

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

Аннотация. В статье рассматриваются вопросы информационно-аналитического обеспечения с использованием автоматизированных логико-аналитических систем в ходе противодействия терроризму и экстремизму. Анализируются проблемы, связанные с созданием интегрированного банка данных антитеррористического назначения и организацией межведомственного информационного взаимодействия в ходе борьбы с терроризмом и экстремизмом.

Ключевые слова: терроризм, экстремизм, автоматизированные логико-аналитические системы; искусственный интеллект; интегрированный банк данных антитеррористического назначения, межведомственное информационное взаимодействие.

Терроризм в наши дни продолжает оставаться общественно-политической проблемой номер один. Он создает проблемы безопасности для всего мира, детерминируя угрозы не только военного, но также экономического, политического и психологического свойства. Размах терроризма в современных условиях настолько широк, что для него не существует государственных границ. Террористы вооружены сегодня передовыми техническими средствами, многие из них в совершенстве владеют современными информационными технологиями. Так, по оценкам специалистов, технологическая вооруженность киберпреступников к 2026 г. позволит им осуществлять целенаправленные атаки на различные объекты критической информационной инфраструктуры с целью выведения их из строя и убийства людей. Как прогнозируют сотрудники исследовательской компании Gartner, использование боевых операционных технологий и других IT-систем только с учетом причинения смерти потерпевшим может нанести всем странам мира ущерб в размере более \$50 млрд [1]. В связи с этим возникают вопросы: насколько эффективно Российская Федерация способна противодействовать данному вселенскому злу и что необходимо предпринять для повышения эффективности антитеррористической деятельности?

Российские спецслужбы и правоохранительные органы в борьбе с проявлениями терроризма должны эффективно использовать все имеющиеся организационно-тактические формы антитеррористической деятельности. Последствия любого проявления терроризма следует оперативно минимизировать и устранять. Для этого необходимо своевременно устанавливать организаторов и исполнителей терактов; незамедлительно предупреждать или пресекать их действия, а лиц, причастных к террористической деятельности, привлекать к строгой юридической ответственности. Силы и средства, предназначенные для этого, должны поддерживаться в постоянной оперативной готовности к их применению. Поэтому в местах массового скопления людей, нахождения важных объектов жизнеобеспечения, транспортных магистралей, пунктов пропуска через государственную границу, таможенных постов, также объектов оборонной и гражданской инфраструктуры и др. – должно быть организовано непрерывное наблюдение, сопряженное с оперативным распознаванием физических лиц, причастных к террористическим актам, орудий и средств совершения преступлений, предметов двойного назначения, а также признаков самих преступных деяний.

Как известно, био- и нанотехнологии, квантовые вычисления, искусственный интеллект и прочие технологические новации используются

сегодня не только силовыми структурами, но и преступными элементами, в том числе и террористами. Этим самым последние нередко лишают правоохранителей их традиционных преимуществ. Американцы, например, вынуждены были приспосабливаться к этим тенденциям, поскольку так и не смогли победить исламских террористов не только в Афганистане и на Ближнем Востоке, но и в виртуальном пространстве [2, с. 19]. Возможно поэтому перед американскими силовыми структурами в свое время была поставлена глобальная задача – заполучить персональные биометрические данные, включая геномную информацию, всего населения Земного шара [3]. Правда, основные цели подобных шагов американцев до конца пока неясны и к проблемам противодействия терроризму они могут иметь лишь косвенное отношение. Тем не менее, если указанные данные будут использованы для обеспечения контроля за потенциальными террористами, то, безусловно, эти меры внесут существенный вклад в борьбу с данным серьезнейшим видом транснациональной преступности.

Однако в рассматриваемом нами контексте важны не только персональные биометрические данные физических лиц, имеющих причастность к терроризму и экстремизму, но и прочие сведения, имеющие прямое или косвенное отношение к этим людям. Речь в данном случае идет о так называемых «больших данных», накапливаемых в различных информационных массивах. Однако ограничиваться одним лишь накоплением подобных сведений нельзя, в противном случае они не принесут никакой пользы. Необходим их эффективный, тщательный анализ, осуществляемый в режиме реального времени. Единственным инструментарием, способным осуществлять анализ «больших данных», являются автоматизированные логико-аналитические системы (АЛАС), основанные на использовании искусственного интеллекта. Подобные системы уже давно и весьма эффективно применяются силовыми структурами как на Западе, так и на Востоке. Ю.Н. Жданов и В.С. Овчинский справедливо отмечают в этой связи, что искусственный интеллект (ИИ) создает принципиально новые возможности для правоохранительной деятельности и что особенно важно, – для обеспечения национальной безопасности государства. В настоящее время полиция ряда государств широко использует ИИ для сбора, классификации и анализа информации. Причем, при обработке сведений на первый план выходят принципиально новые, ранее не применявшиеся методы распознавания различных криминальных событий, и ближайшие годы станут временем тотальной экспансии методов применения ИИ в полицейской практике [4, с. 42].

В последнее время АЛАС, основанные на использовании ИИ, стали появляться и в России. Национальная стратегия развития искусственного интеллекта определяет ИИ как комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как мини-

мум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений, реализующих возможности ИИ, включает в себя информационно-коммуникационную инфраструктуру и программное обеспечение. К технологиям ИИ данная Стратегия относит в частности «компьютерное зрение», «обработку естественного языка», «распознавание и синтез речи», «интеллектуальную поддержку принятия решений» и «перспективные методы искусственного интеллекта» [5]. Без сомнения, АЛАС позволяют не только осуществлять анализ потокового видеоизображения в местах возможного появления террористов с целью оперативного распознавания и отождествления последних, но и обрабатывать имеющие к ним отношение структурированные, неструктурированные и полуструктурированные данные, получаемые из самых различных источников. Что самое важное, отечественным специалистам, посвященным в данные проблемы, об этом было известно уже достаточно давно [6, с. 180–184].

Наряду с этим в рассматриваемом аспекте необходимо реализовать и другие организационные меры. В частности, большое значение для осуществления антитеррористических мер имеет создание в каждом ведомстве, прямо или косвенно вовлеченном в противоборство с терроризмом и экстремизмом, *интегрированного банка данных (ИБД) антитеррористического назначения*, призванного консолидировать различные сведения персонального и событийного характера. Зададимся вопросом: что должен представлять из себя подобный ИБД?

Под интеграцией при создании ИБД антитеррористического назначения следует понимать не простое механическое слияние множества малых учетов в один большой, а прежде всего, – создание единой информационной инфраструктуры, предназначенной для анализа сведений, обладателями которых являются различные субъекты информационного обмена соответствующих ведомств. В качестве приоритетной формы такого обмена, безусловно, должен рассматриваться удаленный доступ с использованием АЛАС.

Таким образом, следует создавать единую информационную инфраструктуру всех силовых ведомств, прямо или косвенно противодействующих терроризму и экстремизму. Для этого необходим *единый межведомственный интегрированный банк данных антитеррористического назначения*. Структурно он должен состоять из объединенных ИБД различных ведомств. Для того чтобы реализовать эту идею на практике, следует обратиться к опыту деятельности специального органа, функционирующего в каждом государстве Европейского Союза (ЕС), – Национального департамента по оперативным данным (НДОД) [7, с. 48–49].

Список использованных источников:

1. Киберпреступники к 2025 г вооружатся технологиями для убийства людей // Securitylab.ru. 2021. 26 июля // URL: <https://www.securitylab.ru/news/522696.php> (дата обращения: 30.03.2025).

2. Кондрашов А. В виртуальной паутине. Как террористы и спецслужбы используют социальные сети // Аргументы недели. 2019. 16 мая. № 18(662). С. 19.

3. Рябова В. Дональд Трамп поручил ускорить внедрение биометрической системы на границах США. URL: d-russia.ru/donald-tramp-poruchil-uskorit-vnedrenie-biometricheskoj-sistemy-na-granitsah-ssha.html (дата обращения: 20.04.2025).

4. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. М.: Международные отношения, 2020. 285 с.

5. Национальная стратегия развития искусственного интеллекта на период до 2030 г.: утв. Указом Президента РФ от 10 октября 2019 г. № 490. П. 5, подп. «а», «б» // URL: <http://static.kremlin.ru/media/events/files/ru/AN4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf> (дата обращения: 20.04.2025).

6. Яковец Е.Н., Журавленко Н.И. Искусственный интеллект в информационно-аналитической работе // Математические методы и информационно-технические средства [Электронный ресурс]: материалы XVIII Междунар. науч.-практ. конф. (17 июня 2022 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко, А.В. Еськов и др. Электрон. дан. Краснодар: Краснодарский университет МВД России, 2022. С. 180–184.

7. OSCE Guidebook on Intelligence-Led Policing. [Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации] // Серия публикаций ДТНУ/ОСВПД. Вена, 2017. Т. 13. 106 с.

Yakovets E.N.

Russian Customs Academy, Lyubertsy

SOME ISSUES OF THE APPLICATION OF NEW INFORMATION TECHNOLOGIES IN THE FIELD OF COUNTERING TERRORISM

Abstract. The article discusses the issues of information and analytical support using automated logical and analytical systems in the course of countering terrorism and extremism. The problems associated with the creation of an integrated anti-terrorist database and the organization of interdepartmental information interaction in the fight against terrorism and extremism are analyzed.

Keywords: terrorism, extremism, automated logical and analytical systems; artificial intelligence; integrated anti-terrorist database, interdepartmental information interaction.