Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2023. – Т. 9 (75). № 4. – С. 221 – 231.

УДК 34:338.48(1-924.71)

ЭКСТРЕМИЗМ КАК УГРОЗА ТУРИСТИЧЕСКОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЫМСКОГО ПОЛУОСТРОВА (КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ)

Буткевич С. А.

Крымский филиал Краснодарского университета МВД России

В статье рассмотрены актуальные вопросы организационного и правового обеспечения криминологической безопасности объектов туристкой инфраструктуры в Республике Крым и городе федерального значения Севастополе. Дана подробная характеристика туристической отрасли в современных условиях, детально описаны положительные и негативные факторы, оказывающие влияние на курортную и инвестиционную привлекательность Крымского полуострова, и их возможные последствия. Особое внимание обращено на реальные и потенциальные угрозы, внутренние и внешние вызовы экстремистского характера, представляющие риски для туристической и информационной безопасности на региональном и федеральном уровнях. Также разработаны отдельные рекомендации для развития внутреннего туризма в Российской Федерации формирования и повышения медиакультуры в обществе, информационной грамотности населения, совершенствования контрэкстремистской деятельности правоохранительных и других государственных органов по обеспечению туристической и информационной безопасности Крымского полуострова.

Ключевые слова: внутренний туризм, вызовы экстремистского характера, информационные угрозы, курортная и инвестиционная привлекательность, туристическая безопасность.

Туристская сфера – одна из важнейших составляющих социально-экономической стратегии государства, направленная на формирование и развитие образовательного, культурного и духовного уровней жизни населения, удовлетворение эстетических потребностей, обеспечение восстановления жизненных сил и трудового потенциала граждан, рационального, интересного и полезного времяпрепровождения и саморазвития. Во всем мире туризм приобрел огромное значение как важнейший фактор сближения народов, социализации, выстраивания мирного диалога между различными этносами и конфессиями, содействия ознакомлению с историческим и культурным наследием, природными богатствами нашей планеты, средство физического и духовного развития личности, катализатор повышения качества жизни населения, роста экономического благополучия стран и формирования их положительного имиджа на международной арене.

Сегодня туризм стал одним из наиболее динамично развивающихся секторов в сфере оказания услуг на различных уровнях – от локального до международного. В Российской Федерации абсолютное большинство регионов всевозможными способами, с разной интенсивностью и эффективностью старается развивать свой туристский рынок, но распределение туристических потоков происходит неравномерно в связи с нестабильной геополитической и эпидемиологической обстановкой, сезонностью, природными поясами и климатическими зонами, меняющимися запросами, желаниями и потребностями контрагентов, а также эскалацией напряженности в локациях пребывания, приграничных регионах и соседних странах. Кроме того, на развитие туризма существенное влияние оказывают конкуренция и реклама, логистика, коммуникации и инфраструктура,

гостеприимство и ценовая доступность, природно-климатические явления и экология, состояние криминогенной обстановки и уровень безопасности населения в целом и туристов в частности.

В последние годы взрывному росту и интенсификации внутреннего туризма способствовали, с одной стороны, эскалация напряженности и ухудшения во взаимоотношениях с рядом зарубежных стран в синергии с их попытками осуществить международную изоляцию Российского государства, финансированием марионеточных правительств в странах постсоветского пространства и «оппозиции» в РФ, а с другой, – государственная поддержка внутреннего туризма, в первую очередь благодаря программам туристического кэшбэка, субсидированным авиа и железнодорожным перевозкам, развитию соответствующей инфраструктуры и социальной рекламе.

После воссоединения с Россией для удовлетворения максимального спроса и вариативных интересов потребителей туристских продуктов или услуг в Республике Крым активно развиваются культурно-познавательный, событийный (в том числе и фестивальный), пешеходный, велосипедный, автомобильный, подводный (дайвинг), конный, этнографический, природоведческий, гастрономический (включая винный), религиозный (паломнический), патриотический, детский, сельский, спелеологический, спортивный и развлекательный (в том числе экстремальный) и другие виды туризма (более 440 видов туристических маршрутов).

Несмотря на то, что начиная с 2014 г. туристический поток на Крымский полуостров ежегодно возрастал, в том числе во многом благодаря развитию транспортной инфраструктуры и интересу к новому региону под хэштегом «Крым наш!», с 2022 г. он значительно снизился. Безусловно, это связано с проведением специальной военной операции по демилитаризации и денацификации Украины, что сопутствовало закрытию воздушного сообщения с полуостровом, совершенными террористическими актами и ракетными атаками на Крымский мост, рядом осуществленных диверсий и информационно-психологических операций, распространяемыми паническими настроениями и слухами, прежде всего из-за рубежа и в интернет-пространстве, о небезопасности пребывания в регионе. Именно поэтому приоритетными задачами уполномоченных субъектов на государственном и региональном уровнях становятся не только обеспечение физической безопасности местных жителей и прибывающих на экскурсии, отдых, лечение или соревнования граждан, но и информационной и ментальной безопасности реальных и возможных туристов. При этом нельзя забывать о логистической доступности гостиничных и рекреационных комплексов, туристских услуг, туристических объектов, высоком уровне индустрии гостеприимства, комфорта и сервисного обслуживания в различных ценовых сегментах, сочетании традиций и инноваций, развитии культуры радушия, доброжелательности и отзывчивости, единстве в продвижении идей Русского мира.

Другими словами, туризм сегодня тесно связан с политической, социальной, экономической, культурной и другими сферами жизни человека, а туристская безопасность граждан – обеспечивается гарантированными им правами и свободами, реализацией законных интересов. Поскольку туризм и право человека на него в первую очередь ассоциируются со свободой передвижения в целях отдыха, просвещения, оздоровления, досуга, приобщения к истории, культуре, религии, природе и

т. д., приоритетным заданием уполномоченных субъектов становится обеспечение туристской безопасности граждан в регионе и на объектах временного нахождения. При этом данную проблему следует рассматривать не только в контексте обеспечения безопасности участников туристского движения, но и жителей туристического региона, конкретной локации и рекреационной местности в целом.

Повышенное внимание к переосмыслению феномена экстремизма в нынешних условиях обусловлено прежде всего модификацией и интенсификацией его проявлений, форсируемыми извне враждебностью (нетерпимостью) к традиционным духовным и семейным ценностям, устоявшимся моральным и нравственным ориентирам, непрекращающимися попытками свергнуть «диктатуру» лидера нации, назначив на его место проевропейски настроенного вассала, сменить «авторитарный» («тоталитарный») режим на «демократический», разделив нашу страну на части по принципу свободной конфедерации. Исследования экстремизма как социального явления и объекта правоохранительной деятельности проводятся в РФ уже не первый год, но его вариации и модусы, сопряженные с изменениями криминогенной обстановки и геополитической ситуации, обуславливают необходимость дальнейшей научной разработки данной проблемы [1]. В частности, в рамках нашего исследования затронуты вопросы противодействия экстремистской деятельности в информационной плоскости, а также предупреждения ее возможных последствий для туристической отрасли РК и города федерального значения Севастополя.

Безусловно, эффективность противодействия тому или иному негативному социальному явлению в значительной мере зависит от правильного понимания его генезиса, семантики и сущности. Именно поэтому институциональная характеристика экстремизма становится чрезвычайно важной как в теоретическом, так и практическом аспектах и приобретает определяющее значение при выработке мер по противодействию этому феномену, поскольку от корректного его понимания напрямую зависит формирование стратегии, реализация тактики и актуальность повестки контрэкстремистской деятельности, постановка целей, определение средств и методов для ее достижения и т. д.

Следовательно, очевидна потребность в модернизирующемся законодательном и комплексном научно-методическом обеспечении организационно-тактической и информационно-технической систем противодействия экстремистской деятельности, функционирующей и развивающейся с учетом актуальных правовых и социально-экономических реалий, разработки и апробации инновационных приемов, методов и средств реагирования на новые формы и виды угроз и вызовов экстремистского и террористического характера. Не секрет, что интенсивная информатизация и виртуализация абсолютно всех сфер жизнедеятельности общества сегодня является одним из определяющих глобальных факторов и драйверов дальнейшего социально-экономического, интеллектуального и ментального развития человечества. В то же время в III тысячелетии мировое сообщество перешло на новый этап своего развития, который можно назвать эрой информационных войн. В частности, информационная составляющая стала ключевым элементом широкомасштабной гибридной войны, ведущейся против Росси. Однако с учетом комбинированности и экстерриториальности информационных угроз, прежде всего в киберпространстве, попыток изоляции РФ от мирового сообщества (продвижение «культуры отмены»), санкции уголовного закона стали бесперспективными и малоэффективными. Имен-

но поэтому национальная безопасность в целом и ее информационная компонента в частности требуют формирования безопасного информационного пространства, последовательного и системного внедрения организационного, правового, психологического и технического инструментария превентивного характера.

В условиях дальнейшего развития информационного общества и ИТ-технологий все большую важность приобретают вопросы обеспечения информационной безопасности, то есть предупреждение и устранение вариативными формами и методами угроз, рисков и вызовов человеку, обществу и государству в информационной сфере. Однако в современном многогранном и динамичном мире проблемы обеспечения информационной безопасности приобретают принципиально новые черты, поскольку они выходят далеко за пределы противодействия войнам и вооруженным конфликтам. В настоящее время они стали их основой, первоисточником и главным оружием, используемым точечно, адресно, для целевой аудитории либо массового поражения.

Иначе говоря, изменения парадигмы обеспечения национальной безопасности с реактивной на проактивную для России становятся чрезвычайно важными, поскольку позволяют правильно определить стратегические приоритеты, консолидировать и оптимизировать усилия по обеспечению информационной безопасности во всех сферах жизнедеятельности социума и на всех этапах развития индивидуума. Вместе с тем глобальная сеть Интернет и различные интернет-площадки в нынешних условиях стали основным театром военных действий, ареной противостояния разных сил и средств, форсированным технологиями искусственного интеллекта, что требует кардинально нового уровня обеспечения национальной безопасности от вариативных угроз информационного опосредования. Кроме того, экстремистские организации успешно маскируют проявления своей противоправной деятельности в информационном пространстве позитивными и социально значимыми лозунгами, риторикой добра и мира, благотворительностью, декламацией и продвижением идей всеобщего процветания и благополучия.

Именно поэтому актуальной проблемой в сфере обеспечения безопасности на коллективных, национальных и региональных площадках остается своевременное (как утопия – превентивное) и симметричное реагирование, оперативная ликвидация (чаще минимизация) существующих и возможных рисков, угроз и вызовов различным сферам жизнедеятельности социума. Успешное решение данной проблемы в контексте глобальных трансформаций, масштабных природных катаклизмов, продуцирования штаммов для пандемий, эпизоотий и эпифитотий, ведения гибридных войн и отстаивания гегемонии однополярного мира невозможно в рамках использования традиционных, «классических» подходов к прогнозированию угроз, редуцированию и избежанию их последствий. То есть агрессивность и враждебность информационного (прежде всего кибернетического) пространства вынуждает постоянно видоизменять содержание и корректировать направления деятельности региональных и федеральных антиэкстремистских структур.

Поскольку научно-технический прогресс и социально-экономическое развитие внесли кардинальные и тотальные изменения в методы урегулирования геополитических, военных, социальных и экономических (включая торговые войны) конфликтов, территориальных споров и других противоречий, силовые методы все больше уступают место информационным. Развитие современного общества

в информационной плоскости сопряжено с использованием киберпространства как сферы осуществления не только социальных, политических и экономических процессов, но и преступной деятельности и даже плацдарма для ведения боевых действий и военных операций. Другими словами, увеличивающаяся в геометрической прогрессии зависимость от информационно-телекоммуникационных ресурсов и технологий делает социум более уязвимым перед возможными негативными последствиями противоправного использования информационного пространства. Поэтому фактически безграничный и растущий потенциал киберпространства и информационных ресурсов используется правительствами отдельных стран, их военно-политическими блоками и временными союзами в военных конфликтах (гибридных войнах) как в целях оптимизации и расширения функциональных возможностей собственных сил и средств обеспечения безопасности и обороны, так и создания новых структур и ресурсов, включая информационное оружие, для экспансии собственных геополитических и военных интересов.

Такое противоборство характеризуется трансграничностью, экстерриториальностью, разветвленностью, многоканальностью, виртуальностью, децентрализованностью, асимметричностью, неопределенностью, амбивалентностью, аморфностью, низкой прогнозируемостью ожидаемых действий и предсказуемостью их последствий, обезличенностью или скрытностью принадлежности сил и средств сторон конфликта (инцидента), в том числе использованием прокси-сил, при отсутствии классических фронта и тыла, каких-либо правил и обычаев. В свою очередь константное развитие информационных технологий и увеличение технического потенциала дает возможность осуществлять атаки по-новому, с применением инновационных способов причинения ущерба или увеличения его размера, ставить другие цели и определять новые объекты для посягательств в кинетическом мире и киберпространстве. Поэтому исследование угроз национальной безопасности, появление и мутации которых связаны с обострением информационного противоборства, а также механизмов противодействия таким вызовам, в нынешних условиях становится одним из наиболее актуальных предметов и объектов научных изысканий, в первую очередь в сфере контрэкстремистской деятельности.

Повторимся, что нормативная правовая неурегулированность (коллизионность, пробельность) информационного, прежде всего кибернетического, пространства вызывает беспокойство не только практиков, но и ученых. Исходя из анализа современных научных исследований, можно сделать вывод о том, что состояние национальной безопасности напрямую зависит от обеспечения информационной безопасности. Причем благодаря научно-техническому прогрессу и эволюционному развитию информационно-телекоммуникационных технологий данная зависимость будет только возрастать. Но законодательное регулирование общественных отношений в киберпространстве не может не только опередить развитие и предугадать рост противоправных действий в этом секторе, но и даже идти с ним в ногу. Это касается и технологического уровня противодействия таким угрозам и вызовам, реальным и потенциальным. Как видится, целесообразно смещать акценты на контентный уровень противодействия негативному информационному воздействию.

Подчеркнем, что в современных реалиях на информационно-коммуникационные технологии и ресурсы также оказывается милитаристское влияние, которое постоянно интенсифицируется. Учитывая это, не сложно спрогнозировать дальнейшее

совершенствование методов ведения информационно-психологической войны и расширение сфер применения соответствующих технологий, что на глобальном уровне может существенно отразиться на стратегическом балансе сил и повлиять на изменения в нынешних критериях его оценки на основе соотношения геополитических, экономических и военных показателей.

Не углубляясь в ретроспективный анализ применения различных информационно-пропагандистских приемов, агитационных средств и манипуляций, с одной стороны, для деморализации, ослабления мобилизационной и боевой готовности (неотвратимость поражения, бессмысленность сопротивления), создания негативного имиджа реального и гипотетического противника (в том числе на международной арене), инспирирования принятия ошибочных управленческих решений, подрыва доверия к военно-политическому руководству оппонента, провоцирования паники (смуты) среди населения, дестабилизации обстановки и эскалации напряженности, с другой – для укрепления морального и боевого духа собственных войск (сил), отметим, что благодаря тотальному распространению и повсеместному использованию мобильных телефонов и сети Интернет значительно усилились мультипликативность, масштабность, вариативность, наглядность и образность средств идеологического и психологического воздействия как на целевую аудиторию, так и на неограниченное количество потребителей контента, их чувства, мотивацию, убеждения, эмоции, реакции, сознание, мышление, нарративы и поведение. Иными словами, наблюдается конвергенция объектов противоправных посягательств и деструктивного воздействия, к которым относятся интересы государства и гражданского общества, права и свободы человека, национальная и ментальная безопасность. Подчеркнем, что последствия информационной агрессии заинтересованных акторов, их доминирование на различных интернет-площадках увеличиваются на порядок не только в случае уязвимости физических объектов посягательств, информационных систем и критической инфраструктуры, но и недостаточной медиакультуры общества. Конечной целью такой негативной и деструктивной деятельности считаем сохранение или достижение информационного господства (преимущества, монополии) над побежденной страной вследствие взлома и изменения культурного кода нации, включая историческую, духовную, социальную, психологическую и национальную память, нравственные идеалы, патриотические традиции, семейные ценности и мировоззренческие приоритеты. Другими словами, это классическая социальная инженерия в информационном пространстве. В то же время не менее значимой для информационного агрессора задачей является недопущение достижения аналогичных целей контрагентами в его информационном поле.

То есть благодаря использованию современных и инновационных информационных технологий, новое тысячелетие дало возможность применять новаторские способы ведения войн с отсутствием фактических, материальных повреждений и минимальным количеством человеческих жертв (или вообще без таковых), но в физическом, а не ментальном смысле. При этом осуществляется целенаправленная, скоординированная и широкомасштабная модерация информационных процессов, систем и моделей для изменения существующей или создания новой, альтернативной картины мира для потребителей информационных продуктов в результате продуцирования, тиражирования, модификации, навязывания, блокирования и удаления определенного контента или ресурсов. Так, к приоритетным заданиям кибервойн,

ведущихся в российском информационном пространстве, русскоязычном сегменте Интернета или с доктриной Русского мира, можно отнести: формирование нигилизма, атмосферы аморальности и бездуховности; отказ от традиционных ценностей и жизненных ориентиров; индифферентное или негативное отношение к историко-культурному наследию и героическому прошлому; нивелирование или стыдливость чувств патриотизма, гражданственности, любви к Родине; манипуляции индивидуальным, групповым и коллективным сознанием, символами и эмоциями, распространение мифологем и симулякров в целях создания нестабильности и напряженности в обществе, подрыва авторитета лидера нации, доверия органам власти и веры в успех специальной военной операции; ретрансляция неуверенности, сомнений, фобий, беспокойства, недоверчивости и подозрительности, инициирование и провоцирование этнонациональных, социальных, политических и экономических конфликтов; изменение направления, приостановление развития или деградация каких-либо общественных отношений, социальных процессов, «размытие» и нивелирование значимости каких-либо дат, фактов, событий, достижений и личностей.

Как следствие, перечисленные выше вмешательства и манипуляции прямо или опосредованно, шоково или поэтапно, разово или длительно и пролонгированно могут воздействовать на коллективное бессознательное через новостную, коммуникативную, образовательную, научную и культурную сферы. Соответственно, уполномоченные субъекты должны учитывать реальные и вероятные уязвимости и болевые точки в сознании и подсознании целевых аудиторий. При этом при наличии мощных и неконтролируемых информационных потоков крайне сложно противодействовать информационным угрозам ограничительными или запретительными методами. Контрмеры будут эффективными лишь при наличии в социуме критической массы духовно-интеллектуальных ресурсов, умений и навыков оптимально и продуктивно использовать и потенциал в контексте обеспечения информационной безопасности человека, общества и государства. Интересно отметить, что украинский исследователь А.А. Верголяс указывает, что методология информационных (электронных) войн широко применяется в «цветных» революциях, когда, не прибегая к боевым действиям, заинтересованная сторона выполняет поставленные ей политические или идеологические задачи [2, с. 41]. Однако автор почему-то не иллюстрирует свой тезис успешно реализованными на Украине западными кукловодами «оранжевой революцией» (2004), «евромайданом» (2014), последующей гражданской войной и террором мирного населения на юго-восточных рубежах своей страны.

Опасность, реальность, масштабность и эффективность проявлений информационной войны также могут обеспечиваться суггестивностью своего воздействия, латентным или закамуфлированным характером, точечностью и адресностью распространяемых данных, в том числе интенсифицируемыми благодаря недоверию официальным и традиционным медиа (по принципу «нет пророка в своем отечестве»), превращая различные информационно-телекоммуникационные ресурсы и площадки для целевой аудитории в иммерсивный театр. Таким образом эти угрозы с помощью информационных технологий, ресурсов и коммуникаций оказывают прямое либо косвенное воздействие на информационные системы или социальные процессы, вследствие которого проблематично или невозможно защитить национальные интересы, реализовать стратегические приоритеты государства и гарантировать эффек-

тивность функционирования системы обеспечения национальной безопасности. В качестве наглядного примера в информационном поле для нашего региона можно привести такие недостоверные и заведомо ложные сведения, распространяемые украинскими пропагандистами, иноагентами и некоторыми зарубежными изданиями, как: ожидаемое контрнаступление ВС Украины и неминуемое «освобождение» («деоккупация») Крымского полуострова; уничтожение Крымского моста, других объектов инфраструктуры и российских военнослужащих благодаря военной помощи стран ЕС и США; преподнесение неофициальными медиа и блогосферой техногенных аварий и происшествий как следствие активности партизанского движения «украинских патриотов» в регионе; неизбежность привлечения к уголовной ответственности или физической ликвидации «оккупантов» и «коллаборантов»; наличие в регионе украинского подполья (включая «ждунов») с разветвленной сетью и безграничными возможностями, широко поддерживаемого местным населением. Безусловно, это сказывается не только на спокойствии и настроениях крымчан, но и на курортной и инвестиционной привлекательности РК и г. Севастополя, их туристическом функционале, рынке недвижимости, дальнейшем развитии гостиничного бизнеса, сферы обслуживания, технологий гостеприимства и рекреационной инфраструктуры, экономическом благополучии региона в целом.

Итак, использование информационной компоненты технического, технологического, идеологического и психологического характера в гибридных войнах XXI в., включая киберинциденты, DDoS-атаки, тенденциозную активность в видеохостингах, социальных сетях и мессенджерах агентов влияния, лидеров мнений, блогеров, троллей, ботов и «оппозиции», поисковых систем и новостных агрегаторов с разветвленным инструментарием, может приводить к росту миграционных процессов, протестных и панических настроений, военным конфликтам и поражению в них, дезорганизовывать работу органов государственной власти и публичного управления, функционирование банковской и финансовой систем, транспортной инфраструктуры и средств коммуникации [3; 4]. А в случае с нашим регионом – еще и к значительному снижению количества туристов и отдыхающих. Соответственно, чем выше уровень цифровизации, экономического развития и благополучия общества, тем больше оно нуждается в обеспечении кибербезопасности, поскольку абсолютное большинство интересов человека удовлетворяется с помощью информационно-телекоммуникационных технологий. А учитывая тот факт, что под воздействием экзистенциональных и семантических манипуляций, фабрикации фактов, информационных спекуляций, шума и триггеров в синергии с определенными алгоритмами нейросетей могут легко видоизменяться мировоззрение и мировосприятие отдельных граждан, их категорий и социума в целом (программирование), навязываться чуждые, аморальные, асоциальные или противоправные интересы, увлечения, ценности, ориентиры и поведенческие паттерны (деформация, демонтаж и перекодировка сознания), главными задачами субъектов противодействия таким угрозам – государства и общества – становятся разработка механизмов выявления и предупреждения данных рисков, уязвимостей и вызовов, устранения их последствий и скорейшего восстановления (реабилитации) после них, а также создание качественного информационного продукта, вызывающего интерес и внушающего доверие у его потребителей, с одновременным сознательным неприятием и отторжением

вредного и опасного контента, в том числе благодаря сформированной в обществе медиакультуре.

В то же время нельзя оставить без внимания и обратную сторону медали – попытки отдельных жителей и гостей Крымского полуострова завоевать сиюминутную популярность, «хайпануть» на происшествии, беде, трагедии благодаря социальным сетям и мессенджерам, выложив на различные интернет-площадки фото- и (или) видеосъемки соответствующего содержания. Такое измененное сознание граждан в совокупности с их асоциальной, антигражданской или даже преступной позицией (оставляя за скобками угрозу их собственной безопасности и неоказание помощи пострадавшим), может приводить к расшифровке позиций ВС РФ, органов безопасности и правопорядка для последующих атак и «контрнаступления». Именно поэтому глава РК С.В. Аксенов в августе 2023 г. выступил с правильной инициативой – на федеральном уровне внести изменения в законодательство в части ужесточения ответственности за распространение в публичном поле, на различных интернет-ресурсах, в социальных сетях, мессенджерах фотографий и видеозаписей расположения и работы военных и стратегических объектов, ПВО и других оборонных система, а также результатов террористических атак, совершенных киевским режимом. Несомненно, медиа уже давно не играют роль общественно-политического медиатора, удовлетворяющего интересы социума, а выполняют функции проводника политических сил и элит. Тем не менее, нужны не только запреты, ограничения и ужесточение санкций, а информатизация общества, развитие и популяризация критического отношения к информации, неизвестным, сомнительным или новым источникам и каналам данным, способные создать у граждан барьеры и фильтры для вредного и опасного контента, обезопасить общество и государство от информационных вмешательств, манипуляций, вбросов и кибератак.

В продолжение затронутой проблемы обратим внимание на то, что на протяжении исторического развития общества в целом и региона исследования в частности наблюдались разнообразные переплетения национальных интересов, смешения этнических стереотипов, культурных традиций, религиозных обычаев, ментальных норм и, как следствие, борьба за их восстановление и самобытность [5]. Вместе с тем менталитет имеет естественные и онтологические детерминанты, поскольку человек может по своему усмотрению самоопределяться, самостоятельно принимать решения, менять привычки и образ жизни. Но современный мир отдает преимущество не общечеловеческим моральным, а национальным ценностям, в частности менталитету. Сформированный менталитет приобретает значимость и важность, когда государство, заботясь о духовном и материальном развитии своих граждан, обеспечивает природно-правовую гармонию с превалированием духовной компоненты. Безусловно, специфика развития мирового сообщества в новом тысячелетии связана с формированием развитой интеллектуальной среды, которая, в свою очередь, становится канвой для прогрессивного развития во всех сферах жизни социума. Только в такой среде могут быть подготовлены и реализованы эффективные управленческие решения, разработаны и внедрены успешные технологические процессы в частности и гарантированы устойчивое развитие общества и его безопасность в целом [6].

Обеспечение национальной безопасности в информационной сфере требует формирования и реализации научно и методически обоснованной государственной

политики, взвешенной и последовательной стратегии и наступательной тактики в информационной сфере, определения системы национальных ценностей, жизненно важных интересов человека, общества и государства в этой сфере, мониторинга, выявления и нейтрализации реальных и потенциальных угроз информационной безопасности, поиска результативных мер для обеспечения последней, защиты от киберугроз и создания качественных информационных продуктов. Обеспечение информационной безопасности сейчас видится приоритетным направлением внутренней и внешней государственной политики, от которого напрямую зависит состояние национальной безопасности страны, ее социально-экономическое развитие и место на международной арене. Безусловно, это касается и регионов, в первую очередь становящихся объектами преступных посягательств со стороны Украины.

Именно в современных условиях феномен информационных технологий, приобретая мультиотраслевое значение, все чаще рассматривается как эффективный инструмент агрессии и информационное оружие, используемое в совокупности со средствами техногенного, коммуникативного и информационно-психологического влияния и методами дистанционного информационного управления, а отношения между технологически развитыми странами обладают всеми признаками информационного противоборства. Кибернетические войны, психологические и информационные операции, социальный инженеринг, нейропсихология, нанотехнологии – все эти явления усиливают роль информационных технологий, особенно в условиях вооруженных конфликтов или даже при ведении агрессивной внешней политики. То есть популярность и привлекательность информационного продукта часто зависят от его технологичности, а применение информационных технологий становится абсолютным и практически неуязвимым оружием массового поражения.

Рассмотренная выше проблематика базируется на понимании феномена рисков и вызовов, ставшими неотъемлемыми атрибутами жизнедеятельности граждан, с широким спектром модусов и масштабами, связанными с социально-историческим развитием общества, и отражением его интенсивности. Поэтому отличительной особенностью государственной политики в этой сфере должны стать: концептуальное изменение философии управления, с возможностью перехода от координации деятельности уполномоченных субъектов к оперативному управлению ими; развитие государственно-частного партнерства, в том числе в части предоставления бизнесу и общественности реальных рычагов влияния в этой сфере; реализация бизнес-проектов в направлении дальнейшего совершенствования устойчивости информационной и телекоммуникационной инфраструктуры; повышение осведомленности и информационной грамотности граждан на всех просветительских и образовательных уровнях (развитие культуры безопасности).

Подытоживая изложенное, отметим, что в начале XXI в. бурное и стремительное развитие и глобальное интенсивное распространение интернет-технологий обусловили появление самостоятельного виртуального информационно-коммуникационного пространства со специфическими принципами и собственными закономерностями функционирования. Ведущую роль в коммуницировании как на индивидуальном, так и на социально-политическом уровнях играют именно информационные технологии. Это существенно влияет на процессы управления общественным сознанием, позволяя субъектам коммуникационного влияния эффективно конструировать восприятие социумом объективной реальности и существующей

действительности. Другими словами, глобальная коммуникационная среда обладает значительным манипулятивным потенциалом, который дает возможность технологически подготовленным субъектам осуществлять транзит и популяризацию идей, догм, образов, ценностей и смыслов в сегменты информационного пространства определенных социальных групп, государств и дестабилизировать социально-политическую обстановку, эскалировать напряженность в региональном, национальном и (или) глобальном масштабах благодаря информационной интервенции.

Список литературы:

1. Нагорный А.П., Попов А.Н. Экстремизм – прямая угроза России // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8. № 2. С. 330–335.
2. Верголяс А.А. Правовое обеспечение специальных информационных операций: дис. … канд. юрид. наук. К., 2020. 287 с.
3. Никитина Л.Н., Коноплева А.А., Чудина-Шмидт Н.В. Детерминанты формирования радикального сознания молодежи // Российский девиантологический журнал. 2023. № 3 (2). С. 195–207.
4. Иванов С.И. Признаковая характеристика объектов поиска в оперативно-розыскной деятельности // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2018. № 4. С. 203–208.
5. Родителева Я.Н. Разновидности экстремизма и их влияние на социально-политическую жизнь России // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2023. Т. 9. № 2. С. 441–208.
6. Костюченко Н.И. Проблемы государственного управления, связанные с соотношением понятий «муниципальное» и «государственное» управление // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2019. Т. 5. № 3. С. 36–42.

Butkevich S.A. Extremism as a threat to tourist and information security of the Crimean Peninsula (criminological aspects) // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2023. – T. 9 (75). № 4. – P. 221 – 231.

The article deals with topical issues of organizational and legal support of criminological security of tourist infrastructure facilities in the Republic of Crimea and the federal city of Sevastopol. A detailed description of the tourism industry in modern conditions is given, positive and negative factors that affect the resort and investment attractiveness of the Crimean Peninsula, and their possible consequences are described in detail. Particular attention is paid to real and potential threats, internal and external extremist challenges that pose risks for tourism and information security at the regional and federal levels. Separate recommendations have also been developed for the development of domestic tourism in the Russian Federation, the formation and improvement of media culture in society, the information literacy of the population, the improvement of the counter-extremist activities of law enforcement and other government agencies to ensure tourism and information security of the Crimean Peninsula.

Key words: domestic tourism, extremist challenges, information threats, resort and investment attractiveness, tourist security.

Spisok literatury:

1. Nagornyj A.P., Popov A.N. Ekstremizm – pryamaya ugroza Rossii // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2022. T. 8. № 2. S. 330–335.
2. Vergolyas A.A. Pravovoe obespechenie special'nyh informacionnyh operacij: dis. … kand. yurid. nauk. K., 2020. 287 s.
3. Nikitina L.N., Konopleva A.A., CHudina-SHmidt N.V. Determinanty formirovaniya radikal'nogo soznaniya molodezhi // Rossijskij deviantologicheskij zhurnal. 2023. № 3 (2). S. 195–207.
4. Ivanov S.I. Priznakovaya harakteristika ob"ektov poiska v operativno-rozysknoj deyatel'nosti // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2018. № 4. S. 203–208.
5. Sm.: Roditeleva YA.N. Raznovidnosti ekstremizma i ih vliyanie na social'no-politicheskuyu zhizn' Rossii // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2023. T. 9. № 2. S. 441–208.
6. Kostyuchenko N.I. Problemy gosudarstvennogo upravleniya, svyazannye s sootnosheniem ponyatij «municipal'noe» i «gosudarstvennoe» upravlenie // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. YUridicheskie nauki. 2019. T. 5. № 3. S. 36–42.

.