Дата поступления рукописи в редакцию: 03.07.2026 г.
Дата принятия рукописи в печать: 01.09.2026 г.
DOI: 10.24412/2224-9133-2026-8-234-241

ТАРАСОВ Александр Анатольевич,
старший преподаватель Департамента уголовного права, процесса и криминалистики Факультета права Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ), ORCID:0000-0078-9276-5211, ResearcherID: T-8912-2023, Scopus AuthorID: 82640173651, e-mail: tarasov.aa@hse.ru

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЕ МЕТОДОВ OSINT

Аннотация. *В статья показаны результаты комплексного исследования уголовно-правовых рисков и вызовов, возникающих в результате криминального использования аналитических инструментов разведки по открытым источникам (OSINT).*

Автор раскрывает уникальный двойственный характер OSINT-технологии, являющейся законным средством сбора, анализа данных для расследований и журналистики, одновременно криминализирующейся в современных условиях. Инструменты поиска по открытым источникам все чаще адаптируются преступным сообществом для подготовки таргетированных фишинговых атак, социальной инженерии, доксинга, незаконного оборота персональных данных и конфиденциальной информации, а также кибермошенничества и вовлечения в террористическую деятельность. В статье сделана попытка классификация OSINT-методов, применяемых в преступной деятельности. Сформулированы предложения по совершенствованию уголовного законодательства. Автор акцентирует внимание на нормативных пробелах и межотраслевых коллизиях, которые сопровождают процесс юридической оценки противоправного использования открытых сведений, разграничивая легитимный поиск информации от уголовно наказуемых деяний. На основе обобщения правоприменительной практики обосновывается необходимость введения квалифицирующего признака "с использованием методов OSINT". Аргументирована целесообразность модернизации уголовно-правовых норм, регламентирующих ответственность за нелегальный оборот персональных данных и законодательного закрепления специфики использования методов OSINT в рамках оперативно-розыскных мероприятий.

Ключевые слова: *OSINT; персональные данные; уголовная ответственность; квалификация преступлений; доксинг; кибермошенничество, вовлечение в террористическую деятельность.*

TARASOV Aleksandr Anatolyevich,
Senior Lecturer at the Department of Criminal Law, Procedure and Criminology, Faculty of Law, National Research University Higher School of Economics (HSE University)

CRIMINAL LAW ASPECTS OF UTILIZING OSINT METHODS

Annotation. *The article presents the results of a comprehensive study on criminal law risks and challenges arising from the criminal exploitation of open-source intelligence (OSINT) analytical tools.*

The author reveals the unique dual nature of OSINT technology: while serving as a legitimate means of data collection and analysis for investigations and journalism, it is simultaneously weaponized under modern conditions. Open-source intelligence (OSINT) tools are increasingly being adapted by the criminal community to prepare targeted phishing attacks, social engineering, doxing, trafficking of personal data and confidential information, as well as cyber fraud and recruitment into terrorist activities. The paper provides a classification of OSINT methods utilized in criminal activities and formulates proposals to improve criminal legislation. The author highlights the regulatory gaps and cross-sectoral conflicts that accompany the legal assessment of the unlawful use of open-source data, distinguishing legitimate information retrieval from criminal acts. Based on

the generalization of law enforcement practice, the necessity of introducing a new aggravating circumstance — committing an offense "using OSINT methods" — is substantiated. The study highlights the need to clarify crime elements in the field of illicit personal data trafficking and to separately regulate the use of OSINT in operational-search activities.

Key words: *OSINT (Open-Source Intelligence); personal data; criminal liability; qualification of crimes; doxing; cyber fraud; recruitment into terrorist activities.*

Стремительная цифровизация современного общества не только открывает новые перспективы развития, но и формирует беспрецедентные угрозы безопасности. Одним из таких вызовов выступает криминальная эксплуатация методов разведки по открытым источникам (OSINT). Следует отметить, что изначально данная технология создавалась и использовалась исключительно в легальном сегменте для журналистских расследований и в целях обеспечения корпоративной безопасности. В настоящее время сбор общедоступных данных из социальных сетей, форумов, государственных реестров и других открытых ресурсов стал для злоумышленников удобным инструментом подготовки и совершения преступлений, от фишинговых атак и социальной инженерии до шантажа и мошенничества [1, с. 98].

Актуальность исследования обусловлена тем, что криминальное использование методов OSINT обеспечено колоссальным массивом утекших сведений. По данным экспертных центров, объем похищенных персональных данных граждан России увеличился на 70%, а общий объем утечек за последние три года превысил 4,5 млрд записей. Накопление указанных данных в открытом доступе привело к качественному изменению структуры ИТ-преступности. Так, атаки с применением социальной инженерии стали таргетированными, а наносимый ими финансовый ущерб увеличился на 36%, достигнув 200 млрд рублей, что подтверждает рост криминального использования OSINT-технологий злоумышленниками [17]. На этом фоне отсутствуют четкие правовые критерии, по которым можно было бы квалифицировать сбор открытых данных как часть противоправной деятельности. Действующие нормы Уголовного кодекса РФ, в том числе статьи 137, 138, 272 и другие, не всегда позволяют эффективно пресекать такие действия, т. к. сам по себе сбор информации из открытых источников юридически не считается незаконным. Для правоохранительных органов это создаёт серьёзные трудности. Сложно доказать преступный умысел и привлечь виновных к ответственности. В этой связи на практике это отражается отсутствием единого подхода в судебном сообществе [13, с. 254].

Целью проведенного исследования являлось выявление и систематизация пробелов в уголовном законодательстве Российской Федерации (в части противодействия преступному использованию OSINT, а также выработка научно обоснованных мер по его совершенствованию. В рамках выполнения задач автором проведен анализ теоретических основ OSINT, дана классификация применяемым в киберпреступности методам сбора данных, проанализированы действующие нормы УК России и смежного законодательства, изучена правоприменительная практика по уголовным делам, связанным с преступным использованием открытых данных [1, с. 104]. Методологическую основу исследования составили общенаучные методы познания (анализ, синтез и системный подход), а также специальные юридические методы (сравнительно-правовой и формально-юридический).

В работе использованы материалы уголовных дел, статистика и научные публикации о проблемах OSINT и уголовно-правовой защите информации [11, с. 503]. Новизна исследования заключается в рассмотрении проблемы одновременно с двух сторон: с технической и с правовой. Данный подход помогает связать особенности OSINT с оценкой того, насколько эффективно работают существующие правовые механизмы, и уже на этой основе сформулировать конкретные предложения по изменению уголовного законодательства. В результате изучения сущности и теоретических основ OSINT (Open Source Intelligence) в контексте информационной безопасности установлено, что указанный термин обозначает "деятельность по сбору, обработке и анализу информации, полученной из общедоступных, открытых источников, осуществляемую в целях дальнейшего использования в решении прикладных задач в сфере безопасности, управления, расследования преступлений и административных правонарушений" [2, с. 618]. В данной дефиниции зафиксирован главный теоретический принцип: берётся массив открытых данных, а потом он анализируется для практических целей, из-за чего OSINT получил широкую сферу применения и понятную методологию. При этом мультиформатный характер открытых данных (публикаций, пользовательского контента, метаданных) существенно повышает информативность OSINT-анализа при условии строгого соблюдения правовых и этических стандартов [15, с. 539].

Внутри методологии OSINT исследователи выделяют типологические направления, ориентированные на изучение организаций, отдельных

людей и фрагментов кода, что оптимизирует целеполагание при сборе информации и выбор адекватного аналитического инструментария [5, с. 4]. С помощью OSINT можно собрать о человеке или компании самую разную информацию: имя, фотографии, контакты, местонахождение, профессиональные связи [5, с. 3]. Полученные сведения способны как детерминировать применение социальной инженерии, так и послужить инструментом ее нейтрализации. С одной стороны, правоохранительные органы эффективно имплементируют OSINT для пресечения угроз и розыска преступников, а журналистское сообщество — для верификации информации и дезавуирования фейков, что имеет ключевое значение для обеспечения публичной безопасности [15, с. 542]. С другой стороны, доступность методик и инструментов открытой разведки делает их удобными для злоумышленников: с их помощью можно находить уязвимые цели, готовить точечные атаки через социальную инженерию и заниматься доксингом, то есть несанкционированным сбором и публичным обнародованием персональных данных либо сведений о частной жизни лица без его согласия, осуществляемыми в целях травли, шантажа или подготовки иных преступлений [15, с. 543]. Таким образом, высокая результативность OSINT на фоне колоссального объема открытых данных обусловливают его дуализм и при условии достаточного объема, а также качества информации данная технология одинаково эффективно служит как целям кибербезопасности, так и оптимизации преступных посягательств [5, с. 3]. М. О. Кузнецова отмечает, что "на основе анализа существующих исследований автором осуществлена классификация методов криминального OSINT по двум ключевым группам в целях повышения точности квалификации преступлений и оптимизации их применения в оперативно-розыскной деятельности" [18].

Так, первая группа методов OSINT, применяемых в преступной деятельности, связана со сбором данных о личности, то есть "Персонифицированный OSINT". В нее входит поиск информации в социальных сетях, профессиональных профилях и публичных базах данных. Исследователи подчеркивают, что посредством OSINT о человеке или организации собирается разнородная информация: от имени и контактов до фотоматериалов, пространственных координат и профессионального круга общения [5, с. 3]. В дальнейшем полученные сведения злоумышленники активно используют в социальной инженерии и фишинге. В научной литературе прямо говорится, что "преступники могут использовать OSINT для выявления перспективных мишеней и слабых мест в защите потенциальной жертвы, подготовки к целевым атакам с использованием социальной инженерии, а также в целях доксинга"[15]. Н. Н. Романова отмечает: "Особую опасность представляет целевой фишинг. Для него сначала проводится разведка по открытым источникам, чтобы собрать контекстную информацию о жертве, например о хобби, семье, работе или отпуске, а потом эти детали идут в сценарий атаки" [14].

Вторая категория включает технические методы OSINT, которые направлены на анализ цифровых следов, вредоносного кода и инфраструктуры атак. Это помогает злоумышленникам находить уязвимости и планировать целевые кибератаки. В рамках данного направления можно выделить тип OSINT, ориентированный на анализ фрагментов используемого злоумышленниками программного кода. Анализ фрагментов вредоносного программного обеспечения позволяет идентифицировать автора, его электронную почту или страну происхождения, что помогает установить личность преступника и его мотивы [5]. Для сбора технической информации преступники активно используют пассивную разведку, в том числе сервисы WHOIS, Shodan, картографические инструменты Google Maps. Данный инструментарий позволяет детально изучить цифровую инфраструктуру жертвы без прямого взаимодействия с ней. В научных исследованиях подчеркивается, что любая кибератака начинается с разведывательной аналитической операции, и именно OSINT обеспечивает первоначальное пассивное получение разведданных, которые потом нужны для планирования атаки [15].

Сбор общедоступных данных в рамках OSINT признаётся законным, при условии соблюдения процессуальных норм, при этом информация релевантна и достоверна, а результаты зафиксированы на материальном носителе. При этом использование автоматизированных инструментов требует отдельной правовой регламентации и аккуратной фиксации полученных массивов данных, чтобы потом не возникало сомнений в их допустимости в процессе. Легитимность OSINT подтверждается тем, что его используют в специальных службах, правоохранительных органах, структурах корпоративной безопасности и журналистике. При этом Г. А. Рукавишникова и А. В. Константинов указывают на необходимость соблюдения этических ограничений и проявления особой осторожности при обращении с чувствительными категориями информации [с. 542; 9, с. 51].

Результаты исследования указывают, что преступное использование OSINT начинается в тот момент, когда собранные данные умышленно направляются на подготовку и совершение противоправных деяний (шантаж, мошенничество, вовлечение в террористическую деятельность и другие). В данном контексте деятельность зло-

умышленников полностью выходит за рамки ординарного информационного поиска. Преступники используют методы OSINT как деструктивный инструмент для выявления уязвимостей в защите потенциальной жертвы, реализации доксинга, а также планирования целевых атак с применением социальной инженерии [15, с. 543]. Таким образом, в подобных случаях изначально правомерный пассивный сбор информации трансформируется в стадию приготовления к совершению преступления. Выступает основой для моделирования угроз и планирования атаки. Следовательно, разграничение легитимного и преступного использования сведений должно осуществляться по критериям их последующего целевого назначения и реальной направленности умысла лица.

Регулирование применения OSINT-анализа в уголовном процессе осуществляется Уголовно-процессуальным кодексом Российской Федерации. При этом для признания полученных данных доказательствами требуется соблюдение ряда условий: достоверности и релевантности информации, соблюдения законных прав и интересов лиц, в отношении которых проводится проверка [1, с. 104]. Информация, полученная в результате OSINT-анализа, приобретает правовой статус доказательств после её официальной фиксации в протоколе следственного действия и закрепления на электронном носителе неизменяемого типа [1, с. 99]. На практике это обусловливает необходимость проведения комплекса следственных действий, обязательного составления протоколов и надлежащего оформления всех этапов сбора данных, включая их фиксацию на специальных электронных носителях. Таким образом обеспечиваются сохранность и неизменность доказательственной информации [1, с. 100]. OSINT объединяет разные инструменты и методики обработки открытых источников в единую систему анализа и позволяет следователю получать нужные сведения на всех стадиях доказывания, от выявления факта до представления материала в суде [1, с. 63]. Методы OSINT-анализа интернет-ресурсов применимы при расследовании киберпреступлений, посягательств против личности, а также преступлений в экономической сфере и в области авторских прав [1, с. 99].

Таким образом, цифровая трансформация превратила информацию в базовый ресурс уголовного судопроизводства, существенно повысив значимость открытых источников при раскрытии преступлений, установлении связей и сборе доказательств. При этом в научной литературе исследователями подчеркивается необходимость нормативного регулирования и систематизации процессуальных подходов к оформлению результатов OSINT-анализа, определению критериев их допустимости и выработке методических рекомендаций для следственной и судебной практики [1, с. 98].

Проведённый анализ действующих норм УК РФ и смежного законодательства показывает, что применение OSINT-методов в деятельности правоохранительных органов специально не урегулировано. При этом открытые источники активно используют при расследовании самых разных преступлений, правовая форма такого использования остаётся неопределённой, а критерии допустимости полученных данных как доказательств выглядят размыто. В научной литературе отдельно отмечается растущая роль информационных технологий в современном судопроизводстве и необходимость правового регулирования работы с открытыми источниками данных [1, с. 98]. В условиях правовой неопределенности результаты OSINT-анализа могут быть легко оспорены стороной защиты. Признание полученных сведений допустимыми доказательствами требует соблюдения строгих процессуальных правил, включая фиксацию данных специализированным программным обеспечением и привлечение специалистов. Однако из-за отсутствия профильного регулирования данные требования не систематизированы и применяются правоприменителем по аналогии с осмотром предметов и документов. Только после выполнения формально-процессуальных требований информация, добытая методом OSINT-анализа, приобретает статус допустимого доказательства и может быть использована при расследовании уголовных дел. Кроме того, нормативно не закреплены и критерии достоверности таких сведений (множественность источников, согласованность данных, отсутствие признаков фальсификации), что создает дополнительные сложности в правоприменительной практике. Серьёзной проблемой остаётся и соблюдение баланса между эффективностью OSINT-анализа и защитой законных прав и интересов тех лиц, которых проверяют. Право на свободу информации, закреплённое в Конституции РФ, не является абсолютным и ограничивается необходимостью защищать личную жизнь и государственную безопасность [9, с. 52]. По мере роста возможностей OSINT чаще возникают вопросы защиты интересов граждан и надлежащего уровня охраны персональных данных [14]. Коллизия между публичным интересом в раскрытии информации и частным интересом в сохранении конфиденциальности также требует нормативного разрешения.

Анализ правоприменительной практики демонстрирует эффективность использования методов OSINT при расследовании различных деяний — от экономических до киберпреступлений [1, с. 98]. Вместе с тем неправомерное обращение к общедоступным информационным ресурсам способно повлечь нарушение законодательства

о персональных данных, затронув права на конфиденциальность и неприкосновенность частной жизни. Следовательно, результативность OSINT в следственной практике напрямую зависит от строгого соблюдения процессуальных норм, а также требований к релевантности и достоверности информации, что позволяет обеспечить баланс между эффективностью расследования и защитой прав граждан.

С учетом того, что предварительный сбор сведений о жертве выступает обязательным этапом приготовления к преступлению и существенно повышает его общественную опасность автором предлагается введение в Уголовный кодекс Российской Федерации нового квалифицирующего признака — совершение деяния «с использованием методов OSINT». Данный шаг обоснован, поскольку для широкого спектра посягательств аккумулирование информации о потерпевшем является неотъемлемым элементом приготовления к преступлению [3, с. 125].

А. А. Семочкина утверждает, что законодательная практика и доктрина обусловливают необходимость отказа от формальной дифференциации персональных данных по форме их выражения и точного определения предмета нормы, во избежание ограничения уголовно-правовой квалификации исключительно компьютерной информацией [3, с. 126]. Предложенный квалифицирующий признак позволит разграничить ответственность и учесть более высокую общественную опасность действий, совершённых с применением методов открытого сбора информации, не смешивая их с обычными подготовительными действиями. Вместе с тем расширение системы квалифицирующих признаков обусловливает необходимость незамедлительной конкретизации критериев разграничения преступного использования OSINT и легитимной работы с открытыми источниками и сервисами. В этой связи нельзя не согласиться с предложением Л. Ю. Лариной о расширении системы квалифицирующих признаков состава преступления, предусмотренного ч. 3 ст. 272.1 УК РФ, посредством включения указания на совершение деяния в отношении двух и более лиц, а также в отношении персональных данных, составляющих коммерческую, банковскую или иную охраняемую законом тайну [12, с. 10]. Автор поддерживает мнение Д. С. Корешникова о том, что критерии разграничения законного сбора общедоступной информации и её неправомерного получения также требуют четкой нормативной фиксации, поскольку использование размещенных в сети Интернет данных само по себе не влечет уголовную ответственность при отсутствии признака незаконности их приобретения [10, с. 52].

Таким образом, нормативная регламентация квалифицирующих признаков и внедрение методических рекомендаций для правоприменителей позволят избежать избыточной пенализации и снизить риск избыточной квалификации одних и тех же деяний по нескольким статьям уголовного закона. Реализация данного подхода также требует официальных разъяснений высших судебных инстанций. Помимо квалифицирующего признака, есть смысл ввести и отдельную норму, которая прямо предусматривала бы ответственность за незаконный сбор, хранение и распространение персональных данных, полученных методами OSINT, если эти данные потом планируется использовать для совершения других преступлений. Так, исследователями констатируется необходимость изменить главу 28 УК РФ, включив понятие "киберпреступление" и добавив дополнительные составы [16, с. 151]. Формулировка новой статьи должна опираться на предмет исследования правовых отношений в сфере охраны персональных данных и показывать общественную опасность их незаконного обращения как части подготовки и совершения других посягательств [12, с. 10]. При разработке такой нормы нужно согласовать её с уже действующими составами и предусмотреть соразмерные санкции, чтобы предупредить злоупотребления, но без лишней уголовно-правовой репрессии.

Учитывая, что в доктрине подчеркивается необходимость четкой регламентации правовой формы применения методов OSINT [11, с. 511], автором предлагается нормативно закрепить порядок использования данных действий в Федеральном законе «Об оперативно-розыскной деятельности» для устранения правовой неопределенности и обеспечения процессуальных гарантий. Это позволит согласовать нормы оперативно-розыскного и уголовно-процессуального законодательства, минимизировав риски признания полученных сведений недопустимыми доказательствами по формальным основаниям.

Отсутствие единой методологии в уголовном процессе обусловливает потребность в стандартизации алгоритмов исследования и легитимной фиксации данных при применении автоматизированных инструментов. В этой связи другим необходимым шагом выступает разработка ведомственных нормативных актов субъектов оперативно-розыскной деятельности, регламентирующих фиксацию, оформление и использование результатов OSINT-анализа. Ведомственная регламентация должна аккумулировать требования к протоколированию этапов сбора информации, правила её хранения на электронных носителях и процедуры верификации, что повысит доказательственное значение результатов и защитит права участников судопроизводства.

Развитие автоматизированных OSINT-

инструментов и технологий искусственного интеллекта создаёт почву для появления новых составов преступлений, связанных с массовым сбором и анализом открытых данных. Так, по мнению Н. Н. Романовой, "инструменты искусственного интеллекта, машинного обучения и автоматизации способны сканировать огромные объёмы данных и коммуникаций, довольно точно выявляя связи и риски, которые требуют дальнейшего изучения" [14, с. 138]. Данный инструментарий активно эксплуатируется злоумышленниками для выявления уязвимостей потенциальных жертв, моделирования угроз, планирования атак и реализации доксинга с применением социальной инженерии. Высокая деструктивность указанных методов обусловливает необходимость упреждающего прогнозирования новых форм преступного использования открытых данных и своевременного формирования уголовно-правовых мер противодействия [15, с. 543]. Таким образом, проведённое исследование подтвердило двойственную природу OSINT. С одной стороны, это вполне легитимный инструмент разведки и расследования, потому что речь идёт о работе с общедоступными данными. С другой стороны, те же методы активно используют киберпреступники, когда готовят фишинговые атаки, занимаются социальной инженерией, собирают персональные данные и совершают другие противоправные действия. Разработанная классификация таких методов помогла разложить по полочкам инструментарий злоумышленников и очертить предмет и границы уголовно-правового воздействия.

Анализ уголовного законодательства РФ показал, что действующие нормы, в том числе статьи 137, 138 и 272 УК РФ, не дают чётких критериев, по которым можно квалифицировать сбор общедоступных данных, если он связан с подготовкой или совершением киберпреступлений. Из-за этого возникают пробелы и коллизии. Изучение правоприменительной практики показало, что результаты OSINT-анализа могут быть серьёзным доказательственным материалом при расследовании киберпреступлений. Однако их применение допустимо лишь при строгом соблюдении процессуальных требований к фиксации и оформлению результатов. В условиях отсутствия единообразной судебной практики и специализированного нормативного регулирования эффективность противодействия преступности снижается, что обусловливает необходимость внедрения дополнительных правовых механизмов.

Минимизация выявленных недостатков требует модернизации уголовного законодательства и смежных нормативных правовых актов. Предложенные меры направлены на укрепление безопасности информационной сферы и повышение результативности противодействия киберпреступности.

Список литературы:

[1] Нисневич, А. К. OSINT-анализ сайтов как метод сбора доказательств по уголовным делам / А. К. Нисневич // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. — 2026. — № 2. — С. 98–105. — DOI: 10.56972/2411-1716.2026.2.98..

[2] Аветисян К. Р. Опыт использования OSINT при противодействии преступлениям в сфере IT / К. Р. Аветисян // Образование и право. — 2026. — № 3. — С. 618–622. — DOI: 10.24412/2076-1503-2026-3-618-622..

[3] Семочкина А. А. Уголовно-правовая характеристика незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а равно создания и (или) обеспечения functioning информационных ресурсов, предназначенных для её незаконных хранения и (или) распространения / А. А. Семочкина, Д. И. Изюмский // Судебная экспертиза и исследования. — 2025. — № 2. — С. 121–128. — DOI: 10.5281/zenodo.2025.02.121..

[4] Батоев В. Б. О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности / В. Б. Батоев // Вестник Уфимского юридического института МВД России. — 2023. — № 2 (100). — С. 66–71. — DOI: 10.52180/1995-1639_2023_2_100_66..

[5] Власенко Д. В. Социальная инженерия. Сбор информации о человеке с помощью метода OSINT, его типы, значение и способы защиты / Д. В. Власенко // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. — 2024. — № 2. — С. 2–11. — DOI: 10.24411/2541-9269-2024-2-2..

[6] Тимофеев С. В. К вопросу добывания оперативно значимой информации в сети Интернет: проблемы и пути их решения / С. В. Тимофеев // Криминалистика: вчера, сегодня, завтра. — 2021. — Т. 18, № 2. — С. 111–117. — DOI: 10.24412/2587-9820-2021-2-111-117..

[7] Щепельков В. Ф. Уголовная ответственность за незаконный оборот персональных данных (статья 272.1 Уголовного кодекса Российской Федерации) / В. Ф. Щепельков // Вестник Волгоградской академии МВД России. — 2025. — № 3 (74). — С. 35–42. — DOI: 10.25726/vvd.2025.74.3.005..

[8] Капинус О. С. Цифровизация преступности и уголовное право / О. С. Капинус // Baikal Research Journal. — 2022. — Т. 13, № 1. — URL: brj-bguep.ru (дата обращения: 28.08.2026). — DOI: 10.17150/2411-6262.2022.13(1).25..

[9] Константинов А. В. Правовые и этические основы поиска и анализа информации с помощью методов OSINT / А. В. Константинов // Вестник

Московского университета МВД России. — 2025. — № 3. — С. 51–55. — DOI: 10.24412/2073-0454-2025-3-51-55..

[10] Корешников Д. С. Конкуренция стандартов защиты персональных данных: разграничение статьи 272.1 Уголовного кодекса Российской Федерации и статьи 13.11 Кодекса Российской Федерации об административных правонарушениях / Д. С. Корешников // Правопорядок: история, теория, практика. — 2025. — № 3 (46). — С. 49–54. — DOI: 10.47475/2311-696X-2025-46-3-49-54..

[11] Кочергин Я. А. Использование открытых источников информации (OSINT) в следственной и оперативно-розыскной деятельности / Я. А. Кочергин // Вестник науки. — 2025. — № 5 (86). — С. 503–512. — DOI: 10.24412/2712-8849-2025-586-503-512..

[12] Ларина Л. Ю. Проблемы квалификации преступлений, связанных с незаконным оборотом персональных данных / Л. Ю. Ларина, И. В. Пантюхина // Вестник Югорского государственного университета. — 2026. — № 2. — С. 10–20. — DOI: 10.17816/byusu20260210-20..

[13] Родивилин И. П. Уголовно-правовая характеристика преступлений, связанных с разглашением сведений о гражданах / И. П. Родивилин, В. В. Коломинов // Вестник Восточно-Сибирского института МВД России. — 2024. — № 2 (109). — С. 254–264. — DOI: 10.55001/2312-3184.2024.28.39.023..

[14] Романова Н. Н. Исследование методом расширенного систематического обзора литературы E-SLR проблемы обеспечения безопасности персональных данных при использовании OSINT / Н. Н. Романова, В. В. Грызунов // Вестник Дагестанского государственного технического университета. Технические науки. — 2024. — № 3. — С. 130–144. — DOI: 10.21822/2073-6185-2024-51-3-130-144..

[15] Рукавишникова Г. А. Общая характеристика технологий OSINT на платформе Telegram для использования в получении значимой информации / Г. А. Рукавишникова, П. М. Титов // Вопросы российской юстиции. — 2023. — № 27. — С. 537–546. — DOI: 10.24412/2658-4506-2023-27-537-546..

[16] Христинина Е. В. К вопросу об уголовно-правовом противодействии киберпреступности / Е. В. Христинина // Вестник Сибирского юридического института МВД России. — 2021. — № 2 (43). — С. 150–154. — DOI: 10.51980/2542-1735_2021_2_150..

[17] Число киберпреступлений в России // TAdviser: государственный и корпоративный ИТ-портал. — 2026. — 15 мая. — URL: tadviser.ru (дата обращения: 28.08.2026).

[18] Кузнецова М. О. Тактические особенности расследования преступлений экстремистской направленности, совершенных молодежными неформальными группировками // Вестник Сибирского юридического института МВД России. 2024. № 1 (54). С. 102–107. DOI: 10.51980/2542-1735_2024_1_102..

References:

[1] Nisnevich, A.K. OSINT-analysis of sites as a method of collecting evidence in criminal cases/ A.K. Nisnevich // Bulletin of the Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin. — 2026. — № 2. - S. 98-105. — DOI: 10.56972/2411-1716.2026.2.98..

[2] Avetisyan K. R. Experience in using OSINT in countering IT crimes/K. R. Avetisyan // Education and law. — 2026. — № 3. - S. 618-622. — DOI: 10.24412/2076-1503-2026-3-618-622..

[3] Semochkina A. A. Criminal law characterization of the illegal use and (or) transfer, collection and (or) storage of computer information containing personal data, as well as the creation and (or) provision of functioning information resources intended for its illegal storage and (or) distribution/ A. A. Semochkina, D. I. Izyumsky // Forensic examination and research. — 2025. — № 2. - S. 121-128. — DOI: 10.5281/zenodo.2025.02.121..

[4] Batoev V. B. On the technology of searching for open sources "OSINT" in operational-search activities/V. B. Batoev // Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia. — 2023. — № 2 (100). - S. 66-71. — DOI: 10.52180/1995-1639_2023_2_100_66..

[5] Vlasenko D.V. Social Engineering. Collecting information about a person using the OSINT method, its types, meaning and methods of protection/ D.V. Vlasenko // Mathematical modeling, computer and field experiment in natural sciences. — 2024. — № 2. - S. 2-11. — DOI: 10.24411/2541-9269-2024-2-2..

[6] Timofeev S.V. On the issue of obtaining promptly significant information on the Internet: problems and ways to solve them / S.V. Timofeev // Forensics: yesterday, today, tomorrow. — 2021. - T. 18, NO. 2. - S. 111-117. — DOI: 10.24412/2587-9820-2021-2-111-117..

[7] Schepelkov V.F. Criminal liability for illegal circulation of personal data (Article 272.1 of the Criminal Code of the Russian Federation) V.F. Schepelkov // Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. — 2025. — № 3 (74). - S. 35-42. — DOI: 10.25726/vvd.2025.74.3.005..

[8] Kapinus O.S. Digitalization of Crime and Criminal Law/O.S. Kapinus // Baikal Research Journal. — 2022. - T. 13, NO. 1. - URL: brj-bguep.ru (access date: 28.08.2026). — DOI: 10.17150/2411-6262.2022.13(1).25..

[9] Konstantinov A. V. Legal and ethical

foundations for the search and analysis of information using OSINT methods/A. V. Konstantinov // Bulletin of Moscow University of the Ministry of Internal Affairs of Russia. — 2025. — № 3. - S. 51-55. — DOI: 10.24412/2073-0454-2025-3-51-55..

[10] Koreshnikov D. S. Competition of personal data protection standards: distinction between Article 272.1 of the Criminal Code of the Russian Federation and Article 13.11 of the Code of Administrative Offenses of the Russian Federation/ D. S. Koreshnikov // Law and order: history, theory, practice. — 2025. — № 3 (46). - S. 49-54. — DOI: 10.47475/2311-696X-2025-46-3-49-54..

[11] Kochergin Ya. A. The use of open sources of information (OSINT) in investigative and operational-search activities / Ya. A. Kochergin // Bulletin of Science. — 2025. — № 5 (86). - S. 503-512. — DOI: 10.24412/2712-8849-2025-586-503-512..

[12] Larina L. Yu. Problems of qualification of crimes related to illegal circulation of personal data/ L. Yu. Larina, I.V. Pantyukhina // Bulletin of Ugra State University. — 2026. — № 2. - S. 10-20. — DOI: 10.17816/byusu20260210-20..

[13] Rodivilin I.P. Criminal law characteristics of crimes related to the disclosure of information about citizens / I.P. Rodivilin, V.V. Kolominov // Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. — 2024. — № 2 (109). - S. 254-264. — DOI: 10.55001/2312-3184.2024.28.39.023..

[14] Romanova N. N. Research by the method of an extended systematic review of the E-SLR literature on the problem of ensuring the security of personal data when using OSINT N. N. Romanova, V. V. Gryzunov // Bulletin of Dagestan State Technical University. Technical sciences. — 2024. — № 3. - S. 130-144. — DOI: 10.21822/2073-6185-2024-51-3-130-144..

[15] Rukavishnikova G. A. General characteristics of OSINT technologies on the Telegram platform for use in obtaining significant information / G. A. Rukavishnikov, P. M. Titov // Issues of Russian justice. — 2023. — № 27. - S. 537-546. — DOI: 10.24412/2658-4506-2023-27-537-546..

[16] Khristinina E.V. On the issue of criminal legal counteraction to cybercrime / E.V. Khristinina // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. — 2021. — № 2 (43). - S. 150-154. — DOI: 10.51980/2542-1735_2021_2_150..

[17] Number of cybercrimes in Russia // TAdviser: government and corporate IT portal. — 2026. - May 15. - URL: tadviser.ru (access date: 28.08.2026).

[18] Kuznetsova M. O. Tactical features of the investigation of extremist crimes committed by youth informal groups // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. 2024. № 1 (54). S. 102-107. DOI: 10.51980/2542-1735_2024_1_102..