УГОЛОВНОЕ ПРАВО И ПРОЦЕСС

Дата поступления рукописи в редакцию: 16.02.2026 г.
Дата принятия рукописи в печать: 03.04.2026 г.
DOI: 10.24412/2076-1503-2026-3-618-622

АВЕТИСЯН Карэн Рафаелович,
старший преподаватель кафедры информационных технологий и организации расследования киберпреступлений Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева,
e-mail: karen-avetisyan-1989@bk.ru

ОПЫТ ИСПОЛЬЗОВАНИЯ OSINT ПРИ ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ В СФЕРЕ IT

Аннотация. *Развитие информационных технологий и повсеместное внедрение цифровых платформ в повседневную жизнь привели к формированию глобального информационного пространства, ключевой характеристикой которого является колоссальный объём данных, доступных из открытых источников. Социальные сети, мессенджеры, форумы, открытые базы данных и иные публичные ресурсы стали не только средством коммуникации, но и важнейшим источником информации, имеющей значение для обеспечения безопасности личности, общества и государства. Использование аналитических платформ и инструментов выступает неотъемлемым компонентом профессиональной деятельности специалиста в области информационной безопасности в борьбе с преступностью.*

Ключевые слова: *информационные технологии, противодействие преступлениям, анализ и корреляция данных открытых источников.*

AVETISYAN Karen Rafaelovich,
Senior Lecturer, Department of Information Technology and Cybercrime Investigation Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev

EXPERIENCE USING OSINT TO COUNTER IT CRIMES

Annotation. *The development of information technology and the widespread adoption of digital platforms in everyday life have led to the formation of a global information space, a key characteristic of which is the colossal volume of data available from open sources. Social networks, instant messengers, forums, open databases, and other public resources have become not only a means of communication but also a vital source of information crucial for ensuring the security of individuals, society, and the state. The use of analytical platforms and tools is an integral component of the professional work of information security specialists in the fight against crime.*

Key words: *information technology, crime prevention, open source data analysis and correlation.*

Современный специалист в области информационной безопасности обязан понимать угрозы, связанные с публикацией данных в открытом доступе, и владеть методами их сбора и анализа для эффективного противодействия киберпреступности [1, с. 25].

Несмотря на очевидную потребность, анализ существующих образовательных программ показывает, что подготовка специалистов в области информационной безопасности не всегда в полной мере учитывает специфику работы с открытыми источниками информации сети Интернет. Зачастую изучение OSINT носит фрагментарный характер и не обеспечивает формирования системных знаний о правовых рамках, инструментарии и методиках анализа. Между тем, как свидетельствует международный опыт, включение специализированных курсов по OSINT в учебные планы становится устойчивым трендом, позволяющим подготавливать квалифицированные кадры, способные выполнять задачи по анализу данных из открытых источников в условиях цифровой трансформации.

Термин OSINT (Open Source Intelligence) обозначает деятельность по сбору, обработке и анализу информации, полученной из общедоступных (открытых) источников, с целью её последующего использования для решения прикладных задач в сфере безопасности, управления и расследования преступлений и административных правонарушений. Как отмечается в аналитических материалах Российского совета по международным делам, в границах России OSINT - достаточно молодое понятие, и его можно отнести к категории низовых инициатив, пришедших со страниц веб-форумов» [2]. Вплоть до 2014 года систематизированная информация об OSINT на русском языке практически отсутствовала, что подчёркивает начальный этап институционализации данной дисциплины в отечественном научном и профессиональном дискурсе [2].

В системе аналитической разведки OSINT занимает особое место как наименее затратный и наиболее доступный вид разведывательной деятельности. В отличие от HUMINT (человеческая разведка), SIGINT (радиоэлектронная разведка) или IMINT (видовая разведка), OSINT не требует специальных оперативных мероприятий и основывается на анализе информации, уже существующей в открытом доступе. При этом, как подчёркивается в экспертном сообществе, OSINT не сводится к простому агрегированию данных, а представляет собой «интеллектуальный анализ», требующий применения сложных методик обработки информации, включая технологии искусственного интеллекта и нейросетевого анализа [2].

Эффективность использования сервисов для осуществления OSINT на IT полигоне напрямую зависит от владения специалистом современным инструментарием, позволяющим автоматизировать сбор, обработку и анализ информации из открытых источников. В профессиональном сообществе принято выделять несколько категорий инструментов в зависимости от объекта поиска и задач, которые необходимо решить в ходе осуществления работы [10, с. 93]. Анализ современных образовательных программ и научных публикаций также позволяет выделить несколько категорий программных средств, коррелирующих с классификацией, изучение которых целесообразно включить в процесс подготовки специалистов по информационной безопасности:

– *Поиск по имени пользователя (username)*. Учитывая распространённую практику использования одних и тех же псевдонимов на различных интернет-платформах, поиск по никнейму позволяет обнаружить аккаунты лица в социальных сетях, на форумах, в комментариях и иных ресурсах. Sherlock и Snoop представляют собой программы с открытым исходным кодом, автоматизирующие поиск аккаунтов по имени пользователя на сотнях онлайн-платформ. Изучение данных инструментов позволяет обучающимся понять принципы работы с API социальных сетей, обработки HTTP-запросов и анализа ответов серверов. Кроме того, работа с открытым кодом способствует формированию навыков программирования и модификации инструментов под конкретные задачи.
– *Поиск по электронной почте*. Электронный адрес часто выступает уникальным идентификатором, привязанным к учётным записям в социальных сетях, мессенджерах, интернет-магазинах и иных сервисах. Анализ email-адреса позволяет не только обнаружить аккаунты лица, но и проверить факт участия в утечках баз данных, что имеет важное значение для оценки цифровых рисков. Epieos и Holehe предоставляют возможность проверки электронной почты на предмет регистрации в различных онлайн-сервисах. Данные инструменты особенно ценны в образовательном контексте, поскольку демонстрируют, как, казалось бы, незначительная информация (email) может раскрыть обширный цифровой профиль личности, включая аккаунты в социальных сетях, профили на форумах, учётные записи в облачных хранилищах и иных ресурсах
– *Поиск по номеру телефона.* Номер мобильного телефона в современном мире прочно связан с цифровой идентичностью человека. Его анализ позволяет определить оператора связи, регион регистрации, а также обнаружить аккаунты в мессенджерах (WhatsApp, Telegram, Viber, Max) и некоторых социальных сетях.
– *Поиск по изображению (обратный поиск)*. Обратный поиск изображений является одним из наиболее востребованных методов OSINT-анализа. Он позволяет установить источник фотографии, обнаружить её более ранние версии, идентифицировать запечатлённые объекты и лица, а также выявить факты использования поддельных или сгенерированных нейросетью изображений.
– *Комплексный анализ связей*. Наиболее сложным и трудоёмким направлением OSINT является построение и анализ графов связей между различными сущностями - людьми, организациями, адресами, электронными устройствами. Инструменты визуализации данных (например, Maltego) позво-

ляют представить сложные взаимосвязи в наглядной графической форме, выявить скрытые закономерности и сформировать целостную картину об объекте исследования. Maltego - Платформа позволяет собиз рать информацию из десятков источников, автоматически выявлять связи между сущностями и представлять их в виде интерактивных графов. В образовательном процессе изучение Maltego способствует формированию системного мышления, навыков структурирования больших объёмов информации и выявления скрытых закономерностей.

Отдельно хотелось бы отметить особое место в современном инструментарии для осуществления разведки по открытым источникам технологий распознавания лиц, основанных на методах машинного обучения.

Современные системы распознавания лиц, как отмечается в научной литературе, основаны на извлечении из изображения уникальных векторных представлений — эмбеддингов (embeddings), которые затем сравниваются между собой с использованием метрик сходства (например, косинусного сходства) [7].

Российская разработка Search4Faces ориентирована на поиск лиц в социальной сети «ВКонтакте». Сервис позволяет не только найти человека по фотографии, но и проанализировать его социальные связи. Международный сервис PimEyes индексирует изображения из открытых источников по всему миру и широко используется специальными организациями и журналистами. Инструмент EyeOfWeb представляет собой локальный «поисковик» с настраиваемыми источниками, основанный на нейросети InsightFace [9]. FaceCheck.ID специализируется на проверке лиц, имеющих профили на зарубежных ресурсах.

Авторским коллективом кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева совместно с кафедрой информационной безопасности учебно-научного комплекса информационных технологий Московском ордена Почета университете МВД России имени В.Я. Кикотя разработан ряд проектов по осуществлению поиска информации в открытых источниках, активно применяемых при обучении на IT полигонах, такие как:

Сервис по поиску информации из открытых источников «ЕНОТ». Система предоставляет инструменты для поиска информации о физических и юридических лицах, а также об их деятельности на основе открытых данных. Программа выполняет функции структурирования и упрощения доступа к большим объемам информации из открытых источников, способствуя оперативному поиску, анализу и подготовке аналитических материалов.

Сервис для предварительного анализа понятийно-категориального аппарата «Тушкан». Система ориентирована на выявление значимых терминов, тематических связей и характерных языковых конструкций с целью снижения вероятности пропуска оперативно-значимой информации. Программа осуществляет сбор, структурирование и лингвистическую обработку текстовых данных, включая выделение ключевых слов и выражений, анализ контекста их употребления, и ряд иных клиент-серверных и десктопных программных продуктов.

Данные решения позволяют существенно оптимизировать и автоматизировать поиск оперативно значимой информации из открытых источников сети Интернет.

Анализ отечественных и зарубежных образовательных программ позволяет предложить трехуровневую модель формирования компетенций в области OSINT, дифференцированную по глубине проработки материала, сложности решаемых задач и требуемому уровню подготовки обучающихся:

Уровень 1. Базовый (оперативная проверка). Первый уровень ориентирован на формирование фундаментальных знаний и навыков, необходимых для проведения оперативных проверок. Целью является овладение базовыми методами сбора и анализа информации из открытых источников, достаточными для быстрой проверки данных и получения ориентирующей информации.

В рамках данного уровня изучаются: основы OSINT и понимание его места в системе информационной безопасности; расширенные методы поиска с использованием операторов; работа с метаданными изображений и документов; базовые методы сбора информации из социальных сетей; использование простых OSINT-инструментов; этические и правовые основы работы с открытыми данными [8]. Результатом освоения базового уровня является способность самостоятельно проводить оперативную проверку по заданным параметрам и оформлять её результаты в виде краткой справки.

Уровень 2. Углублённый анализ. Второй уровень предназначен для подготовки специалистов, способных проводить комплексные исследования и решать сложные аналитические задачи. Целью является формирование навыков системного анализа, построения графов связей и подготовки аналитических материалов для поддержки принятия решений.

Программа второго уровня включает: углублённые методы геолокации и хронологического анализа; исследование поверхностного, глубокого и тёмного веба; работу со специализированными аналитическими платформами (Maltego, SpiderFoot); анализ социальных сетей и создание дискретных аккаунтов для операционной безопасности; методы проверки достоверности и верификации информации; документирование результатов и подготовку аналитических отчётов. Особое внимание уделяется обеспечению операционной безопасности и сохранению цифрового следа самого исследователя. Результатом освоения является способность проводить полноценное OSINT-расследование и представлять его результаты в структурированном виде.

Уровень 3. Профессиональный. Третий уровень ориентирован на подготовку экспертов высшей квалификации, способных решать сложные междисциплинарные задачи и использовать OSINT в сочетании с методами компьютерной криминалистики и искусственного интеллекта.

В рамках третьего уровня изучаются:

– продвинутые методы геолокации и GEOINT-анализ;
– интеграция OSINT с методами цифровой криминалистики;
– анализ криптовалютных операций и блокчейн-транзакций;
– использование искусственного интеллекта для анализа больших массивов данных;
– методы противодействия дезинформации и выявления глубоких подделок (deepfakes);
– разработка и внедрение стандартизированных протоколов расследований (Berkeley Protocol).

Эффективное формирование компетенций в области OSINT невозможно без широкого использования практико-ориентированных форм обучения, позволяющих обучающимся применять полученные знания в условиях, максимально приближенных к реальной профессиональной деятельности.

Лабораторные работы. Лабораторные работы являются основной формой практического обучения на базовом и углублённом уровнях. В ходе лабораторных работ обучающиеся под руководством преподавателя осваивают работу с конкретными инструментами и сервисами, выполняют типовые задания по сбору и анализу информации.

Кейсовые задания. Использование реальных кейсов позволяет сформировать у обучающихся способность применять OSINT-методы для решения конкретных профессиональных задач. Программа Высшей школы экономики включает «анализ реальных кейсов применения OSINT с представителями отраслевых компаний для выработки стратегии предприятия, анализа международных рынков и киберразведки» [9]. Кейсовые задания могут моделировать различные ситуации: проверка лица, расследование инцидента кибербезопасности, поиск утраченных активов, верификация информации в социальных сетях.

Анализ реальных цифровых следов. Важным элементом практико-ориентированного обучения является работа с реальными цифровыми следами, оставленными в открытых источниках. Обучающиеся учатся анализировать профили в социальных сетях, извлекать метаданные из изображений, отслеживать географическую привязку публикаций, анализировать сетевые связи.

В заключении следует отметить, технологии разведки по открытым источникам OSINT перестают быть вспомогательным инструментом и становятся неотъемлемым компонентом профессиональной деятельности специалиста в области информационной безопасности, а их изучение при подготовке специалистов в области информационной безопасности становится необходимым условием формирования профессионала в данной области.

Список литературы:

[1] Мередит Д. OSINT: руководство по сбору и анализу открытой информации в интернете / Дейл Мередит; пер. с англ. Е. Мансуровой. – Астана: Спринт Бук, 2025. 224 с.

[2] OSINT в России: образ, практика и перспективы // Российский совет по международным делам. – 2025. URL: https://russiancouncil.ru/analytics-and-comments/analytics/osint-v-rossii-obraz-praktika-i-perspektivy/ (дата обращения: 15.02.2026).

[3] Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция) (принят Государственной Думой 8 июля 2006 г.: ред. от 8 августа 2024 г.). // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/?ysclid=mmqvdk3gaw693397701 (дата обращения: 15.02.2026).

[4] Кохан Р.Ю. О проблемных вопросах обеспечения конституционных прав граждан в процессе информационно-аналитического обеспечения оперативно-разыскной деятельности, использования технологий OSINT-анализа // Вестник Сибирского юридического института МВД России. – 2024. – № 4. – С. 87–94.

[5] Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 N 144-ФЗ (последняя редакция) (принят Государственной Думой 5 июля 1995 г.). // СПС КонсультантПлюс.

URL: https://www.consultant.ru/document/cons_doc_LAW_7519/?ysclid=mmqvijvc99659512123 (дата обращения: 15.02.2026).

[6] Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 30.11.2024 N 420-ФЗ (последняя редакция) (принят Гос. Думой 30 нояб. 2024 г.). // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_491932/?ysclid=mmqvkc3v2241730170 (дата обращения: 15.02.2026).

[7] Кожин К.Д. TWINFINDER: СФУ в лицах - использование искусственного интеллекта для поиска похожих людей [Текст] / К.Д. Кожин // Региональные проблемы дистанционного зондирования Земли: материалы конференции. – Красноярск: Сибирский федеральный университет, 2024. – С. 340–343.

[8] Open-Source Intelligence (OSINT) : [course description] // Compass Security. – 2026. URL: https://www.compass-security.com/fr/trainings/open-source-intelligence-osint (дата обращения: 15.02.2026).

[9] Обеспечение экономической безопасности методами OSINT в региональных институтах развития : программа повышения квалификации // Национальный исследовательский университет «Высшая школа экономики». – 2025. URL: https://www.hse.ru/edu/dpo/1026432334 (дата обращения: 15.02.2026).

[10] Тисен О.Н. Субъекты досудебного соглашения о сотрудничестве // Судебная власть и уголовный процесс. Воронеж, 2013. – С. 91-95.

References:

[1] Meredith, D. OSINT: A Handbook for Collecting and Analyzing Open Source Information on the Internet / Dale Meredith; trans. from English by E. Mansurova. – Astana: Sprint Book, 2025. 224 p.

[2] OSINT in Russia: Image, Practice, and Prospects // Russian International Affairs Council. – 2025. URL: https://russiancouncil.ru/analytics-and-comments/analytics/osint-v-rossii-obraz-praktika-i-perspektivy/ (date of access: 15.02.2026).

[3] Federal Law “On Personal Data” of 27.07.2006 N 152-FZ (latest revision) (adopted by the State Duma on July 8, 2006: amended on August 8, 2024). // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/?ysclid=mmqvdk3gaw693397701 (accessed: 15.02.2026).

[4] Kokhan R. Yu. On the problematic issues of ensuring the constitutional rights of citizens in the process of information and analytical support for operational-search activities, the use of OSINT analysis technologies // Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. - 2024. - No. 4. - P. 87-94.

[5] Federal Law “On Operational-Investigative Activities” dated 12.08.1995 N 144-FZ (latest revision) (adopted by the State Duma on July 5, 1995). // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_7519/?ysclid=mmqvijvc99659512123 (accessed: 15.02.2026).

[6] Federal Law “On Amendments to the Code of the Russian Federation on Administrative Offenses” dated 30.11.2024 N 420-FZ (latest version) (adopted by the State Duma on 30.11.2024). // SPS ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_491932/?ysclid=mmqvkc3v2241730170 (accessed: 15.02.2026).

[7] Kozhin K.D. TWINFINDER: SFU in Faces - Using Artificial Intelligence to Find Similar People [Text] / K.D. Kozhin // Regional Problems of Remote Sensing of the Earth: Conference Proceedings. - Krasnoyarsk: Siberian Federal University, 2024. - pp. 340-343.

[8] Open-Source Intelligence (OSINT): [course description] // Compass Security. - 2026. URL: https://www.compass-security.com/fr/trainings/open-source-intelligence-osint (date of access: 15.02.2026).

[9] Ensuring Economic Security Using OSINT Methods in Regional Development Institutions: A Professional Development Program // National Research University Higher School of Economics. - 2025. URL: https://www.hse.ru/edu/dpo/1026432334 (date of access: 15.02.2026).

[10] Tisen O.N. Subjects of pre-trial cooperation agreement // Judicial power and criminal procedure. Voronezh, 2013. – P. 91-95.