Научная статья
УДК 343.85:343.102
doi: 10.33463/2687-1238.2025.33(1-4).2.253-262

ПОЛУЧЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОТ ОРГАНИЗАТОРОВ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ: ПРАВОВЫЕ, ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ И НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ

Владимир Викторович Петров[1]
[1] Академия ФСИН России, г. Рязань, Россия, ess-rzn@mail. ru

Аннотация. В статье уточняются понятийные характеристики, правовые, организационные вопросы процесса получения компьютерной информации в оперативно-розыскной деятельности от организаторов распространения информации в сети Интернет. Такие действия могут осуществляться в рамках оперативно-розыскного мероприятия «Получение компьютерной информации». Данный вид оперативно-розыскного мероприятия в уголовно-исполнительной системе востребован для выявления преступлений террористического характера и экстремистской направленности, розыска лиц, уклоняющихся от отбывания наказания, а также при раскрытии преступлений коррупционной направленности.

Ключевые слова: организаторы распространения информации, оперативно-розыскная деятельность, оперативные подразделения, получение компьютерной информации, уголовно-исполнительная система

Для цитирования
Петров В. В. Получение компьютерной информации от организаторов распространения информации в сети Интернет: правовые, организационные аспекты и направления использования в уголовно-исполнительной системе // Человек: преступление и наказание. 2025. Т. 33(1–4), № 2. С. 253–262. DOI: 10.33463/2687-1238.2025.33(1-4).253-262.

Человек: преступление и наказание. 2025. Т. 33(1–4), № 2. ISSN 1999-9917 (print). ISSN 2687-1238 (online)
Man: crime and punishment, 2025, vol. 33(1–4), iss. 2, ISSN 1999-9917 (print), ISSN 2687-1238 (online)

Original article

OBTAINING COMPUTER INFORMATION FROM ORGANIZERS OF INFORMATION DISSEMINATION ON THE INTERNET: LEGAL, ORGANIZATIONAL ASPECTS AND DIRECTIONS OF USE IN THE PENAL SYSTEM

Vladimir Viktorovich Petrov[1]
[1] Academy of the FPS of Russia, Ryazan, Russia, ess-rzn@mail. ru

Abstract. The article clarifies the conceptual characteristics, legal, and organizational issues of the process of obtaining computer information in operational investigative activities from organizers of information dissemination on the Internet. Such actions can be carried out as part of the operational search event "Obtaining computer information". This type of operational search activity in the penal system is in demand for the detection of crimes of a terrorist nature and extremist orientation, the search for persons evading punishment, as well as for the detection of corruption-related crimes.

Keywords: organizers of information dissemination, operational investigative activities, operational units, obtaining computer information, penal system

For citation
Petrov, V. V. 2025, 'Obtaining computer information from organizers of information dissemination on the Internet: legal, organizational aspects and directions of use in the penal system', *Man: crime and punishment,* vol. 33(1–4), iss. 2, pp. 253–262, doi: 10.33463/2687-1238.2025.33(1-4).2.253-262.

Актуальность темы исследования обусловлена следующими обстоятельствами.

1. В условиях, когда лица, содержащиеся в учреждениях уголовно-исполнительной системы (УИС), имеют доступ к средствам связи, использование информационно-телекоммуникационных технологий (ИТТ) для совершения преступлений становится все более актуальной проблемой. Анализ официальной уголовно-правовой статистики МВД России с 2020 по 2023 год показывает высокие показатели преступлений, совершенных с ИТТ или в сфере компьютерной информации. Так, в 2021 г. доля таких преступлений составила 1,4 %[1] от общего числа зарегистрированных преступлений, 2022 г. – 0,8 %[2], в 2023 г. – 29,7 %[3]. Приведенные данные свидетельствуют о необходимости принятия дополнительных мер по фиксации использования ИТТ в преступных целях. Развитие ИТТ в последнее десятилетие характеризуется быстрыми темпами роста и инновациями, которые изменили многие аспекты жизни общества, вследствие чего наблюдается рост количества преступлений, совершенных с использованием ИТТ.

[1] См.: Состояние преступности в России за январь – декабрь 2021 г. URL: https://мвд.рф/reports/item/28021552 (дата обращения: 15.08.2024).
[2] См.: Состояние преступности в России за январь – декабрь 2022 г. URL: https://мвд.рф/reports/item/35396677 (дата обращения: 15.08.2024).
[3] См.: Состояние преступности в России за январь – декабрь 2023 г. URL: https://мвд.рф/reports/item/35396677 (дата обращения: 15.08.2024).

2. Несмотря на то что развитие технологий в целом повлекло за собой ряд положительных изменений в обществе, таких как рост числа интернет-пользователей, развитие социальных сетей и онлайн-торговли, а также увеличение количества устройств, подключенных к сети Интернет, сформировалась благоприятная почва для развития преступности и других форм преступной деятельности, связанной с использованием ИТТ.

3. В современных реалиях формируются новые вызовы, обусловленные развитием ИТТ. Противоправная деятельность осужденных, содержащихся под стражей, все чаще связана с использованием различных ИТТ, таких как мобильные телефоны, ноутбуки, планшеты и другие устройства. Несмотря на то что использование таких устройств лицами, содержащимися в учреждениях УИС, запрещено, все чаще отмечаются случаи их скрытного использования в преступных целях, в том числе для совершения правонарушений за пределами учреждений.

Одной из основных задач оперативно-розыскной деятельности (ОРД) в УИС является своевременное принятие эффективных мер для выявления и предотвращения использования осужденными ИТТ в преступных целях. Таким образом, актуальность темы исследования обусловлена ростом числа противоправных деяний с использованием ИТТ, таких как мошенничество, кража, распространение запрещенных материалов, что требует принятия эффективных мер по предотвращению и раскрытию таких преступлений.

Одним из ключевых направлений улучшения информационного обеспечения ОРД, в том числе и в УИС, является получение компьютерной информации в сети Интернет, что позволит оперативным подразделениям получать необходимую информацию о преступной деятельности и принимать меры по ее предотвращению.

В настоящее время особо актуален вопрос поиска новых способов, используемых в ОРД, которые позволяют наиболее эффективно бороться с теми вызовами со стороны преступности, которые стоят перед оперативными подразделениями УИС. Такими средствами могут стать организаторы распространения информации (ОРИ) в сети Интернет, которые могут играть важную роль в обеспечении безопасности и правопорядка в УИС. По своему свойству ОРИ обязаны предоставлять информацию о пользователях и их деятельности в Интернете по запросу уполномоченных органов. Это дает возможность оперативным подразделениям получать необходимую информацию о преступной деятельности и принимать меры по предотвращению совершения новых преступлений.

Данное исследование опирается на широкий спектр источников, включая нормативно-техническую и инструктивно-методическую документацию, результаты научных исследований. Эти источники позволяют более глубоко пониматьпроблемы, связанные с оперативно-розыскной деятельностью, и найти новые подходы к их решению.

В связи с упомянутой тенденцией к развитию новых технологий дистанционного получения информации в сетевых ресурсах и криминальной заинтересованности к ним той части общества, которая имеет преступные намерения, все чаще возникает необходимость применения адекватных оперативно-розыскных мероприятий (ОРМ) и соответствующих средств ОРД в борьбе с преступностью в информационно-телекоммуникационной среде [1, с. 542]. Важное значение имеет ОРМ «Получение компьютерной информации» в сети Интернет, используя организаторов распространения информации.

Несмотря на то что применяемый перечень ОРМ является единым и общим для всех субъектов ОРД, в УИС такое мероприятие, как Получение компьютерной информации, указанное в ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-

розыскной деятельности» (далее – Закон об ОРД), до настоящего времени не нашло практического применения и требует подробного изучения. Ведь часто недостаточно обладать специальными полномочиями, которые определены действующим законодательством, однако не урегулированы в полной мере в контексте ведомственных нормативно-правовых актов. Много споров вызывает и тот факт, что Федеральная служба исполнения наказаний наделена государством специальными полномочиями, дающими право осуществлять ОРД и проводить в том числе ОРМ «Получение компьютерной информации».

Такое средство получения компьютерной информации, как организаторы распространения информации может применяться исключительно в рамках ОРМ, а значит, с использованием возможностей и ресурсов, указанных в ч. 4 ст. 6 Закона об ОРД в строгом соблюдении требований межведомственных нормативных актов, а также соглашений между субъектами ОРД.

Понятие «организатор распространения информации» впервые появилось в российском законодательстве в 2014 г., когда была введена ст. 10.1 в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Исходя из норм статьи организатором распространения информации в сети Интернет считается юридическое или физическое лицо, которое осуществляет свою деятельность по обеспечению работы информационных систем и программ для электронных вычислительных машин, предназначенных для приема, передачи, доставки и обработки электронных сообщений пользователей сети Интернет. Согласно данному Федеральному закону под понятием «информационная система» понимается набор данных, хранящихся в базах, а также информационные технологии и технические средства, обрабатывающие такую информацию.

Виды хранимой информации в сети Интернет урегулированы тем же Федеральным законом, а организаторы распространения информации в сети Интернет обязаны в установленные сроки обеспечить хранение такой информации, которая может быть следующих видов:

– информация о действиях пользователей в сети Интернет, таких как прием, передача, доставка или обработка голосовых сообщений, текстов, изображений, звуков, видео или других электронных сообщений, а также информация о самих пользователях, которая хранится в течение одного года с момента завершения этих действий.

– текстовые сообщения, голосовые сообщения, изображения, звуки, видео и другие электронные сообщения пользователей сети Интернет, которые сохраняются в течение шести месяцев с момента завершения их приема, передачи, доставки или обработки.

Изучая российское законодательство, регламентирующее данную деятельность, можно сделать вывод о том, что организаторы распространения информации обязаны хранить записи голосовых переговоров пользователей в течение шести месяцев с момента их обработки, хотя законодательно нет конкретной нормы, указывающей на этот срок именно для голосовых разговоров, а в Федеральном законе от 7 июля 2003 г. № 126-ФЗ «О связи» и Федеральном законе «Об информации, информационных технологиях и о защите информации» устанавливаются общие правила хранения информации о пользователях и контенте. Согласно этим правилам информация о пользователях хранится год, а контент, включая тексты, изображения, видео, аудио, – шесть месяцев.

Следует отметить, что ОРИ обязаны предоставлять накапливаемую ими информацию лишь уполномоченным на это государственным органам, осуществляющим оперативно-

розыскную деятельность или обеспечивающим безопасности Российской Федерации, в случаях, установленных федеральными законами. Постановлением Правительства Российской Федерации от 31 июля 2014 г. № 743 «Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети Интернет с уполномоченными государственными органами, осуществляющими ОРД или обеспечение безопасности Российской Федерации» утверждены специальные правила взаимодействия ОРИ в сети Интернет с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечивающими безопасность Российской Федерации.

Вместе с тем целесообразно уточнить, каким конкретно субъектам ОРД и в рамках каких оперативно-розыскных мероприятий ОРИ должны предоставлять информацию.

Для начала ответим на вопрос: «Кто определяет в деятельности организаций, рассматриваемых в данной статье, признаки ОРИ?

По нашему мнению, существует два способа. К первому способу относятся случаи, когда юридические и физические лица самостоятельно признают себя организаторами распространения информации в сети Интернет и уведомляют об этом Роскомнадзор, который, в свою очередь, вносит запись в соответствующий реестр ОРИ. Второй способ – случаи, когда регуляторы [Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор или ФСБ России)] могут уведомить юридических и физических лиц о том, что их деятельность подпадает под определение ОРИ и соответственно подлежит правовому регулированию в указанной правовой области.

Более подробно необходимо остановиться на вопросе, кто же из субъектов ОРД получает необходимую информацию от ОРИ. Ответ на этот вопрос содержится в приказе Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29 октября 2018 г. № 571 «Об утверждении Требований к оборудованию и программно-техническим средствам, используемым организатором распространения информации в сети Интернет в эксплуатируемых им информационных системах, для проведения уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, мероприятий в целях реализации возложенных на них задач». В п. 4 указанных Требований определено, что поиск, обработка и передача на пункт управления уполномоченного подразделения органа Федеральной службы безопасности данных, хранимых в информационных системах ОРИ и программно-технических средств (ПТС) ОРИ, при их реализации осуществляются с использованием таких средств по запросу уполномоченного подразделения органа Федеральной службы безопасности или в автоматическом режиме, то есть формируется понимание процесса и ведомственными актами урегулирована процедура подключения информационных систем ОРИ к пульту управления органа Федеральной службы безопасности.

Для понимания процесса деятельности крупных ОРИ, которые внесены в реестр Роскомнадзора, рассмотрим некоторые из них.

Head Hunter (номер в реестре: 360-РР) – это одна из крупнейших онлайн-платформ для поиска работы и подбора персонала в России и странах СНГ. Основанная в 2000 г., она предоставляет широкий спектр услуг как для соискателей, так и для работодателей.

Авито (номер в реестре: 145-РР) – это одна из крупнейших онлайн-платформ для размещения объявлений в России. Основанная в 2007 г., она предоставляет

пользователям возможность покупать и продавать товары и услуги в различных категориях.

Яндекс – одна из крупнейших IT-компаний в России, предоставляющая широкий спектр интернет-услуг и продуктов:

– заправки Яндекс (номер в реестре: 419-РР) – это сервис, предоставляемый Яндексом для удобного поиска и оплаты заправок автомобилей;

– Яндекс.Драйв (номер в реестре: 420-РР) – это сервис каршеринга от Яндекса, предоставляющий возможность аренды автомобилей на короткий срок;

– Яндекс.Доставка (номер в реестре: 421-РР) – это сервис от Яндекса, предоставляющий услуги доставки товаров и еды;

– Яндекс.Афиша (номер в реестре: 423-РР) – это сервис от Яндекса, предоставляющий информацию о культурных и развлекательных мероприятиях;

– Яндекс.Здоровье (номер в реестре: 427-РР) – это сервис от Яндекса, предоставляющий пользователям доступ к медицинским услугам и информации о здоровье;

– Яндекс.ОФД (номер в реестре: 428-РР) – это сервис от Яндекса, предоставляющий услуги оператора фискальных данных (ОФД) для бизнеса;

– Яндекс.Такси (номер в реестре: 328-РР) – это сервис от Яндекса, предоставляющий услуги такси и перевозок;

– Яндекс.Лавка (номер в реестре: 329-РР) – это сервис от Яндекса, предоставляющий услуги быстрой доставки продуктов и товаров первой необходимости;

– Яндекс.Go (номер в реестре: 330-РР) – это единое приложение от Яндекса, объединяющее несколько сервисов для удобного передвижения и заказа услуг;

– Mail.Yandex.ru (номер в реестре: 1-РР) – это почтовый сервис, предоставляемый компанией Яндекс;

– ВКонтакте (номер в реестре: 4-РР) – это одна из крупнейших социальных сетей в России и странах СНГ;

– Telegram (номер в реестре: 90-РР) – это популярный мессенджер, который предоставляет пользователям множество функций для общения и обмена информацией;

– ТамТам (номер в реестре: 5-РР) – это мессенджер, разработанный компанией Mail.ru Group.

Приведенный перечень не является исчерпывающим, нами рассмотрены наиболее часто встречающиеся в повседневной деятельности ресурсы. В настоящее время в реестр ОРИ, который ведет Роскомнадзор, внесены 349 записей.

Для того чтобы понять, как происходит передача необходимой информации от ОРИ к уполномоченным органам, получающим такую информацию, рассмотрим, какими возможностями обладают специализированные программно-аппаратные решения для осуществления рассматриваемых в статье функций. Например, в сети Интернет размещено в качестве коммерческого предложения для организаций, чья деятельность подпадает к ОРИ, таких технических средств, как «СОРМ 571 ПАК ПТС «Январь ОРИ»». Данный комплекс предназначен для обеспечения ОРМ на сервисах ОРИ и владельцев технологических сетей связи, имеющих номер автономной системы. Данное техническое решение может быть реализовано как:

– отдельный программно-аппаратный комплекс;

– отдельный программный модуль в инфраструктуре заказчика;

– сервис, размещаемый в центре обработки данных (ЦОД), обеспечивающий выполнение организационных и технических мер по обеспечению безопасности персональ-

ных данных пользователей в соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119 и приказом ФСТЭК от 18 февраля 2013 г. № 21 и подключаемый к информационным системам заказчика.

Фактически данное оборудование предназначено для работы с субъектами ОРИ, что позволяет выполнять функции по обеспечению ОРД в интернет-системах и сервисах знакомств и общения в социальных сетях, сервисах электронной почты, файловых хранилищах, мессенджерах, интернет-форумах и информационных порталах, игровых сервисах, видеохостингах, интернет-сервисах операторов связи, интернет-сервисах клиентского обслуживания и прочих информационных системах интернет-сервисов, включенных в реестр ОРИ.

Следует отметить, что органам, осуществляющим ОРД, для проведения ОРМ «Получение компьютерной информации» необходимо судебное решение, а также наличие информации о характере деяний, которые по своему свойству должны считаться противоправными, и с условием, что по ним должно осуществляться предварительное следствие, либо составлять действия или события, являющиеся угрозой для военной, экономической, государственной, информационной либо экологической безопасности Российской Федерации.

Для контроля за деятельностью ОРИ в сети Интернет, связанной с хранением информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или других электронных сообщений пользователей сети Интернет и информации об этих пользователях, постановлением Правительства РФ от 8 апреля 2015 г. № 327 утверждены специальные Правила. Данными Правилами на ОРИ также возложен ряд обязанностей, а их деятельность осуществляется в соответствии с установленными требованиями законодательства, такими как обязанность хранения определенной информации и предоставление ее уполномоченным госорганам, осуществляющим ОРД или обеспечивающим безопасность государства. К такой информации относятся данные о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений интернет-пользователей и сведения об этих пользователях. Содержание сообщений пользователей, направляемых или получаемых ими в рамках обмена данными с иными пользователями, сюда не входит.

Одной из проблем при осуществлении функции ОРД, в том числе и в УИС, является анонимное использование сети Интернет. Большие массивы данных, передаваемых в системах документальной электросвязи (СДЭС), по нашему мнению, затрудняют изобличение лиц, причастных к преступлениям террористического характера и экстремистской направленности, выявление средств связи, используемых данной категорией лиц как инструмента для осуществления своей противоправной деятельности.

Оперативное и достоверное получение важной информации является ключевым фактором в достижении цели проводимых оперативно-розыскных мероприятий, которая заключается в установлении местонахождения и задержании разыскиваемых лиц. Для повышения результативности розыскной работы необходимо совершенствовать практику применения оперативно-розыскных методов и средств, улучшить качество работы и оптимизировать процессы розыска осужденных, уклоняющихся от отбывания уголовного наказания [2, с. 163].

Под рассматриваемыми техническими каналами понимаются средства связи, способные передавать или принимать знаки, сигналы, излучение или голосовую информацию,

а также письменный текст, изображения и звуки или сообщения любого рода посредством радиосистем, проводных, оптических и других электромагнитных систем [3, с. 127].

Нельзя не остановиться на средствах, служащих основой для рассматриваемого ОРМ, которые представляют собой системы технических средств по обеспечению оперативно-розыскных мероприятий (СОРМ) и позволяют получать компьютерную информацию в процессе предоставления услуг передачи данных и телематических служб, включая сеть Интернет, на оборудовании организаций, предоставляющих услуги связи [3, с. 128]. В таких системах выполняется фиксация и контроль в процессе использования СОРМ за передачей факсимильной, телеграфной и иных видах документальных сообщений, а также обмена такими данными между электронно-вычислительными машинами информацией, передаваемой по пейджинговым и иным радио и проводным каналам [3, с. 127–128].

Необходимо уточнить, что рассматриваемые ОРМ и информация, находящаяся у ОРИ, является информацией, сохранность которой гарантируется Конституцией РФ, а право на тайну телефонных переговоров, переписку, почтовые отправления, телеграфных и иных сообщений, включая получение компьютерной информации, передаваемых по сетям электросвязи и сетям почтовой связи, может быть ограничено только уполномоченными подразделениями субъектов ОРД в рамках законодательства Российской Федерации.

Проведение оперативно-розыскных мероприятий с использованием ОРИ может также помочь бороться с еще одной комплексной проблемой – побеги из учреждений УИС. Когда заключенные совершают побег, они не только избегают ответственности, но и создают угрозу для общества. Нападения на охрану, убийства и захват заложников – это только некоторые из негативных последствий побегов. Кроме того, побеги могут подорвать принцип неотвратимости наказания и создать впечатление, что осужденные могут избежать ответственности, поэтому принятие эффективных мер по предотвращению побегов и обеспечение общественной безопасности является крайне важным [4, с. 468].

Совершенствование технологий безопасности в УИС является приоритетным направлением развития. Для этого необходимо разработать и внедрять инновационные решения, направленные на повышение эффективности ОРД и улучшение качества применения оперативно-розыскных методов и средств. Такой процесс не должен ограничиваться оптимизацией систем и средств охраны, надзора и контроля для достижения максимальной безопасности в УИС. Все новые методы и средства требуют тесного сотрудничества между теоретиками и практиками, а также нуждаются в постоянном мониторинге и оценке результатов [5, с. 404].

Цифровая трансформация оперативно-розыскной деятельности – это комплексный процесс, который включает в себя несколько ключевых компонентов. Он предполагает создание цифровой инфраструктуры, которая обеспечивает электронное взаимодействие между субъектами и участниками оперативно-розыскной деятельности, а также автоматизацию процессов сбора, обработки и выдачи оперативно-розыскной информации. Это позволяет принимать решения на основе цифровых данных в реальном времени и использовать интеллектуальные цифровые технологии для повышения эффективности оперативно-розыскной деятельности [6, с. 98–99].

На основе изложенного сделаем следующие теоретически-прикладные выводы и предположения.

1. В результате проведения оперативно-розыскных мероприятий по получению компьютерной информации от организаторов распространения информации для выпол-

нения задач оперативно-розыскной деятельности возможно выявлять средства связи, используемые в качестве инструмента в своей противоправной деятельности подозреваемыми, обвиняемыми и осужденными за преступления террористической направленности и экстремистского характера, которые не отказались от преступной деятельности, продолжают совершать их скрытно, незаконно используя для этого современные технические средства и системы. Такие мероприятия прежде всего нацелены на контроль за оперативной обстановкой в учреждениях УИС, а также документированием противоправной деятельности осужденных и лиц, содержащихся под стражей за преступления террористического характера и экстремистской направленности.

2. Для контроля за оперативной обстановкой в учреждениях УИС, выявления преступных намерений и радикальных течений оперативные подразделения должны своевременно проводить необходимые и наиболее подходящие оптимальные в каждом конкретном случае оперативно-розыскные мероприятия, включая оперативно-розыскное мероприятие «Получение компьютерной информации». Возможность получения компьютерной информации от организаторов распространения информации может быть инструментом, позволяющим контролировать оперативную обстановку, вследствие чего может достигаться снижение числа правонарушений и других преступлений в учреждениях УИС.

3. Проведение оперативно-розыскных мероприятий по получению компьютерной информации способствует расширению возможностей оперативных подразделений при раскрытии преступлений коррупционной направленности.

4. Получаемая информация от организаторов распространения информации может существенно оптимизировать работу подразделений розыска УИС, сократить время на установление местонахождения лиц, совершивших побег из исправительных учреждений.

5. Меры, направленные на применение в практике получения компьютерной информации от организаторов распространения информации, способствуют повышению эффективности оперативно-розыскной деятельности и могут рассматриваться как перспективное направление улучшения оперативно-розыскной деятельности в условиях цифровой трансформации.

Список источников

1. Епифанов С. С. Методологический аспект научного исследования оперативно-розыскной деятельности и средств ее обеспечения // Человек: преступление и наказание. 2022. Т. 30, № 4. С. 534–545.

2. Епифанов С. С., Моисеев Н. Д., Вечкаев Н. С. Совершенствование розыска лиц, уклоняющихся от отбывания наказания: вопросы информационно-аналитического обеспечения // Право и государство: теория и практика. 2021. № 10(202). С. 163–166.

3. Об оперативно-розыскной деятельности : комментарий к Федеральному закону / под ред. В. С. Овчинского. М., 2022. 488 с.

4. Епифанов С. С., Ткаченко И. И., Шерхов Р. Р. Предупреждение и раскрытие побегов осужденных: оперативно-розыскной, юридико-психологический и криминалистические аспекты // Право и государство: теория и практика. 2024. № 4(232). С. 467–471.

5. Епифанов С. С., Моисеев Н. Д., Шерхов Р. Р. Некоторые теоретические и правовые аспекты обеспечения безопасности в уголовно-исполнительной системе // Право и государство: теория и практика. 2023. № 6(222). С. 402–404.

6. Епифанов С. С. Актуальные направления организации оперативно-розыскной деятельности в условиях цифровой трансформации и научно-технического развития //

Уголовно-исполнительная система на современном этапе с учетом реализации Концепции развития уголовно-исполнительной системы Российской Федерации на период до 2030 года : сб. тез. выступ. и докл. участников Междунар. науч.-практ. конф. по проблемам исполнения уголовных наказаний : в 2 т. Рязань : Академия ФСИН России, 2022. С. 98–101.

References

1. Epifanov, S. S. 2022, 'Methodological aspect of scientific research of operational investigative activity and its means of support', *Man: crime and punishment,* vol. 30, iss. 4, pp. 534–545.

2. Epifanov, S. S., Moiseev, N. D. & Vechkaev, N. S. 2021, 'Improving the search for persons evading punishment: issues of information and analytical support', *Law and the State: theory and practice,* iss. 10(202), pp. 163–166.

3. Ovchinsky, V. S. (ed.) 2022, *On operational investigative activities: commentary to the Federal Law,* Moscow.

4. Epifanov, S. S., Tkachenko, I. I. & Sherkhov, R. R. 2024, 'Prevention and detection of escapes of convicts: operational-investigative, legal-psychological and criminalistic aspects', *Law and the State: theory and practice,* iss. 4(232), pp. 467–471.

5. Epifanov, S. S., Moiseev, N. D. & Sherkhov, R. R. 2023, 'Some theoretical and legal aspects of ensuring security in the penal system', *Law and the State: theory and practice,* iss. 6(222), pp. 402–404.

6. Epifanov, S. S. 2022, 'Actual directions of the organization of operational investigative activities in the context of digital transformation and scientific and technical development', in *The penal system at the present stage, taking into account the implementation of the Concept of the development of the penal system of the Russian Federation for the period up to 2030: collection of abstracts of speeches and reports of participants of the International Scientific and Practical Conference on the problems of execution of criminal penalties,* in 2 vols, pp. 98–101, Academy of the FPS of Russia, Ryazan.

Информация об авторе

В. В. Петров – адъюнкт факультета подготовки научно-педагогических кадров.

Information about the author

V. V. Petrov – adjunct of the faculty of scientific and pedagogical personnel training.

Примечание

Содержание статьи соответствует научной специальности 5.1.4. Уголовно-правовые науки (юридические науки).

Статья поступила в редакцию 23.09.2024; одобрена после рецензирования 14.11.2025; принята к публикации 20.05.2025.

The article was submitted 23.09.2024; approved after reviewing 14.11.2025; accepted for publication 20.05.2025.