в Никарагуа – с преодолением структурных ограничений. Универсальность метода подчеркивает необходимость международного сотрудничества для создания адаптивных руководств, учитывающих культурную специфику.

Болычев Н.И.

Воронежский институт МВД России

Методы киберразведки при проведении несогласованных публичных акций

Киберразведка, как инструмент мониторинга цифрового пространства, играет ключевую роль в предотвращении несогласованных публичных акций. В условиях роста протестной активности государства активизируют методы анализа соцсетей, мессенджеров и открытых данных для выявления угроз общественному порядку. Однако правовое регулирование таких мер варьируется в зависимости от юрисдикции. В статье проводится сравнительный анализ законодательства России и Никарагуа, регулирующего применение киберразведки в контексте несанкционированных акций, с выделением ключевых правовых и этических аспектов.

Киберразведка включает:

– мониторинг социальных сетей – выявление призывов к участию в акциях через алгоритмы анализа ключевых слов;

– анализ метаданных – отслеживание геолокации и времени сообщений;

– взаимодействие с интернет-провайдерами – получение данных о пользователях;

– использование систем распознавания лиц – интеграция с камерами видеонаблюдения.

Эти методы позволяют властям прогнозировать и блокировать несогласованные мероприятия, но требуют четкой правовой регламентации для соблюдения баланса между безопасностью и правами граждан.

Российское законодательство предоставляет широкие полномочия для применения киберразведки:

– Федеральный закон «О собраниях, митингах, демонстрациях» (2004 г.) обязывает организаторов уведомлять власти о мероприятиях. Несогласованные акции признаются незаконными;

– Федеральный закон «Об информации, информационных технологиях и о защите информации» (2006 г.) разрешает блокировку ресурсов, распространяющих «запрещенную информацию», включая призывы к участию в акциях;

– Федеральный закон «Об оперативно-розыскной деятельности» (1995 г.) легализует сбор цифровых данных без судебного решения в случаях «угрозы национальной безопасности»;

– «Пакет Яровой» (2016 г.) обязывает телеком-компании хранить данные пользователей и предоставлять их по запросу силовых структур.

Ключевой аспект: правовые нормы сфокусированы на превентивном подавлении протестов, что расширяет возможности кибербразведки, но критикуется за нарушение приватности (ст. 23 Конституции РФ).

В Никарагуа правовое регулирование менее детализировано, но более жесткое:

– Ley Especial de Ciberdelitos (2020 г.) криминализирует распространение «ложной информации», под которой могут трактоваться призывы к протестам. Наказание – до 5 лет тюрьмы.

– Ley de Regulación de Agentes Extranjeros (2020 г.) позволяет контролировать финансирование НКО, участвующих в организации акций.

– Конституция Никарагуа (глава IV) гарантирует свободу собраний, но на практике разрешение властей требуется для любых публичных мероприятий.

Особенность: отсутствие четких процедур судебного надзора за кибер-разведкой. Мониторинг Интернета осуществляется силовыми структурами без публичной отчетности.

Обе страны используют кибербразведку для подавления несогласованных акций, но Россия формально гарантирует больше правовых гарантий.

В Никарагуа доминирует карательный подход, тогда как в России – превентивный.

Международные организации (ООН, Amnesty International) критикуют обе юрисдикции за нарушение свобод собраний и приватности.

Правовые системы России и Никарагуа демонстрируют различные подходы к регулированию кибербразведки. Если в Российской Федерации методы регламентированы, но используются для превентивного контроля, то в Никарагуа доминирует силовой контроль. Общим остается конфликт между безопасностью и правами человека, требующий поиска баланса через международные стандарты (например, рекомендации ОБСЕ по свободе собраний).