Научная статья
УДК 342.951:355.42
https://doi.org/10.24412/2073-0454-2023-7-100-104
EDN: https://elibrary.ru/jxantm
NIION: 2003-0059-7/23-903
MOSURED: 77/27-003-2023-07-102

Комплексный подход при противоборстве организации массовых беспорядков

Олег Валентинович Зиборов[1], Карэн Рафаелович Аветисян[2]
[1] Московский университет МВД России имени В.Я. Кикотя, Москва, Россия
[2] Министерство внутренних дел Российской Федерации, Москва, Россия, Karen-Avetisyan-1989@bk.ru

Аннотация. Инструментарий организации массовых беспорядков в информационном противоборстве выходит на совершенно новый уровень, интеграция достижений науки и техники в общественные отношения определяет необходимость комплексного подхода в обеспечении порядка и безопасности общества и государства [3]; в условиях информационных надстроек, диктующих со стороны противоборствующих сил инфоповоды через основные площадки коммуникации, их частоты и объема информации реализация аналитических функций должна проводиться в обязательном порядке на основе обученных, с высокой точностью идентификации, интеллектуальных систем и применением аппаратно-программных комплексов, что позволит точечно выявлять и устанавливать ключевых лиц и действовать превентивно, заблаговременно и негласно, не вызывая общественного резонанса и сохраняя государственный строй и общественную безопасность.

Ключевые слова: информационное противоборство, организация массовых беспорядков, искусственный интеллект, информационные технологии, порядок и безопасность

Для цитирования: Зиборов О. В., Аветисян К. Р. Комплексный подход при противоборстве организации массовых беспорядков // Вестник Московского университета МВД России. 2023. № 7. С. 100–104. https://doi.org/10.24412/2073-0454-2023-7-100-104. EDN: JXANTM.

Original article

An integrated approach to countering the organization of mass riots

Oleg V. Ziborov[1], Karen R. Avetisyan[2]
[1] Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia
[2] Ministry of Internal Affairs of Russia, Moscow, Russia Karen-Avetisyan-1989@bk.ru

Abstract. The tools for organizing mass riots in information warfare are reaching a completely new level, the integration of science and technology achievements into public relations determines the need for an integrated approach to ensuring order and security of society and the state [3]; in the conditions of information superstructures dictating information flows through the main communication platforms, their frequency and volume of information, the implementation of analytical functions should be carried out mandatory on the basis of trained, highly accurate identification, intelligent systems and the use of hardware and software complexes, which will allow to pinpoint and identify key individuals and act proactively, in advance and behind the scenes, without causing a public outcry and preserving the state system and public safety.

Keywords: information warfare, organization of mass riots, artificial intelligence, information technology, law and order

For citation: Ziborov O. V., Avetisyan K. R. An integrated approach to countering the organization of mass riots. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2023;(7):100–104. (In Russ.). https://doi.org/10.24412/2073-0454-2023-7-100-104. EDN: JXANTM.

В Российской Федерации в соответствии со ст. 31 Конституции РФ граждане РФ имеют право собираться мирно, без оружия, проводить собрания, митинги и демонстрации, шествия и пикетирование [1].

Однако следует помнить, что в ст. 17 Конституции РФ указано, что осуществление прав и свобод человека и гражданина не должно нарушать прав и свобод других лиц. Следовательно, при проведении массовых мероприятий права и свободы лиц, не задействованных в данном мероприятии, не должны быть нарушены в связи с проведением мероприятия [1]. Для обеспечения данного права 19 июня 2004 г. был издан Федеральный закон № 54-ФЗ «О собраниях, митингах, демонстрациях, шествиях и пикетированиях». Федеральный закон вводит понятия для основных видов мероприятий, четко разъясняет порядок проведения мероприятий и указывает, каким образом организовать их законно [8]. Одним из главных требований к организаторам мероприятий выдвигается уведомление органа исполнительной власти субъекта Российской Федерации или органа местного самоуправления о проведении публичного мероприятия в срок не ранее десяти и не позднее пяти дней до дня проведения публичного мероприятия.

Массовые беспорядки представляют собой нарушение основ общественной безопасности, но не всегда массовые беспорядки перерастают из массовых мероприятий; так в течение последних пяти лет во

многих крупных городах Российской Федерации начали проводиться незаконные акции. Нередки случаи, когда протестные акции и волнения внезапно перерастали в неконтролируемые погромы, поджоги и насилие в отношении граждан [4; 5]. Так как данные мероприятия не прошли установленную настоящим законом процедуру, ввиду чего органами власти было принято решение об их пресечении.

В современном обществе информационно-телекоммуникационная сеть Интернет стала неотъемлемой частью жизни. Внедрение средств массовой информации, а также развитие интернет-технологий привело к упрощению механизма распространения ложных сведений и призывов, в том числе о дискредитации органов власти, о нелигитимности государственного строя и призывов к массовым беспорядкам и свержению власти. Использование данных средств позволяет координаторам беспорядков в кратчайшие сроки собирать массы людей в конкретном месте, а также в последующем производить координацию их действий [2]. Обозначим ряд направлений применения информационных технологий в вопросах организации массовых беспорядков:

♦ вызов роста социальной напряженности путем публикации информации, не соответствующей действительности;

♦ призывы к проведению массовых беспорядков;

♦ координация между участниками в режиме реального времени и др.

Помимо пресечения массовых беспорядков правоохранительными органами проводится анализ социальных сетей и информационно-телекоммуникационной сети Интернет на наличие призывов к совершению массовых беспорядков. Мессенджеры и социальные сети выступают одной из наиболее актуальных площадок для коммуникации и являются одним из простейших и эффективных способов аккумуляции масс пользователей — людей, в целях формирования и продвижения соответствующей повестки.

Сбор значимой информации о ключевых лицах, установление места, времени и траектории их передвижения по промежуточным или оконечным пунктам сбора, распределение задач, целей и т. д. позволяют произвести тщательную подготовку, планирование и впоследствии установить по ролям организаторов, их помощников, а также иных ключевых лиц – участников подготавливаемой незаконной акции.

Как уже ранее было отмечено основными площадками коммуникации участников массовых акций выступают социальные сети: «Вконтакте», «Одноклассники» и др., в целях координации в режиме реального времени используют мессенджеры «WhatsApp» и «Telegram», платформы-видеохостинга по типу «Rutube», «Youtube» либо «Twitch» должны анализироваться системно при значительной аудитории (последователи/подписчики канала). Распространение информации на данных платформах отвечает критериям избирательности (личные сообщения или отдельные группы в мессенджерах), массовости (отправка сообщений в общие чаты, либо опубликование новостей на стене) и незамедлительности; следовательно, при грамотной координации со стороны организаторов протестной акции может быть нанесен значительный ущерб обществу и государству [2; 3].

Использование виртуальных частных сетей или же прокси-серверов, которые позволяют скрыть свой настоящий IP-адрес, как правило, принадлежащих иностранным компаниям, а, следовательно, оборудование (ЦОДы, сервера) находится вне территории РФ, осложняет процедуру установления лиц, представляющих оперативную значимость.

Помимо применения способов сокрытия действительного IP-адреса могут использоваться одноразовые или временные аккаунты на данных платформах, виртуальные номера телефонов зарубежных стран для осуществления регистрации на данных сервисах, а также заведомо ложные идентифицирующие данные при регистрации. Все это позволяет сокрыть установочные персональные данные организаторов беспорядков.

Однако использование открытых платформ для взаимодействия и распространения информации при организации массовых беспорядков, несанкционированных митингов, шествий, демонстраций или пикетирований позволяет органам исполнительной власти заранее быть готовыми к осуществлению своей деятельности и предотвращению реализации планов данных лиц.

Возможности создания и использования искусственных нейронных сетей или искусственного интеллекта позволяют исследовать, анализировать и выявлять информацию о готовящихся мероприятиях, которые могут перерасти в массовые беспорядки. Создание и обучение искусственного интеллекта или нейронной сети до высокого процента точности выявления необходимого материала по семантике текста, аудиозаписей, фото- или видеоизображений, которые публикуются на открытых плат-

формах, требует достаточного дата-сета для обучения. Материалы, которые публикуется в социальных сетях, мессенджерах или на видеохостингах, — ненормализованные (различного формата).

Организаторы массовых беспорядков получили новые инструменты для коммуникации и распространения ложной информации. Организаторы массовых беспорядков активно используют цифровые технологии для взаимодействия между собой и для возможности распространения запрещенной информации через информационно-телекоммуникационные сети, тем самым они оставляют множество различных цифровых следов. Правоохранительные органы могут использовать эту информацию для выявления подобного рода преступлений.

Органы правопорядка централизовано обеспечиваются современными аналитическими решениями в целях противоборства указанным незаконным акциям. Примером одного из решений, основанных на нейронных сетях, выступает интеллектуальная система «Окулус», запущенная в феврале 2023 г., которая отслеживает незаконный контент в сети Интернет. Данная система успешно обнаруживает сцены, содержащие противоправный характер, материалы, а также текстовые массивы, распространяемые в виде фото- или видеоизображений. «Окулус» способен выбирать кадры из видеопотока в случае, если исследуемое изображение несет в себе экстремистский характер, призывы к массовым незаконным мероприятиям, иной противоправный контент, распространяемый в сети Интернет.

Системы данного типа позволяют выявлять на просторах сети Интернет оперативно значимую информацию, своевременно идентифицировать и реагировать органам правопорядка, а также повышают эффективность обнаружения искомых лиц.

Для предупреждения и пресечения массовых беспорядков сотрудники правоохранительных органов проводят профилактические мероприятия, направленные на выявление и устранение причин и условий, способствующих возникновению массовых беспорядков, а также осуществляют контроль за соблюдением законодательства Российской Федерации о массовых мероприятиях.

Одним из способов противодействия массовым беспорядкам является повышение правовой культуры граждан и формирование у них негативного отношения к противоправным действиям. Большая роль в этом принадлежит средствам массовой информации, которые должны объективно освещать события, связанные с массовыми беспорядками, и разъяснять гражданам последствия участия в них.

Для задержания лиц, которые оказывали сопротивление и не были задержаны на месте проведения акции, сотрудниками органов внутренних дел использовались специализированные информационные системы. Это такие системы, как «Безопасный город» — городская система видеонаблюдения, с модулем «Парсив», а также система биометрического распознавания лиц «Сфера». Данные системы способны различать уникальный биометрический ключ — лица человека в потоке, и сверять их с эталонными изображениями — биометрическими ключами из баз данных МВД России. Система способна распознавать лица под разными углами и с разным уровнем доступности поступающего потока входных данных к сравнительному анализу. При установлении совпадения искомого объекта в базе данных разыскиваемых лиц автоматически посылается уведомление оператору системы. Благодаря «Сфере», лица, которые могли бы скрыться от сотрудников полиции в день незаконной акции, впоследствии будут установлены, так как определены их маршруты передвижения с оконечными пунктами дислокации [6; 7].

Криминалистические исследования с цифровыми следами становятся все более распространенными. Для эффективного и точного анализа цифровых следов используются специальные программные продукты, позволяющие сократить время и усилия, затрачиваемые на обработку информации, а также увеличить точность результатов.

Существует множество программных средств, предназначенных для выявления и анализа цифровых следов. Они могут отличаться функциональностью, доступностью, стоимостью и рядом других параметров. Программные продукты для выявления и анализа цифровых следов следует классифицировать.

1. Назначение: в зависимости от того, для каких целей предназначен программный продукт, он может быть классифицирован как инструмент для изучения файловой системы, регистра Windows, браузерных данных.

2. Тип цифровых следов: в зависимости от типа цифровых следов, с которыми работает программный продукт, его можно классифицировать как инструмент для работы с данными изображений, аудио, видео, метаданных.

3. Тип анализа: программные продукты могут быть классифицированы по типу анализа, который они позволяют выполнять. Например, инструменты

для анализа цифровых следов могут проводить временной анализ, статический анализ, анализ контента.

4. Формат входных данных: программные продукты могут быть классифицированы по типу формата входных данных, которые они принимают. Например, инструменты для анализа цифровых следов могут работать с файлами в форматах JPEG, PDF, DOCX и др.

5. Уровень сложности: в зависимости от уровня сложности, программные продукты могут быть классифицированы как инструменты не требующих специализированных знаний, интуитивно-адаптивным и доброжелательным интерфейсом и т. д.

Каждый продукт может быть уникален и предназначен для выполнения конкретных задач. Перечень программных продуктов для выявления и анализа цифровых следов:

1) EnCase Forensic: это программа, которая позволяет проводить детальный анализ жестких дисков, USB-устройств, мобильных устройств и других носителей данных;

2) X-Ways Forensics: это программное обеспечение, которое предназначено для изучения данных на жестких дисках, флэш-устройствах, мобильных устройствах и других носителях данных;

3) Cellebrite UFED (Universal Forensic Extraction Device): это программа, которая используется для сбора и анализа данных с мобильных устройств, устройств GPS и других электронных устройств;

4) Belkasoft Evidence Center: это программа для сбора и анализа данных, которая используется в расследованиях преступлений и восстановлении данных;

5) Passware Kit Forensic: эта программа является всесторонним решением для обнаружения и расшифровки зашифрованных электронных данных, позволяющая обнаружить и дешифровать сведения элементы на носителе, защищенные паролем.

Для идентификации подозреваемых лиц по цифровым следам необходимо провести тщательный анализ всех доступных данных и использовать различные методики, такие как сравнение голосов, анализ графики, распознавание лиц и др. Важно отметить, что процесс идентификации подозреваемых лиц по цифровым следам требует высокой квалификации и опыта от специалиста-криминалиста (аналитика/компьютерного эксперта).

Кроме того, при идентификации подозреваемых лиц по цифровым следам необходимо соблюдать правовые и этические нормы, чтобы избежать нарушения конфиденциальности данных и прав подозреваемых. Поэтому при работе с цифровыми данными следует учитывать все соответствующие нормы, а также проводить процедуры аутентификации и авторизации в целях защиты конфиденциальности как своих, так и исследуемых данных.

Согласно официальной статистике от компании Google, количество смартфонов с операционной системой Android превышает три миллиарда, что делает вопрос извлечения информации из таких устройств актуальным как никогда. В программном обеспечении «Мобильный Криминалист Эксперт» реализована возможность быстрого извлечения данных из самого популярного браузера Opera для Android-устройств с помощью собственной разработки компании — «Android-Агента». Функционал позволяет получить правоохранительным органам данные о паролях, сохраненных страницах, загрузках, закладках, банковских картах, контактах для автозаполнения, об учетной записи и истории посещений, а затем импортировать информацию на указанный носитель для последующего анализа.

В случаях механического повреждения материнских плат смартфонов приходится выпаивать флешпамять и считывать с нее информацию. Следует вскрыть телефон и оценить состояние платы и других элементов. Если поврежденными оказались микросхемы, восстановить данные будет затруднительно.

Исследование сведений на сим-картах представляет интерес в процессе расследования инцидентов. Несмотря на набирающую популярность esim (электронную SIM, не требующую использования физической карты) в последних моделях Android и iOS-устройств, спрос на обычные SIM-карты продолжает расти во всем мире и составляет не менее 5 млрд в год.

Учитывая такое широкое распространение, возможность криминалистического исследования SIM-карт не теряет своей актуальности, так как позволяет построить «вектор» связей лица, представляющего оперативный интерес и установить иных ключевых лиц, связанных по расследуемому инциденту. SIM-карта не обладает большим объемом памяти и может вместить примерно до 256 Кб данных. Из этого объема больше половины занимают данные сотового оператора, а остальное — операционная система и данные владельца. Используя ридер для подключения карты к ПК, специалист может изучить данные с SIM-карты в удобном представлении.

Изучение списка: журнала вызовов, данные телефонной книги, сохраненные на SIM (имя, телефонный номер), сообщений и их получателей, номера

абонента, номера SMS-центра, времени получения и самого текста сообщения и др.

Использование специализированного программного обеспечения для выявления и анализа цифровых следов является важным инструментом в работе правоохранительных органов, который помогает быстро и эффективно обрабатывать большие объемы данных, а также извлекать ценную информацию из различных носителей информации. Обеспечение порядка и безопасности массовых мероприятий включает в себя целый комплекс мер превентивного характера, планирование сил и средств, включающее в себя применение достижений науки и техники правоохранительными органами, получение оперативно значимой информации, как гласно, так и при помощи средств и методов негласного характера [6].

Список источников

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с изм., одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс».

2. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

3. «Концепция общественной безопасности в Российской Федерации» утверждена Президентом РФ от 14 ноября 2013 г. № Пр-2685 // СПС «КонсультантПлюс».

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс».

5. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СПС «КонсультантПлюс».

6. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс».

7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

8. Федеральный закон от 19 июня 2004 г. № 54-ФЗ «О собраниях, митингах, демонстрациях, шествиях и пикетированиях» // СПС «КонсультантПлюс».

References

1. The Constitution of the Russian Federation: adopted by popular vote on December 12, 1993 (with amendments approved during the all-Russian vote on July 1, 2020) // LRS «ConsultantPlus».

2. Decree of the President of the Russian Federation dated December 5, 2016 No. 646 «On approval of the Information Security Doctrine of the Russian Federation» // LRS «ConsultantPlus».

3. «Concept of public security in the Russian Federation» approved by the President of the Russian Federation dated November 14, 2013 No. Pr-2685 // LRS «ConsultantPlus».

4. Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 // LRS «ConsultantPlus».

5. Code of the Russian Federation on Administrative Offenses of December 30, 2001 No. 195-FZ // LRS «ConsultantPlus».

6. Federal Law of February 7, 2011 No. 3-FZ «On Police» // LRS «ConsultantPlus».

7. Federal Law No. 149-FZ of July 27, 2006 «On Information, Information Technologies and Information Protection» // LRS «ConsultantPlus».

8. Federal Law No. 54-FZ of June 19, 2004 «On Meetings, Rallies, Demonstrations, Marches and Picketing» // LRS «ConsultantPlus».

Информация об авторах

О. В. Зиборов — первый заместитель начальника Московского университета МВД России имени В.Я. Кикотя, доктор юридических наук, профессор;

К. Р. Аветисян — Министерство внутренних дел Российской Федерации.

Information about the authors

O. V. Ziborov — First Deputy Head of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Doctor of Legal Sciences, Professor;

K. R. Avetisyan — Ministry of Internal Affairs of Russia.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 24.11.2023; одобрена после рецензирования 30.11.2023; принята к публикации 18.12.2023.
The article was submitted 24.11.2023; approved after reviewing 30.11.2023; accepted for publication 18.12.2023.