Секция «Государственная политика и управление в условиях геополитической неопределенности»

Разведка по открытым источникам (OSINT) как угроза национальной безопасности в современных геополитических условиях

Научный руководитель – Потапова Елена Петровна

Беляев Данил Сергеевич
Студент (бакалавр)
Владимирский филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Факультет управления, Кафедра государственного и муниципального управления, Владимир, Россия
E-mail: dbelyaev33@gmail.com

Развитие средств информационной коммуникации в современном мире открывает простор для анализа огромных массивов данных, касающихся как деятельности отдельных лиц, так и государственной политики. Многочисленная информация, оказывающаяся в открытом доступе (в том числе в Интернете), нуждается в анализе, проверке на достоверность и систематизации, исходя из даты, времени и контекста создания материала, его принадлежности, геолокации, соотношения с другими источниками информации и т.д. Одним из актуальных способов интерпретации данных из открытых источников является разведка по открытым источникам, более известная как OSINT («ОСИНТ»).

В работе проведено системное исследование метода OSINT как актуальной угрозы национальной безопасности в современных геополитических условиях. Дано определение методу OSINT, приведены основные формы его применения сегодня. Сформулированы направления применения метода OSINT, угрожающие национальной безопасности Российской Федерации в условиях международной конфронтации. Разработаны общие рекомендации по минимизации связанных с применением метода OSINT рисков в информационном сопровождении деятельности органов власти.

OSINT (англ. – Open source intelligence) – это сбор и аналитика данных из разных источников для выработки различных стратегических и тактических решений с целью повышения конкурентоспособности частных и государственных организаций, проводимые в рамках закона и с соблюдением этических норм. В узком смысле OSINT – это сбор информации для обеспечения преимущества в различных областях [4]. Открытые источники содержат общедоступную информацию и не имеют законодательных ограничений в доступе к ним физических лиц. Разведкой по открытым источникам занимаются как государственные ведомства, крупные коммерческие компании и аналитические агентства, так и обычные пользователи Интернета, обладающие определёнными компетенциями в работе с открытыми данными.

Область возможного применения технологий OSINT обширна:

1. Сбор информации о человеке, организации или продукте.

2. Анализ сетевой активности пользователей, эффективности брендов и рекламы. Отслеживание общественного мнения.

3. Коммерческие исследования. Сбор информации о конкурентах и потребителях, отслеживание актуальных запросов потребителя и тенденций на рынке.

4. Национальная безопасность и внешняя разведка. Поиск сведений с целью предотвращения совершения или выявления правонарушений. Информационная борьба с внешними угрозами.

5. Академические исследования. Сбор эмпирических данных и статистических показателей для проведения научных исследований и др. [3]

В последние десятилетия актуальным направлением использования OSINT является военная разведка и анализ современных военных конфликтов. Это стало возможным благодаря развитию средств геолокации и спутниковой съёмки, активности участников конфликтов в социальных сетях и мессенджерах, массовому применению беспилотных летательных аппаратов с встроенными средствами видеосвязи и т.д. Мониторинг и объективный контроль открытых данных позволяет делать выводы о ситуации на фронте, передвижении военных подразделений, применении тех или иных видов вооружений, соотношении потерь воюющих сторон. Верная интерпретация полученных данных может способствовать выявлению уязвимостей цепочек поставок, защиты стратегически важных объектов и информационных систем, а также анализу эффективности используемых тактик и вооружений. На технологиях OSINT основана деятельность российских независимых военно-аналитических ресурсов, таких как LostArmour и MilitaryMaps.

Хотя технологии OSINT берут своё начало в 1940-х гг., с момента создания в США Службы мониторинга зарубежных трансляций, именно развитие Интернета привело к быстрому росту объёмов открытой информации. Работу с открытыми данными осуществляют и официальные ведомства в Российской Федерации, например, в сфере противодействия коррупции (с помощью государственной информационной системы «Посейдон»). Однако, использование технологий OSINT другими государствами может представлять угрозу для национальной безопасности России. Сегодня технологии разведки по открытым источникам применяются спецслужбами разных стран мира.

Таким образом, информационно-аналитическое сопровождение деятельности органов публичной власти Российской Федерации в условиях продолжающегося развития технологий OSINT (с возможностью интеграции нейронных сетей) нуждается в более строгом контроле. Особенно это касается информации, публикуемой должностными лицами, чья деятельность связана с сведениями, составляющими государственную тайну:

1. Военная область (стратегические планы, военное строительство, производство и технологическое развитие, подготовка и проведение военных операций).

2. Экономика, наука и техника (сведения, которые могут использоваться в целях промышленного шпионажа).

3. Некоторые сведения в области внешней политики и экономики.

4. Разведывательная, контрразведывательная и оперативно-розыскная деятельность.

Объектом разведки может стать личная информация, публикуемая должностными лицами в социальных сетях. Поддержание имиджа государственного или муниципального служащего важно в процессе взаимодействия общества и государства, но также должно соотноситься с требованиями национальной безопасности. Предоставление в открытый доступ информации, несущей угрозу безопасности государства, может рассматриваться как правонарушение вплоть до государственной измены (ст. 275 УК РФ). Опасность деятельности специальных служб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве признаётся на уровне стратегического планирования обеспечения национальной безопасности [1].

Ещё одно направление развития метода OSINT – пропагандистская работа, в том числе в процессе информационной войны. Цель пропагандистской работы в информационном противостоянии состоит в деморализации общества, подрыве доверия к институтам власти и государства, дестабилизации внутреннего социального положения [2]. OSINT позволяет проводить объективный мониторинг общественного мнения. Работа с открытыми данными в деятельности средств массовой информации, с одной стороны, может использоваться для опровержения дезинформации, а с другой – данные могут быть сфальсифицированы или ложно интерпретированы в целях манипуляции общественным мнением.

Предотвращение утечки данных требует профилактической работы со стороны струк-

турных подразделений по защите государственной тайны в органах власти в том числе в форме дополнительного профессионального образования по работе с открытыми и конфиденциальными данными. Государственные и муниципальные служащие должны осознавать риски от опубликования закрытых данных и последующую правовую ответственность. Лицам, имеющим доступ к указанным ранее сведениям, следует минимизировать использование социальных сетей и мессенджеров, подозреваемых в организации утечек персональных данных, как средств передачи закрытых сведений. К таковым относятся как ресурсы, доступ к которым ограничен по решению Роскомнадзора, так и незапрещённые (в том числе WhatsApp и Telegram) [5]. Аналогичные риски представляют и «неосторожные» публикации в СМИ. В сфере информационно-пропагандистского противостояния необходим отход от чрезмерного формализма и доказательное опровержение «фейков» и дезинформации.

Источники и литература

1) О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 02.07.2021 N 400 // Собр. законодательства Российской Федерации. - 2021. - № 27, ст. 5351.
2) Аджиева З.И., Текеева Л.Д., Кокова А.С. Реализация государственной информационной политики в условиях информационной войны // Власть истории и история власти. – 2022. – Т. 8, № 8(42). – С. 96-105.
3) Бондаренко Н.А., Гусева Т.М. Характеристика OSINT и эффективность его использования // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики : Материалы XXII Международной научно-практической конференции, Ростов-на-Дону, 21–22 ноября 2022 года. – Ростов-на-Дону: Ростовский государственный экономический университет "РИНХ", 2022. – С. 322-327.
4) Лемайкина С.В. Новый арсенал OSINT в цифровом мире. Разведка по открытым источникам // Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности : Сборник научных статей. – Орел : Орловский юридический институт Министерства внутренних дел Российской Федерации имени В.В. Лукьянова, 2021. – С. 27-31.
5) Прифронтовая разведка методами OSINT [электронный ресурс] / Habr.com : сайт. URL: https://habr.com/ru/companies/tomhunter/articles/741518/ (Дата обращения: 04.03.2025).