телефона с номером конкретного абонента;
2. О принятых и набранных вызовах, о введённых в память телефонных номерах с именами, адресами друзей, сослуживцев, коллег, соучастников преступления;
3. О сохранённых в памяти различных сообщениях;
4. О записанной аудио-, фото- и видеоинформации;
5. О технических данных, участвующих в процессе идентификации телефона в мобильной сети.

Полученная информация фиксируется в протоколе следственного действия, а средства мобильной связи и иные мобильные устройства приобщаются к материалам уголовного дела как вещественное доказательство.

Одним из важных следственных действий является обыск. Обыск может проводится у лица, скрывающегося от сотрудников полиции, также проживающего в настоящий момент в данном жилище. Важно, что данное следственное действие должно производиться безотлагательно, так как лицо может быстро уничтожить всю

информацию со своих электронных носителей. Первым признаком того, что данное лицо совершило преступление, является наличие в помещении множества электронных устройств: компьютеров, ноутбуков, системных блоков и иных устройств. Выемка электронной информации – очень сложный процесс. Сотрудник должен знать, где именно и на каком устройстве содержится нужная нам информация. Так как мы имеем дело с лицами, работающими в сфере компьютерной информации, то следует учитывать, что данное лицо могло «спрятать» данный файл на своём устройстве, сделать его невидимым. Все данные и носители информации будут способствовать получению информации о субъектах уголовного преследования: где был потерпевший или подозреваемый, что делал, какое программное обеспечение установлено на компьютере.

Следующее процессуальное действие – опрос свидетелей и потерпевших. Сотрудник правоохранительных органов должен удостовериться в понимании и изложении ими фактов преступления, должен понимать, что они могут ошибаться в изложении фактов, особенно если они не обладают хорошими знаниями компьютерной техники и интернетом. Если лицо, совершившее преступление, неизвестно, то в рамках доследственной проверки и при производстве по уголовному делу следователем производится ряд типичных проверочных действий. Изначально направляется несколько запросов об обстоятельствах дела в организации, занимающиеся интернет-кошельками, либо банки, если имеется информация о передаче денег на банковский счёт с целью получения IP-адресов, с которых производились открытия кошельков и, соответственно, клиентов. В связи с этим следователь должен правильно сформировать вопросы к подозреваемому с учетом определённых знаний [5, с. 64]:

1. Сам ли подозреваемый создал данный сайт для совершения преступления?
2. Через какую систему идёт списание денег у потерпевших лиц?
3. У каждого лица списываются денежные средства, которые посещают сайт, или идёт выборка?
4. На какой стадии списываются денежные средства, заложен ли этот процесс в систему или только через подтверждение подозреваемого идёт списание средств?
5. В течение какого времени разрабатывался данный сайт и с помощью каких программ, находятся ли они в свободном доступе или ограниченном?

Наиболее затруднительной является работа следователей на первоначальном этапе расследования, что заключается в нехватке времени и недостаточной информации, неумении раскрывать киберпреступления, недостатке знаний и невозможности использовать определённые технические средства. Проблемным в раскрытии и расследовании таких мошенничеств является то, что потерпевшие проживают в различных регионах России, в то время как сам преступник может находиться в регионе, не связанном с местом проживания заявителей. В связи с этим органы предварительного следствия не могут в кратчайшие сроки провести технические мероприятия на территории другого региона. Определение государственной границы в интернете невозможно, поэтому единственным способом контроля государства становится блокировка информации. Для этого создан единый реестр доменных имён, страниц сайтов в интернете и электронных адресов, которые содержат информацию, распространение которой запрещено на территории Российской Федерации на основании ст. 15.1 Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1].

[1] Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федер. закон Рос. Федерации 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

В соответствии с законом оператор связи должен ограничить доступ к таким сайтам. Таким образом, мошенничество в сети Интернет с использованием компьютерных сетей существенно возросло количественно. Мошенники, как правило, пользуются тем, что лицо самостоятельно предоставляет ему собственные данные либо обманным путём прибегают к помощи родственников. Способ, при котором мошенником могут быть получены данные банковской карты, является одним из самых опасных, так как мошенники могут и в дальнейшем воспользоваться личными данными лица [6, с. 76]. Это один из самых распространённых способов преступлений, совершаемых с применением информационно-коммуникационных технологий в сети Интернет. Среагировать на данное преступление достаточно быстро невозможно, так как денежные средства могут списываться продолжительное время или ожидание поступления на счёт обратно денежных средств занимает время. В связи с этим преступник уже удаляет свой IP-адрес либо скрывается с места преступления.

Проблемы, связанные с легализацией кибердоходов, заключаются в следующем:

– сложность выявления: кибердоходы часто имеют неясное происхождение, а также трассирование операций и транзакций может оказаться сложным из-за степени анонимности в интернете;

– отсутствие жёсткой правовой регуляции: сфера криптовалют и электронных платежей часто имеет недостаточную правовую регламентацию;

Основными проблемами раскрытия киберпреступлений являются:

– обеспечение конфиденциальности: предотвращение утечки информации о потенциальных угрозах;

– постоянное изменение технологий: непостоянность компьютерных систем и программных средств, что требует постоянного обновления навыков и знаний специалистов в сетевой безопасности;

– отсутствие международного сотрудничества: отсутствие единого международного законодательства и сотрудничества между странами мира в борьбе с киберпреступностью.

Легализация кибердоходов также сталкивается с рядом проблем и вызывает опасения в обществе:

– отсутствие нормативно-правовой базы: недостаточная разработанность правил регулирования для операций в киберпространстве, особенно в отношении криптовалют;

– мошенничество: использование киберпространства для легализации незаконных доходов в криптовалюте;

– неконтролируемый рост киберпреступлений, связанных с хищением криптовалюты.

В то же время данные вроде адреса, интернет-провайдера, трафика, использование или отсутствие шифрования легкодоступны. Сейчас провайдеры хранят их на протяжении длительного времени и анализируют в определённых случаях. Это положение соответствует требованию статьи 6 Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»[1] – обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных. Множество точек соединяет между собой реальную личность человека и сетевую: паспорт и водительские права, почтовые адреса и номера телефонов, адреса электронной почты, банковские счета, карты, аккаунты в социальных сетях. Конфиденциальность и анонимность в реальном и правовом мире невозможны. Для создания цифрового профиля человека используются следующие источники данных: физическое окружение,

[1] О персональных данных [Электронный ресурс]: Федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

почта, голосовая связь и передача данных, финансовые операции, активность в социальных сетях, камеры наблюдения, электронные системы оплаты за проезд.

Рассмотрим случай обеспечения анонимности на примере. Так, цель браузера *Tor* – легального программного обеспечения – сделать пользователей не отличимыми друг от друга, то есть анонимными. Все пользователи *Tor* обладают разным оборудованием, которое невозможно отследить. Такая практика в дальнейшем помогает разрабатывать новые, более эффективные средства и методы обнаружения преступных действий, а также оперативно оповещать граждан о возможности совершения киберпреступления в сети Интернет. С развитием методов и технологий совершенствуются следственные процессы, а также повышается эффективность расследования преступлений. Современные компьютерные технологии поднимают на более высокий уровень работу криминалистов, ускоряя расследование преступлений и облегчая сбор и анализ доказательств.

Среди примеров таких технологий можно назвать автоматизированную уголовную регистрацию, технику для сбора фото-, видео- и аудиозаписей в сборе доказательств, геоинформационные системы для анализа местоположения преступлений и анализ зашифрованных данных.

Правоохранительные органы активно используют различные базы данных для хранения и обработки информации о преступлениях и подозреваемых, что способствует более быстрому раскрытию преступлений. Существует специализированная автоматизированная система следственного комитета МВД РФ, помогающая ускорить расследование преступлений. Дальнейшие перспективы внедрения современных технологий в сфере правопорядка предлагают новые возможности для раскрытия преступлений. Следователи могут использовать различные программные комплексы для извлечения и анализа информации, хранящейся на мобильных устройствах предполагаемых преступников. Компьютерная экспертиза играет особую роль при расследовании преступлений, обнаруживая следы преступлений на носителях информации. Использование современных компьютерных технологий и программных продуктов позволяет с большой эффективностью раскрывать преступления. Применение новейших технологий в сфере следственной деятельности оказывает значительное положительное воздействие на процессы расследования преступлений. С высокой вероятностью можно предположить, что в будущем использование искусственного интеллекта и аналитики данных позволит оперативно и точно выявлять закономерности в различных видах онлайн-коммуникаций киберпреступников, их поведенческих особенностей в сети, раскрывать взаимосвязи между различными событиями, проводить анализ обширных объёмов информации об интернет-пользователях. Применение цифровой криминалистики уже позволяет извлекать и анализировать цифровые доказательства, такие как данные социальных сетей, сообщения, изображения, и видеозаписи, что существенно повышает эффективность методов расследования. Следовательно, в будущем требуется дальнейшее развитие этих методов, включая использование экспертных знаний и навыков сотрудников правоохранительных органов.

Персоналу правоохранительных структур следует активно проводить образовательные мероприятия, направленные на повышение уровня киберграмотности населения, освещать методы защиты от киберугроз и пропагандировать безопасное поведение в Сети. Кроме того, взаимодействие с международными партнёрами в сфере кибербезопасности, обмен информацией и координация действий являются важными для более эффективного противодействия киберпреступности. В настоящее время необходимо разработать систему знаний и провести практическое применение описанных в данной статье баз данных, справочных и образовательных систем. Общие

усилия по раскрытию и противодействию как киберпреступлениям, так и традиционным видам преступлений остаются актуальными задачами в современном информационном обществе. Для эффективного решения данных проблем крайне важно активизировать международное сотрудничество и усилить меры по обеспечению кибербезопасности как на уровне государства, так и в частном секторе.

Сегодня разрабатываются законы, направленные на точную идентификацию пользователей интернета. Социальные сети привязываются к номеру телефона пользователя, рекомендуется указывать реальные имя и фамилию, а для восстановления доступа к аккаунту могут потребовать фото пользователя с его паспортом. А законы, направленные против публикации фейковых новостей в СМИ, подтвердили, что информация о пользователях может быть передана правоохранительным органам. С другой стороны, обязанность хранения этой информации переложили на провайдеров, мобильных операторов и владельцев сервисов, что не всегда реализуется тщательно и правильно. Необходимость хранить эти данные приводит к повышенному расходу ресурсов, которые могли бы применяться для более важной работы. Вся личная переписка, контент отдельных групп, поисковые запросы в социальных сетях передаются сотруднику силовых структур, если он просто проявит к пользователю интерес.

Таким образом, детальное изучение элементов криминалистической характеристики мошенничеств в сети Интернет позволило прийти к выводу о том, что способ преступления является центральным элементом в структуре криминалистической характеристики преступлений как информационного фундамента частных криминалистических методик расследования. Тем не менее важным является изучение всех элементов криминалистической характеристики рассматриваемого преступления в их взаимосвязи для получения полной информационной базы, необходимой для выбора эффективной тактики производства отдельных следственных действий.

Итак, раскрытие киберпреступлений и легализация кибердоходов являются актуальными проблемами в условиях развития информационных технологий и глобализации интернет-пространства. Необходимость разработки универсальных методов противодействия и законодательных актов требует активизации международного сотрудничества и развитие сферы сетевой безопасности на государственном и частном уровнях. Благодаря международному сотрудничеству можно обеспечить обороноспособность и безопасность государства, развитие экономики и социальной сферы без вмешательства интернет-мошенников. В марте 2025 года по итогам заседания коллегии МВД России было объявлено, что борьба с IT-преступностью является одним из основных направлений работы органов внутренних дел на ближайшее время. Именно поэтому преступность в интернете – это большая проблема каждого современного государства [7. с. 66]. Преступность в интернете будет искоренена лишь в том случае, если абсолютно вся Глобальная сеть по всему миру будет контролироваться одной организацией, что на практике невозможно.Таким образом, обстановка с преступностью в сети Интернет требует активных мер по профилактике и предупреждению.

Главными направлениями профилактики являются:

– подготовка кадров;
– вопрос наступления ответственности.

Доскональное расследование дел и предание наказанию виновных – это одна из тенденций профилактики преступлений этой направленности. Важно наказать не только непосредственных исполнителей, но и всех субъектов преступной цепочки, что на практике довольно затруднительно. Обучение и подготовка специалистов в области киберпреступлений для правоохранительных органов имеют свои особенности. Для

эффективного противодействия киберпреступности необходимы специализированные знания. Например, сотрудники должны знать методы защиты от хакерских атак, процедуры обработки и анализа электронных улик. Кроме того, важно использовать инновационные методы обучения. Например, симуляторы атак и облачные платформы позволяют проводить практические упражнения в реальном времени, что помогает улучшить навыки реагирования на киберугрозы. Междисциплинарный подход также играет важную роль в обучении специалистов. Например, в сфере киберпреступлений часто требуется взаимодействие с экспертами в области юриспруденции, психологии и киберэтики. Знание различных аспектов позволяет сотрудникам правоохранительных органов более эффективно расследовать киберпреступления и принимать интегрированные решения. Наконец, обучение специалистов в области киберпреступлений должно учитывать международное сотрудничество и обмен опытом. Глобализация киберугроз требует совместных усилий правоохранительных органов разных стран. Например, участие в международных тренингах и семинарах по обмену опытом помогает специалистам быть в курсе последних тенденций в области кибербезопасности. Таким образом, учёт всех перечисленных особенностей в обучении и подготовке специалистов в области киберпреступлений для правоохранительных органов является ключевым фактором в борьбе с киберпреступностью.

1. Струков А. Е. Понятие и способы мошенничества // Вестник магистратуры. 2022. № 1-2(124). С. 86–88.
2. Вакула А. И., Плиев И. М. Интернет как очевидная угроза информационной безопасности личности // Авакьяновские чтения. Сборник научных статей студентов, магистрантов, преподавателей, II Международного молодежного юридического форума. 2019. С. 210–219.
3. Майкулов Ж. Ж. Проблемы криминализации киберпреступлений // Научное сообщество студентов: междисциплинарные исследования: сб. ст. по мат. X междунар. студ. науч.-практ. конф. № 7(10). 34 с.
4. Мошенничество в сфере компьютерной информации: анализ судебной практики // URL: https://pravo163.ru/moshennichestvo-v-sfere-kompyuternoj-informacii-analiz-sudebnoj-praktiki/ (дата обращения: 03.03.2025).
5. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе: дис. ... канд. юрид. наук: Воронеж, 2010. 198 с.
6. Шумилин В. П. Мошенничество в области интернет-банкинга // Научный портал МВД России. 2023. № 3(63). С. 75–80.
7. Матросова Л. Д., Кислицин И. А. Инструменты для поиска оперативно-значимой информации по открытым источникам // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4 (93). С. 65–72.

1. Strukov A. E. Ponyatie i sposoby` moshennichestva // Vestnik magistratury`. 2022. №1-2 (124). S. 86–88.
2. Vakula A. I., Pliev I. M. Internet kak ochevidnaya ugroza informacionnoj bezopasnosti lichnosti // Avak`yanovskie chteniya. Sbornik nauchny`x statej studentov, magistrantov, prepodavatelej, II Mezhdunarodnogo molodezhnogo yuridicheskogo foruma. 2019. S. 210–219.
3. Majkulov Zh. Zh. Problemy` kriminalizacii kiberprestuplenij // Nauchnoe soobshhestvo studentov: mezhdisciplinarny`e issledovaniya: sb. st. po mat. X mezhdunar. stud. nauch.-prakt. konf. № 7(10). 34 s.

4. Moshennichestvo v sfere komp`yuternoj informacii: analiz sudebnoj praktiki // URL: https://pravo163.ru/moshennichestvo-v-sfere-kompyuternoj-informacii-analiz-sudebnoj-praktiki/ (data obrashheniya: 03.03.2025).
5. Agibalov V. Yu. Virtual`ny`e sledy` v kriminalistike i ugolovnom processe : dissertaciya ... kandidata yuridicheskix nauk: Voronezh, 2010. 198 s.
6. Shumilin V.P. Moshennichestvo v oblasti internet-bankinga // Nauchnyj portal MVD Rossii. 2023. № 3 (63). S. 75–80.
7. Matrosova L. D., Kislicin I. A. Instrumenty` dlya poiska operativno-znachimoj informacii po otkry`ty`m istochnikam // Nauchny`j vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk`yanova. 2022. № 4 (93). S. 65–72.

Информация об авторах

Владимир Петрович Шумилин. Доцент кафедры информационных технологий в деятельности органов внутренних дел, кандидат педагогических наук.
Орловский юридический институт МВД России имени В.В. Лукьянова.
302027, Российская Федерация, г. Орел, ул. Игнатова, 2.

Надежда Геннадьевна Шумилина. Доцент кафедры теории и методики начального образования, кандидат педагогических наук.
Орловский государственный университет имени И.С. Тургенева.
302026, Российская Федерация, г. Орел, ул. Комсомольская, 95.

Information about the authors

Vladimir P. Shumilin. Associate Professor of the Department of Information Technologies in the Activities of Internal Affairs Bodies. Candidate of Pedagogical Sciences.
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.
302027, Russia, Orel, Ignatova Str., 2.

Nadezhda G. Shumilina. Associate professor of the department of theory and methodology of primary education. Candidate of Pedagogical Sciences.
Turgenev Oryol State University.
302026, Russia, Orel, Komsomolskaya Str., 95.

Статья поступила в редакцию 09.04.2025; одобрена после рецензирования 20.05.2025; принята к публикации 17.06.2025.
The article was received in the editorial office on 09.04.2025; approved after review on 20.05.2025; accepted for publication on 17.06.2025.