Дата поступления рукописи в редакцию: 22.05.2025 г.
Дата принятия рукописи в печать: 02.06.2025 г.
DOI: 10.24412/2076-1503-2025-5-562-568

ШЕСТАК Виктор Анатольевич,
доктор юридических наук, доцент,
профессор 25 кафедры (военной администрации,
административного и финансового права)
Военного университета имени князя Александра Невского
Министерства обороны Российской Федерации,
e-mail: viktor_shestak@mail.ru

ХУРТИН Тимофей Игоревич,
бакалавр права, соискатель магистерской степени,
Московская академия Следственного комитета
Российской Федерации имени А.Я. Сухарева,
e-mail: tim.khurt@gmail.com

О ЦЕЛЕСООБРАЗНОСТИ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ РАЗВЕДКИ ПО ОТКРЫТЫМ ИСТОЧНИКАМ (OSINT) В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ЗАКОНОДАТЕЛЬСТВЕ

Аннотация. *Исследование посвящено раскрытию сущность разведки по открытым источникам (OSINT) как метода криминалистики, определению ее цели и задач в роли инструмента в раскрытии, расследовании и и предупреждения преступлений. Целью исследования является подтверждение необходимости нормативного урегулирования разведки по открытым источникам как процессуального действия. Авторы приходят к выводу, что OSINT является необходимым инструментом в раскрытии, расследовании и предупреждении преступлений, поскольку данный метод предполагает возможность получения криминалистически значимой информации ориентирующего и доказательственного характера, которая может быть использована для выдвижения версий, планирования конкретного следственного действия и процесса расследования уголовного дела, прогнозирования возможного противодействия участников уголовного судопроизводства. Анализируя действующее законодательство, авторы приходят к выводу, что использование OSINT не противоречит действующему российскому законодательству и выдвигают предложения о возможности ее правовой регламентации для обеспечения использования уполномоченными лицами в ходе досудебного производства по уголовному делу в современных условиях.*

Ключевые слова*: OSINT, разведка по открытым источникам, цифровая криминалистика, предварительное расследование, доказательства, информационные технологии, публичная информация.*

SHESTAK V.A.,
Professor of the 25th Department
(Military Administration, administrative and financial law)
of the Prince Alexander Nevsky Military University
of the Ministry of Defense of the Russian Federation,
Doctor of Juridical Science,
Moscow

KHURTIN T.I.,
Bachelor of Law, Master's Degree candidate,
A.Ya. Sukharev Moscow Academy of the Investigative Committee
of the Russian Federation

ON THE EXPEDIENCY OF LEGAL REGULATION OF OPEN SOURCE INTELLIGENCE (OSINT) IN CRIMINAL PROCEDURE LEGISLATION

Annotation. *The study is dedicated to uncovering the essence of open source intelligence (OSINT) as a method of criminology, determining its goals and objectives as a tool in the detection, investigation and prevention of crimes. The purpose of the study is to confirm the need for a regulatory regulation of open source intelligence as a procedural action. The authors conclude that OSINT is a necessary tool in the detection, investigation and prevention of crimes, since this method assumes the possibility of obtaining criminalistically significant information of an orientation and evidentiary nature, which can be used to advance theories, plan a specific investigative action and the process of investigating a criminal case, and predict possible opposition from participants in criminal proceedings. Analyzing the current legislation, the authors conclude that the use of OSINT does not contradict the current Russian legislation and put forward proposals on the possibility of its legal regulation to ensure the use by authorized persons during pre-trial criminal proceedings in modern conditions.*

Key words: *OSINT, open source intelligence, digital forensics, preliminary investigation, evidence, information technology, public information.*

Преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, носят преимущественно латентный характер. Такие уголовно наказуемые деяния, как правило, не оставляют видимых следов и сложны с точки зрения раскрытия и собирания доказательственной информации в связи с особенностью объектов – носителей этой информации, широким применением средств удаленного доступа и рядом других причин [1]. Так, согласно сведениям Министерства внутренних дел Российской Федерации в период с 2019 по 2024 года, удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, непрерывно прогрессивно возрастал, и по итогам 2024 года на них приходилось уже почти каждое третье преступление. В связи с ростом числа таких преступлений, многие отечественные исследователей предлагали ввести такое понятие как «киберпреступление», самую широкую дефиницию которому, по нашему мнению, сформулировала С. И. Буз, определившая его как любое преступление, совершенное с помощью информационных технологий (технические средства, так и сама информация и ее носители), либо в информационном пространстве (информационно-телекоммуникационные сети (например, Интернет), компьютерные локальные сети и т.д.) [2].

Распространенность киберпреступлений в преступной среде обусловила необходимость внедрения инновационных инструментов, обеспечивающих эффективность и оперативность их раскрытия, расследования и предупреждения. Таким инструментом может стать и разведка по открытым источникам, или же «OSINT» (от англ. «open source intelligence») – деятельность, приемы которой заключаются в поиске, сборе и анализе информации, добытой в открытых общедоступных источниках. Рассматривая разведку по открытым источникам в сфере деятельности правоохранительных органов, полагаем, целесообразно её определить не только как один из важных и эффективных инструментов поиска и сбора информации, но и как специальный метод криминалистики, представляющий собой способ обнаружении, фиксации и изъятии криминалистически значимой информации, находящейся в источниках открытого доступа, в целях раскрытия, расследования и предупреждения преступлений.

Опираясь на функции правоохранительных органов, в современных условиях полагаем возможным выделить пять основных задач, определяющих сущность информационной разведки по открытым источникам в целях раскрытия, расследования и предупреждения преступлений: идентификация личности; оценка цифрового окружения личности; анализ сферы интересов личности; исследование «цифрового» социального поведения личности; формирование криминалистического портрета личности. Так, к процессу идентификации личности целесообразно отнести сбор и анализ той информации, которая будет представлять личные персональные данные субъекта преступления, а именно: фамилию, имя и отчество, дату рождения, место жительства, сведение об образовании и проч. Не менее важное значение имеют и фотографии, альбомы и изображения, в которых может быть отражена информация ориентирующего, а в отдельных случаях и доказательственного характера. Следовательно, в них может содержаться как образ самого субъекта преступления, так и изображение домов, дворов, построек, общественных мест, которые могут принадлежать тому городу (населенному пункту, поселку и т.д.), в котором непосредственно может дислоцироваться субъект преступления.

Окружение субъекта преступления, которые преимущественно входят в круг его общения, могут находиться во вкладке «друзья» или «подписки». Проанализировав данные этих пользователей, имеется возможность с помощью них выйти

непосредственно на самого субъекта преступления путем обнаружения его окружения в ходе оперативно-разыскной деятельности и, в дальнейшем, проведением допроса, других следственных и иных процессуальных действия для выяснения обстоятельств по делу. Также профили этих пользователей могут служить связующим звеном для определения факта реального пребывания субъекта преступления [3].

Подписки субъекта на группы и сообщества могут характеризовать его сферу интересов, в которых можно найти публикации пользователя-правонарушителя, его участие в обсуждениях, форумах и т.д. Имеющаяся информация может носить ориентирующий характер, с помощью которой есть необходимость проводить оперативно-разыскные мероприятия.

Социальное поведение в сети может включать в себя различные виды коммуникации, которые включают в себя разные речевые продукты, с которые с помощью специальных знаний могут быть использованы для диагностики определенных демографических характеристик автора, которые могут составлять пол, возрастную группу, этническую принадлежность, территориальную принадлежность, уровень речевой культуры и образования; род занятий, профессиональную принадлежность, социальный статус и проч [4]. В частности, речевые продукты также могут носить доказательственный характер, и входить в элемент состава определенного преступления как экстремистско-террористического, так и религиозного характера, следовательно, в случае расследования данных видов преступлений, использование специальных знаний будет необходимо в целях установления всех обстоятельств по уголовному делу, подлежащих доказыванию [5].

Содержание криминалистического портрета личности, полагаем могут составлять сведения о биологических, психологических и социальных свойствах лица, которые могут сыграть роль в проведении определенных следственных действиях или оперативно-разыскных мероприятиях.

Исходя из рассмотренных преимуществ разведки по открытым источникам в деятельности правоохранительных органов и целесообразности ее использования в раскрытии, расследовании и предупреждении не только киберпреступлений, но и преступлений общеуголовной направленности, полагаем, возникает общественная потребность ее внедрения в уголовно-процессуальное законодательство с целью правовой регламентации по следующим причинам.

Во-первых, криминалистически значимая информация, полученная в ходе разведки по открытым источникам, будет выступать связующим логическим звеном для:

– выдвижения криминалистических версий, где из большого массива собранной информации будет выделяться лишь та информация, которая будет иметь значение для расследуемого дела, образуя при этом причинно-следственную связь не только с событием преступления, но и между собой [6];
– прогнозирования возможных действий со стороны преступника или лиц, заинтересованных в исходе дела и активно противодействующих установлению истины по нему [7];
– планирования конкретного следственного действия или всего процесса предварительного расследования в целом, в рамках которого будет определяться необходимость привлечения к их осуществлению сотрудников правоохранительных органов, специалистов и иных лиц, а также ставиться задачи, которые должны быть решены с использованием полномочий в сфере оперативно-разыскной и административной деятельности [8];
– проведения судебных экспертиз, предметом которых будет выступать полученная информация;
– создание криминалистического портрета (профиля) лица, совершившего преступление, который может служить опорой при оперативно-разыскных мероприятиях или следственных действиях [9].

Во-вторых, ряд ученых-криминалистов относит разведку по открытым источникам к функциям оперативно-разыскной деятельности. Так, А.А. Бессонов справедливо полагая, что оперативно-разыскная информация выступает основой получения сведений обо всех обстоятельствах подготавливаемого, совершаемого и совершённого преступления, о причастном к нему лице, подтверждает необходимость использования этого метода оперативными подразделениями [10].

Вместе с тем полагаем, что полномочиями по проведению разведки по открытым источникам должны быть наделены не только уполномоченные должностные лица оперативных подразделений, но и лица, осуществляющие уголовное преследование в ходе досудебного производства по уголовному делу. Как верно отметила Д.Р. Бельдеубаева, при раскрытии и расследовании преступлений необходимо оперативно получать данные для их своевременного анализа и использования в служебной деятельности [11].

Подобный подход уже внедрен в следственную практику органов предварительного расследования в Республике Беларусь, где законодатель проявил инициативу в целях адаптации борьбы с киберпреступлениями и наделил органы предва-

рительного расследования возможностью проведения нового следственного действия – осмотра компьютерной информации. Так, согласно статье 204.1 Уголовно-процессуального кодекса Республики Беларусь [18] осмотр компьютерной информации проводится на месте производства любого следственного действия. Белорусский законодатель, гарантируя обеспечение защиты конституционных прав граждан на тайну частной жизни, а также сведений, составляющих охраняемую законом тайну, или иную информацию, распространение и (или) предоставление которой ограничено, установил, что осмотр компьютерной информации, доступ к которой осуществляется посредством аутентификации пользователя может проводиться только с согласия обладателя информации и в его присутствии. Однако законодатель имплементировал в норму и исключения из этого правила (то есть установил случаи, когда согласие обладателя информации и его присутствие не требуется):

– во-первых, по постановлению следователя, органа дознания с санкции прокурора или его заместителя;
– во-вторых, в случаях, не терпящих отлагательства, осмотр компьютерной информации может быть проведен по постановлению следователя, органа дознания без санкции прокурора с последующим направлением ему в течение 24 часов сообщения о проведенном осмотре;
– в-третьих, осмотр компьютерной информации, хранящейся в компьютерной системе, сети или на машинных носителях, изъятых при производстве процессуальных действий, санкционированных прокурором, проводится без санкции прокурора.

Кроме того, в ходе осмотра компьютерной информации следователем, органом дознания могут производиться действия, предусмотренные функционалом информационных систем, информационных ресурсов, а также использоваться научно-технические средства, оборудование, аппаратура, приборы, компьютерные программы.

При этом законность действий обеспечивается обязательным составлением протокола о проведении осмотра компьютерной информации, в котором должны быть указаны использованные научно-технические средства, оборудование, аппаратура, приборы, компьютерные программы и описаны порядок осуществления доступа к компьютерной информации, произведенные в ходе осмотра действия и полученные результаты.

Рассматривая вопрос о целесообразности внедрения возможности проведения разведки по открытым источникам в процессуальные полномочия лица в ходе досудебного производства по уголовному делу, нельзя не упомянуть тот факт, что не является проблемой переквалификация и переобучение таких лиц методу разведки по открытым источникам, так как необходимые специальные знания в области данной деятельности почти не требуются – следователям (дознавателям), осуществляющим предварительное расследование, понадобится небольшой промежуток времени для изучения основных приемов, которые будут включать в себя технические аспекты работы с основными базами данных и целенаправленными инструментами. В свою очередь, А.Г. Качалов пришел к выводу, что такая образовательная программа должна включать в себя изучение лишь тех вопросов, которые связаны с обучением принципам оптимизации и поискового продвижения веб-ресурсов, в том числе использование открытых поисковых технологий в сети «Интернет», и изучение различных инструментов для управления индексацией сайтов [12]. В целях обеспечения реализации данных знаний достижение полной эффективности использования OSINT останется за профессиональными качествами сотрудников, поскольку метод интернет-разведки построен на умении анализа и синтеза, логическом мышлении и знании психологии, которыми должен обладать обычный рядовой сотрудник следственных органов [13].

Отметим, что ключевое отличие OSINT от других форм разведки, заключается в том, что результатом её функционирования является информация, добытая непосредственно только из открытых источников без нарушения законодательства [14]. Вместе с тем отечественная правовая система не будет противоречить внедрению в российский уголовный процесс соответствующего следственного действия, поскольку собирание публичной информации не нарушает конституционные права и свободы граждан. К такому выводу пришла Л.Г. Шобей, анализируя положения действующего национального законодательства России: Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», регулирующие вопросы, связанные с получением, обработкой, передачей и хранением информации, относящейся к физическим лицам; Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»; Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации», регулирующие случаи признания интернет-сайта средством массовой информации; Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе», которые применимы к интернет-отношениям [15].

Вместе с тем еще в 2017 году Арбитражный суд города Москвы определил, что обработка персональных данных допускается в случаях, когда

они доступны неопределенному кругу лиц, имеется согласие владельца данных и сведения предоставлены непосредственно самим субъектом. Суд пришел к выводу о том, что персональные данные являются общедоступными при выполнении двух условий: они предоставлены владельцем и доступны неопределенному кругу лиц. Следовательно, из-за отсутствия согласия владельца персональных данных на размещение сведений о нем в социальных сетях, нельзя их отнести к общедоступным источникам. При этом оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных, в случае его отзыва, только при наличии соответствующих оснований, в частности, для противодействия терроризму или коррупции [19].

Однако в 2020 году Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» был дополнен статьей 10.1, устанавливающей специальные требования и форму получения согласия субъекта на обработку персональных данных, разрешенных для распространения в открытом доступе [20]. Поскольку общедоступные источники персональных данных могут создаваться в целях информационного обеспечения, то все эти данные должны быть в любое время исключены из общедоступных источников по требованию субъекта или по решению суда. Как следствие, использование третьими лицами публичной информации, размещенной в сети «Интернет», исключает неправомерность, так как субъект заранее не заявил требования об исключении своей персональной информации из открытых источников.

И хотя статья 137 Уголовного кодекса Российской Федерации устанавливает уголовную ответственность за незаконное собирание или распространение информации о частной жизни лица без его согласия либо распространение ее в публичном пространстве [21], но высшая судебная инстанция страны в пункте 2 Постановления своего Пленума № 46 от 25.12.2018 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина» определила, что собирание такой информации не влечет за собой уголовную ответственность, если сведения о частной жизни гражданина ранее стали общедоступными либо были преданы огласке самим гражданином или по его воле [22].

В этой связи, полагаем, что в современных условиях поиск и сбор данных о субъекте в открытых источниках, проводимый уполномоченными лицами в ходе досудебного производства по уголовному делу, не противоречит закону. Да, действительно, следует отличать процесс поиска и сбора информации от ее распространения. Закон не запрещает собирать данные о физическом лице с помощью методов OSINT, однако собранные и аналитически обработанные данные уже представляют собой качественно новую информацию, распространение которой без согласия субъекта может повлечь наступление уголовной ответственности [16]. И здесь, полагаем, нельзя не согласиться с позицией О.В. Химичевой в части того, что при всей очевидной полезности новых технологий для уголовного судопроизводства нельзя забывать про специфичность этого вида государственной деятельности, предполагающей в связи с совершенным преступлением серьезное вмешательство в повседневную жизнь попадающих в его орбиту участников. Именно поэтому все нововведения, какими привлекательными с позиций упрощения и ускорения процессуальных процедур они не были, требуют тщательной проработки с целью недопущения необоснованного, чрезмерного ограничения прав и законных интересов граждан и юридических лиц [17].

Таким образом, полагаем возможным выдвинуть предложения о целесообразности разработки и нормативного закрепления возможности осуществления в ходе досудебного производства по уголовному делу уполномоченными уголовно-процессуальным законом лицами разведки по открытым источникам в целях раскрытия, расследования и предупреждения преступлений.

Список литературы:

[1] Лантух, Э. В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э. В. Лантух, В. С. Ишигеев, О. П. Грибунов // Всероссийский криминологический журнал. – 2020. – Т. 14, № 6. – С. 882-890.

[2] Буз, С. И. Киберпреступления: понятие, сущность и общая характеристика / С. И. Буз // Юристъ-Правоведъ. – 2019. – № 4(91). – С. 78-82.

[3] Сааков, Т. А. Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора / Т. А. Сааков // Законы России: опыт, анализ, практика. — 2020. — № 4. — С. 97-103.

[4] Янгаева, М. О. Использование методов OSINT для криминалистического изучения личности преступника / М. О. Янгаева // Правовое обеспечение суверенитета России: проблемы и перспективы : Сборник докладов XXIV Международной научно-практической конференции и XXIV Международной научно-практической конференции Юридического факультета МГУ им. М.В. Ломоносова в рамках XIII Московской юридической недели. В 4-х частях, Москва, 21–24 ноября 2023

года. – Москва: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. – С. 339-342.

[5] Никишин, В. Д. Место судебной экспертизы материалов религиозного характера экстремистско-террористической направленности в классификации судебных экспертиз / В. Д. Никишин // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2018. – № 7(47). – С. 187-198.

[6] Трухачев, В. В. К вопросу о криминалистической версии / В. В. Трухачев // Общество и право. – 2013. – № 4(46). – С. 179-181.

[7] Замылин, Е. И. Криминалистическое прогнозирование в правоприменительной деятельности / Е. И. Замылин // Общество и право. – 2019. – № 3(69). – С. 85-90.

[8] Козловский П.В. Планирование расследования преступлений / П.В. Козловский // Вестник Волгоградской академии МВД России. – 2019. №3. – С. 90-95.

[9] Янгаева, М. О. Получение криминалистически значимой информации о личности преступника путем поиска по открытым источникам (OSINT) / М. О. Янгаева // Алтайский юридический вестник. – 2023. – № 4(44). – С. 181-190.

[10] Бессонов, А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) / А. А. Бессонов // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Сборник научных трудов Межведомственной научно-практической конференции, Москва, 16 сентября 2022 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2022. – С. 40-45.

[11] Бельдеубаева, Д. Р. Применение OSINT-технологий в качестве повышения эффективности деятельности органов внутренних дел // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сборник материалов Всероссийской научно-практической конференции. Москва, 2020. С. 160-161.

[12] Качалов, А. Г. Подготовка специалистов по работе с открытыми данными в сети интернет (OSINT) в гражданских и ведомственных вузах / А. Г. Качалов, М. М. Лантаев // Юридическая наука: история и современность. – 2021. – № 9. – С. 98-106.

[13] Писарев, Е. В. Оценка значимости криминалистической информации / Е. В. Писарев, М. А. Золотов // Вестник Волжского университета им. В.Н. Татищева. – 2018. – Т. 1, № 2. – С. 181-189.

[14] Иванов, В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. 2023. № 1. С. 62–66. С. 63.

[15] Шобей, Л. Г. К вопросу об особенностях правового регулирования общественных отношений, складывающихся в информационно-телекоммуникационной сети «Интернет» / Л. Г. Шобей, К. Е. Григорьев, П. А. Чернова // Балтийский гуманитарный журнал. – 2019. – Т. 8, № 2(27). – С.190-193.

[16] Ельчанинова, Н. Б. Технологии OSINT в оперативно-разыскной деятельности и их законность / Н. Б. Ельчанинова, Н. С. Велигурина // Проблемы информационной безопасности социально-экономических систем : Труды X Международной Юбилейной научно-практической конференции, Симферополь ¾ Гурзуф, 15–17 февраля 2024 года. – Симферополь: ИП Зуева Т.В., 2024. – С. 117-119.

[17] Химичева, О. В. Следственные действия: о цифровой трансформации их производства / О. В. Химичева // Криминологический журнал. – 2023. – № 2. – С. 170-174.

[18] Кодекс Республики Беларусь от 16.07.1999 № 295-З «Уголовно-процессуальный кодекс Республики Беларусь». – Электронный ресурс. – URL: https://etalonline.by/document/?regnum=HK9900295 (дата обращения 30.03.2025).

[19] Решение Арбитражного суда города Москвы от 5 мая 2017 года по делу № А40-5250/17-144-51

[20] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. – Электронный ресурс. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения : 30.03.2025).

[21] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025). – Электронный ресурс. – URL: https://www.consultant.ru/document/cons_ doc_LAW_10699 (дата обращения: 30.03.2025).

[22] Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)». – Электронный ресурс. – URL: https://www.consultant.ru/document/cons_doc_LAW_314616 (дата обращения: 30.03.2025).

Spisok literatury:

[1] Lantux, E`. V. Ispol`zovanie special`ny`x znanij pri rassledovanii prestuplenij v sfere komp`yuternoj informacii / E`. V. Lantux, V. S. Ishigeev, O. P. Gribunov // Vserossijskij kriminologicheskij zhurnal. – 2020. – T. 14, № 6. – S. 882-890.

[2] Buz, S. I. Kiberprestupleniya: ponyatie, sushhnost` i obshhaya xarakteristika / S. I. Buz // Yurist``-Pravoved``. – 2019. – № 4(91). – S. 78-82.

[3] Saakov, T. A. Sudebnaya avtorovedcheskaya e`kspertiza ob``ektov iz cifrovoj sredy` pri ustanovlenii demograficheskix xarakteristik avtora / T. A. Saakov // Zakony` Rossii: opy`t, analiz, praktika. — 2020. — № 4. — S. 97-103.

[4] Yangaeva, M. O. Ispol`zovanie metodov OSINT dlya kriminalisticheskogo izucheniya lichnosti prestupnika / M. O. Yangaeva // Pravovoe obespechenie suvereniteta Rossii: problemy` i perspektivy` : Sbornik dokladov XXIV Mezhdunarodnoj nauchno-prakticheskoj konferencii i XXIV Mezhdunarodnoj nauchno-prakticheskoj konferencii Yuridicheskogo fakul`teta MGU im. M.V. Lomonosova v ramkax XIII Moskovskoj yuridicheskoj nedeli. V 4-x chastyax, Moskva, 21–24 noyabrya 2023 goda. – Moskva: Izdatel`skij centr Universiteta imeni O.E. Kutafina (MGYuA), 2024. – S. 339-342.

[5] Nikishin, V. D. Mesto sudebnoj e`kspertizy` materialov religioznogo xaraktera e`kstremistsko-terroristicheskoj napravlennosti v klassifikacii sudebny`x e`kspertiz / V. D. Nikishin // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). – 2018. – № 7(47). – S. 187-198.

[6] Truxachev, V. V. K voprosu o kriminalisticheskoj versii / V. V. Truxachev // Obshhestvo i pravo. – 2013. – № 4(46). – S. 179-181.

[7] Zamy`lin, E. I. Kriminalisticheskoe prognozirovanie v pravoprimenitel`noj deyatel`nosti / E. I. Zamy`lin // Obshhestvo i pravo. – 2019. – № 3(69). – S. 85-90.

[8] Kozlovskij P.V. Planirovanie rassledovaniya prestuplenij / P.V. Kozlovskij // Vestnik Volgogradskoj akademii MVD Rossii. – 2019. №3. – S. 90-95.

[9] Yangaeva, M. O. Poluchenie kriminalisticheski znachimoj informacii o lichnosti prestupnika putem poiska po otkry`ty`m istochnikam (OSINT) / M. O. Yangaeva // Altajskij yuridicheskij vestnik. – 2023. – № 4(44). – S. 181-190.

[10] Bessonov, A. A. Ispol`zovanie v raskry`tii prestuplenij informacii iz otkry`ty`x istochnikov informacii (OSINT) / A. A. Bessonov // Aktual`ny`e voprosy` teorii i praktiki operativno-razy`sknoj deyatel`nosti: Sbornik nauchny`x trudov Mezhvedomstvennoj nauchno-prakticheskoj konferencii, Moskva, 16 sentyabrya 2022 goda. – Moskva: Moskovskij universitet Ministerstva vnutrennix del Rossijskoj Federacii im. V.Ya. Kikotya, 2022. – S. 40-45.

[11] Bel`deubaeva, D. R. Primenenie OSINT-texnologij v kachestve povy`sheniya e`ffektivnosti deyatel`nosti organov vnutrennix del // Aktual`ny`e voprosy` e`kspluatacii sistem oxrany` i zashhishhenny`x telekommunikacionny`x sistem: sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii. Moskva, 2020. S. 160-161.

[12] Kachalov, A. G. Podgotovka specialistov po rabote s otkry`ty`mi danny`mi v seti internet (OSINT) v grazhdanskix i vedomstvenny`x vuzax / A. G. Kachalov, M. M. Lantaev // Yuridicheskaya nauka: istoriya i sovremennost`. – 2021. – № 9. – S. 98-106.

[13] Pisarev, E. V. Ocenka znachimosti kriminalisticheskoj informacii / E. V. Pisarev, M. A. Zolotov // Vestnik Volzhskogo universiteta im. V.N. Tatishheva. – 2018. – T. 1, № 2. – S. 181-189.

[14] Ivanov, V. Yu. Ispol`zovanie OSINT v raskry`tii i rassledovanii prestuplenij // Vestnik Ural`skogo yuridicheskogo instituta MVD Rossii. 2023. № 1. S. 62–66. S. 63.

[15] Shobej, L. G. K voprosu ob osobennostyax pravovogo regulirovaniya obshhestvenny`x otnoshenij, sklady`vayushhixsya v informacionno-telekommunikacionnoj seti “Internet” / L. G. Shobej, K. E. Grigor`ev, P. A. Chernova // Baltijskij gumanitarny`j zhurnal. – 2019. – T. 8, № 2(27). – S.190-193.

[16] El`chaninova, N. B. Texnologii OSINT v operativno-razy`sknoj deyatel`nosti i ix zakonnost` / N. B. El`chaninova, N. S. Veligurina // Problemy` informacionnoj bezopasnosti social`no-e`konomicheskix sistem : Trudy` X Mezhdunarodnoj Yubilejnoj nauchno-prakticheskoj konferencii, Simferopol` ¾ Gurzuf, 15–17 fevralya 2024 goda. – Simferopol`: IP Zueva T.V., 2024. – S. 117-119.

[17] Ximicheva, O. V. Sledstvenny`e dejstviya: o cifrovoj transformacii ix proizvodstva / O. V. Ximicheva // Kriminologicheskij zhurnal. – 2023. – № 2. – S. 170-174.

[18] Kodeks Respubliki Belarus` ot 16.07.1999 № 295-Z «Ugolovno-processual`ny`j kodeks Respubliki Belarus`». – E`lektronny`j resurs. – URL: https://etalonline.by/document/?regnum=HK9900295 (data obrashheniya 30.03.2025).

[19] Reshenie Arbitrazhnogo suda goroda Moskvy` ot 5 maya 2017 goda po delu № A40-5250/17-144-51

[20] Federal`ny`j zakon «O personal`ny`x danny`x» ot 27.07.2006 № 152-FZ. – E`lektronny`j resurs. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801 (data obrashheniya : 30.03.2025).

[21] Ugolovny`j kodeks Rossijskoj Federacii ot 13.06.1996 № 63-FZ (red. ot 28.02.2025). – E`lektronny`j resurs. – URL: https://www.consultant.ru/document/cons_ doc_LAW_10699 (data obrashheniya : 30.03.2025).

[22] Postanovlenie Plenuma Verxovnogo Suda RF ot 25.12.2018 № 46 «O nekotory`x voprosax sudebnoj praktiki po delam o prestupleniyax protiv konstitucionny`x prav i svobod cheloveka i grazhdanina (stat`i 137, 138, 138.1, 139, 144.1, 145, 145.1 Ugolovnogo kodeksa Rossijskoj Federacii)». – E`lektronny`j resurs. – URL: https://www.consultant.ru/document/cons_doc_LAW_314616 (data obrashheniya: 30.03.2025).