Болычев Н.И.

Воронежский институт МВД России

Использование методов кибербразведки при противодействии экстремизму

В статье рассматриваются современные методы кибербразведки (Cyber Threat Intelligence, OSINT, SOCMINT, Dark Web-monitoring и др.) и их применение для раннего выявления, диагностики и нейтрализации экстремистских угроз в цифровом пространстве Российской Федерации. Проведен анализ нормативной базы, технических возможностей и организационных аспектов интеграции кибербразведки в систему противодействия экстремизму, определены перспективные направления развития.

Подписанный 28 декабря 2024 г. Указ Президента РФ № 1124 утвердил новую Стратегию противодействия экстремизму в Российской Федерации и придал приоритетный статус мониторингу сетевых коммуникаций и превентивному выявлению угроз в Интернете[1]. Одним из ключевых инструментов достижения поставленных целей является кибербразведка, позволяющая получать упреждающую информацию о мотивах, планах и тактике экстремистских сообществ.

Систему кибербразведки целесообразно развертывать по многоуровневой модели «данные → аналитика → реакция». На уровне данных используются сенсоры DPI и социальные краулеры, данные поступают в TI-платформу, где коррелируются с базами IoC и знаниевой графовой моделью экстремистских групп. Реакционную составляющую формирует SOAR-платформа, автоматически генерирующая задачи по блокировке доменов и отключению каналов распространения. Российский опыт внедрения подобных систем в банковском секторе показывает сокращение среднего времени обнаружения (MTTD) инцидентов на 37 % и времени реагирования (MTTR) на 42 %[2].

Методы кибербразведки в контексте борьбы с экстремизмом

[1] Об утверждении Стратегии противодействия экстремизму в Российской Федерации : Указ Президента РФ от 28.12.2024 № 1124.

[2] Середкин С. П. Кибербразведка как эффективная стратегия защиты от киберугроз // Информационные технологии и математическое моделирование в управлении сложными системами. 2024. № 4. С. 14-22.

Группа методов	Краткая характеристика	Практическая ценность
OSINT (Open-Source Intelligence)	Автоматизированный сбор и корреляция данных из открытых источников (социальные сети, форумы, медиа-порталы).	Раннее обнаружение вербовочных материалов, сленга и «триггер-слов», используемых экстремистами [1].
SOCMINT (Social Media Intelligence)	Глубокая аналитика социальных графов, динамики аудиторий, вирусных постов.	Определение лидеров мнений и каналов распространения идеологии [1].
Threat Intelligence Feeds	Поставщики CTI (BI.ZONE TI, Positive Technologies TI и др.) агрегируют индикаторы компрометации (IoC), TTP группировок.	Корреляция сетевых индикаторов с объектами критической инфраструктуры; быстрая настройка средств фильтрации [5].
Dark Web-monitoring	Скрининг анонимных площадок (Tor, I2P, закрытые мессенджеры) на предмет торговли оружием, пропаганды, подготовки атак.	Выявление подготовки офлайн-акций и финансирования радикальных групп [2].
AI-driven Content Analysis	Распознавание аудио, видео и изображений, семантический анализ.	Масштабное семантическое «просеивание» контента с минимальными ложными срабатываниями.

Важным при противодействии экстремизму с использованием методов OSINT представляется кейс-анализ:

– выявление «групп-ретрансляторов». Корреляция OSINT-данных и метаданных мессенджеров позволила определить сеть из 12 пабликов-зеркал, распространявших запрещенный контент в течение 18 минут после исходной публикации. Блокировка зеркал снижала охват экстремистской публикации на 65 %[1].

– Dark Web-финансирование. Анализ BTC-транзакций с использованием Clustering Heuristics выявил кошелек-донор, который за три месяца финансировал 27 аккаунтов в Российской Федерации. Информация передана в Росфинмониторинг; сеть заблокирована[2].

Проблемы и направления развития

1. Правовой баланс. Совмещение требований ФЗ «О персональных данных» и необходимости глубокой аналитики контента требует уточнения норм процессуального доступа.

2. Информационное «шумоподавление». Высокий объем ложноположительных срабатываний при мониторинге сленга требует развития нейросетей с доменно-специфической обучающей выборкой.

[1] Меликян О.А. Оперативно-розыскная деятельность в сети Интернет в условиях противодействия экстремизму: некоторые вопросы правового регулирования // Молодой ученый. 2023. № 19 (466). С. 370–373.

[2] BI.ZONE Threat Intelligence. Threat Zone 2024: исследование ландшафта кибер угроз в России и СНГ. М.: BI.ZONE, 2024.

3. Межведомственное взаимодействие. Синхронизация TI-данных МВД, Роскомнадзора и частных SOC позволит закрыть разрывы в горизонте наблюдения и ускорит блокировку вредоносных ресурсов.

Комплексная киберразведка становится критически важным компонентом экосистемы противодействия экстремизму. Сочетание многоканального сбора данных, Threat Intelligence-аналитики и автоматизированного реагирования позволяет переходить от реактивной к проактивной модели безопасности, минимизируя окно возможностей для радикальных групп. Дальнейшее развитие данной сферы должно опираться на нормативное закрепление механизмов межведомственного обмена CTI-данными и внедрение отечественных платформ, способных в полном объеме обрабатывать кириллицу и региональные языковые особенности.

Лебедева М.Е.,

кандидат психологических наук
Санкт-Петербургский университет МВД России

Особенности применения профайлинга в рамках HUMINT

В статье рассматриваются ключевые аспекты использования профайлинга – метода психолого-поведенческого анализа личности – в разведывательной дисциплине HUMINT (Human Intelligence). Актуальность обусловлена усложнением оперативной обстановки, ростом гибридных угроз и необходимостью повышения точности оценки человеческого фактора в процессах рекрутирования и вербовки.

Профайлинг, изначально разработанный для криминалистики, все чаще применяется в сферах разведки и контрразведки[1]. В рамках HUMINT он позволяет минимизировать риски при отборе источников, оптимизировать методы получения информации и повышать достоверность оперативной оценки[2].

Целью настоящего исследования является определение специфики использования профайлинга в HUMINT и выработка практических рекомендаций. Для достижения цели решались задачи:

1) анализ существующих методик профайлинга;

2) выявление факторов, влияющих на их эффективность в HUMINT;

3) формулирование предложений по интеграции данных методик в цикл агентурной работы.

[1] Спектор Е.Б. Профайлинг: теория и практика. М.: Эксмо, 2020. 352 с.

[2] Егоров А.Н., Малова Т.Г. HUMINT: методы и технологии. СПб.: Питер, 2021. 288 с.