УДК 340, 341, 347

С.В. Аксенов[1]
Д.В. Сироткин[2]
А.А. Тыртышный[3]
А.А. Тыртышный-младший[4]

СОВРЕМЕННОЕ ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО: ПУБЛИЧНО-ПРАВОВЫЕ И ЧАСТНОПРАВОВЫЕ АСПЕКТЫ

S.V. Aksenov
D.V. Sirotkin
A.A. Tyrtyshny
A.A. Tyrtyshny-junior

MODERN INFORMATION WARFARE: THE PUBLIC-LAW AND PRIVATE-LAW ASPECTS

Необходимость реализации публично-правовых и частноправовых аспектов в обеспечении информационной безопасности России в условиях современного информационного противоборства отражена в положениях Стратегии национальной безопасности РФ (далее – Стратегия) и Военной доктрине РФ (далее – Доктрина). Так, описывая механизм обеспечения национальной безопасности, Стратегия определяет, что «обеспечение национальной безопасности – это реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов» [1]. Законодатель, таким образом, выделил взаимодействие государства и институтов гражданского общества по реализации информационных и правовых мер в сфере национальной безопасности в число приоритетов и предусмотрел возможности применения мер публично-правового и частноправового регулирования для ее обеспечения.

На совершенно новом уровне регулирует вопросы информационной безопасности и информационного противоборства Военная доктрина РФ, принятая 25 декабря 2014 года. Определяя военные угрозы, в Доктрине (ст. 11) отмечается, что в современных условиях «наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации» [2]. Традиционно подразделяя военные опасности на внутренние и внешние, Доктрина относит к внешним опасностям достаточно опосредованный публично-правовой фактор – использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности (п. м, ст. 12). А при определении внутренних военных

[1] Доктор технических наук, профессор АНО ВО «Российский новый университет».

[2] Магистрант АНО ВО «Российский новый университет».

[3] Кандидат психологических наук, доцент, декан юридического факультета АНО ВО «Российский новый университет», член экспертного совета комитета по образованию Государственной думы Федерального собрания Российской Федерации.

[4] Аспирант АНО ВО «Российский новый университет».

опасностей, по нашей оценке, три из четырех относятся к сферам информационной безопасности и информационного противоборства. Причем, эти опасности, именно в таком ключе в Доктрине изложены впервые. Сформулированы такие внутренние военные опасности, как:

а) деятельность, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, дезорганизацию функционирования органов государственной власти, важных государственных, военных объектов и информационной инфраструктуры Российской Федерации;

в) деятельность по информационному воздействию на население, в первую очередь – на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества;

г) провоцирование межнациональной и социальной напряженности, экстремизма, разжигание этнической и религиозной ненависти либо вражды. И хотя в последней разновидности внутренних военных опасностей не называется прямо информационная сфера, очевидно, что сфера информационной безопасности и информационного противоборства является приоритетной для провоцирования социальной напряженности и экстремизма, разжигания ненависти или вражды.

Над детальной разработкой структуры и содержания внешних и внутренних военных опасностей работают сегодня аналитики и специалисты в различных сферах: политологии, информационных технологий, социальной психологии. Недостаточным представляется участие специалистов в области публичного и частного права в доктринальных и прикладных исследованиях вопросов информационной безопасности и информационного противоборства. Подразумевается, что анализ публично-правовых и частноправовых аспектов внешних военных опасностей будут предметом пристального внимания специалистов в области международного публичного и международного частного права, международного гуманитарного права (права вооруженных конфликтов) и права прав человека.

Говоря об анализе внутренних военных опасностей с точки зрения публично-правового и частноправового регулирования информационной безопасности и информационного противоборства, целесообразно, на наш взгляд, наряду с отмеченными выше отраслями права привлекать специалистов в области конституционного, уголовного, административного, военного, информационного права, права интеллектуальной собственности и других отраслей национального права России.

Характеризуя основные черты и особенности современных военных конфликтов, Доктрина наряду с комплексным применение военной силы констатирует применение политических, экономических, информационных и иных мер невоенного характера, реализуемых с широким использованием протестного потенциала населения и сил специальных операций. Другой важнейшей особенностью вооруженных конфликтов является массированное применение систем вооружения и военной техники, высокоточного, гиперзвукового оружия, средств радиоэлектронной борьбы, оружия на новых физических принципах, сопоставимого по эффективности с ядерным оружием, информационно-управляющих систем, а также беспилотных летательных и автономных морских аппаратов, управляемых роботизированных образцов вооружения и военной техники. Доктрина отмечает, что воздействие на противника будет осуществляться на всю глубину его территории одновременно в глобальном информационном пространстве, в воздушно-космическом пространстве, на суше и на море.

Относительной новизной для современной Военной доктрины РФ при характеристике вооруженных конфликтов является акцент на участии в военных действиях иррегулярных вооруженных формирований и частных военных компаний, а также на применении непрямых и асимметричных способов действий.

Определяя цели, задачи и направления деятельности Российской Федерации по сдерживанию и предотвращению военных конфликтов, Доктрина отмечает, что основные задачи Российской Федерации должны быть решены посредством объединения усилий государства, общества и личности по защите Российской Федерации, путем разработки и реализации мер, направленных на повышение эффективности военно-патриотического воспитания граждан Российской Федерации и их подготовки к военной службе. Достижение этих целей возможно за счет создания условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности.

В Доктрине отмечается, что основными задачами развития военной организации являются: повышение эффективности и безопасности функционирования систем государственного и военного управления, обеспечение информационного взаимодействия между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, иными государственными органами при решении задач в области обороны и безопасности; совершенствование военного планирования; совершенствование системы информационной безопасности Вооруженных сил, других войск и органов.

Наконец, определяя задачи оснащения Вооруженных сил, других войск и органов вооружением, военной и специальной техникой, в Доктрине впервые отмечена необходимость развития сил и средств информационного противоборства и качественного совершенствования средств информационного обмена на основе использования современных технологий и международных стандартов, а также единого информационного пространства Вооруженных сил, других войск и органов как части информационного пространства Российской Федерации (ст. 46).

Характеризуя положение России в современном мире, в Стратегии отмечается, что «все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории» (ст. 21). Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий (ст. 22).

Основными угрозами национальной безопасности (государственной и общественной) выступают:

– деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию работы органов государственной власти, уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, устрашение населения, в том числе путем завладения оружием массового уничтожения, радиоактивными, отравляющими, токсичными, химически и биологически опасными веществами, совершения актов ядерного терроризма, нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации;

– деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе.

По мнению экспертов, в настоящее время происходит смещение объекта воздействия с собственно информации (технологий, продуктов, разработок, объектов инфраструктуры) в сторону формирования оборонной политики, деятельности государств в военной сфере и сфере национальной безопасности. Так, выступая на IV Московской конференции по международной безопасности в прошлом году, министр обороны Республики Беларусь генерал-майор Андрей Равков заявил, что «составляющей межгосударственных конфликтов является информационное противоборство, направляемое на дискредитацию внешней и внутренней политики страны – объекта воздействия» [14]. По оценке Минобороны Беларуси, это является серьезным вызовом военной безопасности, а эффективность информационного воздействия становится соизмеримой с военными действиями.

Военное планирование по подготовке планов по применению Вооруженных сил США после событий 11 сентября 2001 года и в последующие годы значительно улучшилось и ускорилось. Действия военных структур всех уровней были кардинально пересмотрены, а оценки ситуаций, в которые могут быть использованы войска США, и перечни экстренных ситуаций, которые требуют быстрого вмешательства с использованием военной силы, были расширены и принципиально изменены. Показательно, что в феврале 2015 года в США была принята новая Стратегия национальной безопасности.

Какие возможные способы реагирования в правовой сфере в рамках информационной безопасности и информационного противоборства могут рассматриваться в современных условиях? Представляется, что наряду с традиционными вариантами разработки нормативных правовых актов по обеспечению национальной безопасности и обороне страны возникает необходимость теоретического обоснования и разработки правовых моделей регулирования сфер информационной безопасности и информационного

противоборства. Такие модели должны отвечать современным вызовам в указанных сферах, а также содержащимся в Доктрине и Стратегии военным угрозам и опасностям, как внешним, так и внутренним.

На необходимость разработки подобных моделей указывают представители профессиональных сообществ: военачальники, юристы, ученые и специалисты в сфере информационной безопасности и права. Так, начальник 8-го управления Генштаба генерал-майор Юрий Кузнецов, выступая на «Инфофоруме-2016» [15], сообщил, что руководители ведущих государств мира пришли к пониманию необходимости правового регулирования в сфере кибербезопасности: «Первым шагом на пути к созданию таких условий послужит пакт об электронном ненападении, который планируется к подписанию под эгидой ООН».

По мнению специалистов, необходимость подобного документа объясняется тем, что «глобализация информатизации общества позволяет использовать современные технологии в целях дестабилизации социальной обстановки внутри государств и информационного воздействия на само население». Пакт об электронном ненападении должен содержать обязательства о соблюдении принципов и правил поведения в киберпространстве. Основное внимание в указанном документе предполагается уделить вопросам недопущения в мирное время атак на критически важные и информационные ресурсы государств.

Необходимо отметить, что Евросоюз подготовил первый нормативно-правовой акт в сфере информационной безопасности, который будут обязаны соблюдать все его члены [3].

Документ содержит требования к финансовым компаниям, коммунальным предприятиям, интернет-компаниям и другим организациям, от которых зависит жизнь общества. Директива Network and Information Security (NIS) Directive в сфере информационной безопасности будет действовать во всех странах Евросоюза после формального утверждения Европарламентом и Европейским советом. Согласно Директиве, компании, владеющие интернет-поисковиками, маркетплейсами и облачными хранилищами, включая такие компании, как Google, Apple, Microsoft и Amazon, интернет-провайдеры и регистраторы доменных имен, должны будут предпринимать соответствующие меры безопасности и уведомлять правительство о любых инцидентах, связанных с информационной безопасностью. То же самое будет касаться кредитных и финансовых организаций, медицинских учреждений и нефтегазовых компаний, коммунальных предприятий, включая электрические сети и водоснабжение, и транспортных компаний (все виды транспорта – авиаперевозки, автомобильные и железные дороги и водное сообщение). Необходимо отметить, что как и все директивы Евросоюза, настоящая Директива предъявляет требования ко всем 28 членам Евросоюза. Правительство каждой страны будет обязано соблюдать указанные в ней требования и создать собственный центр реагирования на инциденты, связанные с компьютерной безопасностью (CERT), а также центра соблюдения директивы в каждом государстве. В России такие центры тоже есть. Один из последних был создан Банком России в июне 2015 г. Он специализируется на хакерских атаках в банковской сфере. Кроме того, согласно Директиве, в Евросоюзе будет создан единый координационный центр по информационной безопасности, который будет служить площадкой для взаимодействия членов Евросоюза**.** Руководство этого центра будет назначено Еврокомиссией. После утверждения Директивы Европарламентом и Европейским советом государства Евросоюза получат 21 месяц на приведение в соответствии с ней собственного законодательства и шесть месяцев на регистрацию всех компаний, которых затрагивают новые правила.

В определенном смысле, такие новеллы в европейском и российском правовых полях определяют необходимость разработки современной методологии правового регулирования информационной безопасности и в особенности – информационного противоборства. Данная методология должна включать различные модели правового регулирования, опираясь на лучшие достижения отечественной и зарубежной правовой мысли, современную систему преподавания и подготовки кадров юристов [8]. Кроме этого, исходя из специфики объекта (информационная и военная безопасность) и предмета регулирования (деятельность по информационному противоборству), научные исследования должны носить комплексный характер. К разработке моделей правового регулирования информационной безопасности и информационного противоборства целесообразно привлечь кроме военных специалистов и специалистов в сфере информационных технологий, юристов, имеющих необходимые наработки в сфере публичного и частного права. Информационная область как объект правового регулирования подразделяется на ряд основных предметных сфер.

Среди них можно выделить: сбор и распро-

странение различных видов информации; формирование информационных ресурсов, подготовка информационных продуктов и оказание информационных услуг; реализация права на поиск, обработку, оценку, передачу и использование информации; создание и применение информации, информационных технологий и средств их обеспечения; разработка и применение на практике средств и методов информационной безопасности.

Этот перечень необходимо дополнить еще одной сферой информационных отношений – сферой информационного противоборства. Остановимся подробнее на том, что представляет собой сфера информационного противоборства как объект правового регулирования.

В публикациях правовое регулирование в сфере информационного противоборства рассматривается как целенаправленное правовое воздействие (в том числе применение) специальной системы собственно юридических средств на взаимоотношения между субъектами мирового сообщества или политической системы, в рамках которых одни субъекты путем активного информационно-психологического воздействия на информационную сферу других субъектов стремятся получить превосходство над противостоящей стороной в экономической, политической, военной или иной областях. Цель правового регулирования в сфере информационного противоборства – обеспечение гарантированной с позиций закона информационной безопасности и защиты публичных и частных интересов указанных субъектов, упорядочение информационных отношений противоборствующих сторон и приведение их в соответствие с нормами права. Информационные отношения характеризуются при этом наличием определенных субъектов информационной деятельности (государств, государственных органов, организаций, СМИиК, граждан и пр.); объектов (информации, информационных систем, технологий, Интернета и др.); связей между субъектами и объектами через информационные отношения; наличием норм различных отраслей права, используемых в ходе правового регулирования.

Современный период развития информационного противоборства [4] характеризуется его особым обострением и выходом на качественно новый уровень, что обусловлено следующими факторами:

– информатизацией основных областей деятельности большинства государств;

– быстрыми темпами формирования глобальной информационной инфраструктуры и превращением ее в базисный элемент жизнедеятельности мирового сообщества;

– значительными достижениями в развитии информационных технологий воздействия на сознание, волю и чувства людей;

– активным развитием программно-технических средств нанесения ущерба компьютерным и телекоммуникационным системам;

– недостаточным уровнем развития средств и методов обеспечения защиты национальных информационных пространств, сознания населения;

– несовершенством государственной информационной политики;

– отсутствием механизма правового регулирования в сфере информационного противоборства, в том числе норм международного права, устанавливающих международную ответственность государств – инициаторов информационно-психологической агрессии.

Статья 20 проекта Доктрины информационной безопасности Российской Федерации (далее – Доктрины ИБ) характеризует нынешнее состояние правового регулирования в сфере информационной безопасности и противоборства как «отсутствие норм регулирования межгосударственных отношений в информационном пространстве и соответствующих международно-правовых механизмов, учитывающих специфику информационных технологий» [5]. Такое состояние правового регулирования затрудняет формирование системы международной информационной безопасности, призванной содействовать стратегической стабильности и способствовать равноправному стратегическому партнерству. Деятельность государственных органов в сфере обеспечения информационной безопасности Российской Федерации, по мнению разработчиков проекта Доктрины ИБ, должна основываться на следующих принципах: законность и правовое равенство всех участников общественных отношений в информационной сфере, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом; соблюдение баланса между потребностью граждан и общества в свободном обмене информацией и необходимыми ограничениями на распространение информации в целях обеспечения национальной безопасности, в том числе в информационной сфере.

В Доктрине ИБ отмечается, что стратегической целью обеспечения информационной безопасности в области стратегической стабильности

и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

Обеспечение информационной безопасности Российской Федерации в области стратегической стабильности и равноправного стратегического партнерства должно быть направлено:

– на поддержание суверенитета Российской Федерации в информационном пространстве путем реализации самостоятельной и независимой политики в целях защиты национальных интересов в информационной сфере;

– на содействие в формировании системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационных технологий в агрессивных, террористических, экстремистских и криминальных целях;

– на создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

– на развитие национальной системы управления российским сегментом сети «Интернет» при ведущей роли государств в этом процессе.

Эксперты отмечают [6], что реализация национальных интересов в информационной сфере должна быть нацелена на формирование безопасной среды оборота достоверной информации в интересах обеспечения конституционных прав и свобод граждан, устойчивого социально-экономического развития страны, а также национальной безопасности. Еще одна угроза, отмеченная в Доктрине, касается возрастающих масштабов компьютерной преступности, прежде всего в денежно-кредитной, валютной, банковской сферах и иных сферах финансового рынка. Кроме того, увеличивается число инцидентов, связанных с нарушением законных прав граждан на защиту личной и семейной тайны, персональных данных при использовании информационных систем и сетей связи.

Как отмечено в документе, методы, способы и средства совершения преступлений с использованием информационных технологий становятся всё изощреннее.

На необходимость разработки мер адекватного правового регулирования в сфере информационной безопасности отмечает Председатель Следственного комитета РФ А.И. Бастрыкин в своей статье «Пора поставить действенный заслон информационной войне»: «Представляется целесообразным предусмотреть внесудебный (административный) порядок включения информации в федеральный список экстремистских материалов, а также блокировки доменных имен сайтов, которые распространяют экстремистскую и радикал-националистическую информацию. При этом, если обладатели такой информации не считают ее экстремистской, пусть сами обжалуют соответствующие действия уполномоченных госорганов в суд и доказывают там свою правоту» [7]. По его мнению, целесообразно в этом плане (по вопросу определения пределов цензурирования в Интернете) опираться на опыт зарубежных государств, противостоящих США и их союзникам. В связи с беспрецедентным информационным давлением ряд стран пошли на ограничения иностранных СМИ в целях защиты национального информационного пространства.

По решению китайских властей, с 10 марта 2016 года введен запрет на работу электронных СМИ, полностью или частично принадлежащих иностранным резидентам. Такие СМИ больше не смогут распространять информацию через Интернет, в лучшем случае – посредством печатных изданий. Согласно этому решению, китайские СМИ сотрудничают с иностранными онлайн-СМИ компаниями только при наличии разрешения министерства промышленности и информатизации Китая. В руководстве национальных СМИ смогут работать только граждане Китая, а серверы онлайн-СМИ компаний могут находиться только в КНР.

Необходимы унифицированный перечень оснований для ограничений и перечень случаев прямого ограничения прав и свобод с последующим их закреплением в законе.

Итак, на основании вышесказанного, можно сделать следующие выводы:

1. На сегодняшний день ответственность за международную информационную деятельность обычно не предусматривает применения санкций к государству – нарушителю норм и носит преимущественно рекомендательный характер.

2. Конвенцию о международном праве опровержения подписали всего около 10 государств, и на практике механизм передачи опровержения не действует.

3. Международное публичное право отводит государству роль гаранта прав человека на информацию, которые регулируются непосредственно международно-правовыми нормами. При этом почти всегда возникают коллизии между нормами международного публичного права и частного права, международного гуманитарного права, права прав человека и национального (внутригосударственного) права.

4. Реализация основных прав и свобод граждан в информационной сфере относится к числу национальных интересов всех государств, в том числе и России. Она основывается на сочетании принципов свободы информации, суверенитета государств и необходимости защиты публичных интересов в этой сфере. Эти принципы закреплены в основных международных правовых документах, в Конституции Российской Федерации и ряде других законов, а также в новой Военной доктрине РФ, Стратегии информационной безопасности РФ и проекте Доктрины информационной безопасности.

5. Реализуемые в новых нормативных документах РФ ограничения в области прав и свобод человека в сферах информационной безопасности и противоборства должны быть оправданными и соразмерными той цели, которая преследуется этими ограничениями. При этом должна учитываться как цель, которая преследуется ограничением (в этом случае играет роль ценностное содержание «пограничного» права или интереса), так и цель существования и реализации права, которое ограничивается. Если свобода слова ограничивается в целях защиты нравственности населения, то помимо определения цели ограничения, ценностного содержания охраняемого интереса (нравственности) должна учитываться и цель существования свободы слова, ее ценностный критерий.

Государство отвечает за обеспечение в рамках своей юрисдикции права человека на информацию и свободу слова в объеме, определенном в международных документах, в первую очередь – в Международном пакте о гражданских и политических правах, где в ст. 19 сказано:

1. Каждый человек имеет право беспрепятственно придерживаться своих мнений.

2. Каждый человек имеет право на свободное выражение своего мнения; это право включает свободу искать, получать и распространять всякого рода информацию и идеи независимо от государственных границ устно, письменно, посредством печати или художественных форм выражения, или иными способами по своему выбору.

Возможные ограничения в реализации указанных прав должны быть установлены законом и являться необходимыми:

а) для уважения прав и репутации других лиц;

б) для охраны государственной безопасности, общественного порядка, здоровья и нравственности населения [10].

Так, статья 20 Пакта содержит указания на конкретные виды информации, запрещенные для распространения международным правом:

«Всякая пропаганда войны должна быть запрещена законом. Всякое выступление в пользу национальной, расовой или религиозной ненависти, представляющее собой подстрекательство к дискриминации, вражде или насилию, должно быть запрещено законом».

Соответственно, государства – участники Пакта обязаны запретить распространение этих видов информации на своей территории и с нее в законодательном порядке.

Статья 10 Конвенции о защите прав и основных свобод человека, принятой Советом Европы в 1950 году, провозглашает право человека на свободное выражение мнений, на «получение и распространение информации и идей без вмешательства публичных властей и независимо от государственных границ» [11]. Конвенция (п. 2 ст. 10) предусматривает возможность ограничений права на информацию, которые могут быть связаны с обеспечением национальной безопасности, территориальной целостности или общественного порядка, с предупреждением беспорядков или преступлений, с охраной здоровья или нравственности, с защитой репутации или прав других людей, с предупреждением обнародования информации, полученной конфиденциальным путем, или с поддержанием авторитета или беспристрастности судебных властей.

Впоследствии право человека на свободу информации было закреплено в Международном пакте о гражданских и политических правах 1966 года, ставшем основным международно-правовым документом в этой области. Декларация 1948 года является резолюцией Генеральной Ассамблеи ООН и носит рекомендательный характер, в отличие от Пакта, имеющего обязательную юридическую силу. Следовательно, при определении права человека на свободу информации необходимо ориентироваться на положения ст. 19 и 20 Международного пакта о гражданских и политических правах человека.

Универсальность норм пактов, ограничивается тем, что они не были ратифицированы рядом стран (США, Бельгией, ЮАР, Швейцарией и др.). Некоторые государства (Нидерланды, Швеция, Дания, Финляндия и др.) сделали оговорки о праве на информацию относительно ст. 19 и 20 Международного пакта о правах [12].

В ноябре 1997 года в парламенте Японии рассматривался законопроект о «предотвращении шпионской деятельности», положения которого можно было бы использовать для ущемления свободы слова и печати. В законопроекте пред-

усматривалось тюремное заключение за разглашение государственной тайны, но этому понятию не дано четкого определения. Согласно проекту, обвинение не обязано доказывать, что разглашение «государственной тайны» поставило под угрозу национальную безопасность. Отсутствие четких критериев создавало возможность различных интерпретаций положений законопроекта, произвольного ограничения свободы слова и печати [13].

Таким образом, концепция «неограниченности» права человека на информацию не воплощается в законодательной практике большинства государств. Предложения закрепить в международных документах понимание права человека на свободу информации не подкреплено практикой.

Из этого сравнительного анализа можно сделать следующий вывод: если основные информационные права и свободы человека и гражданина закреплены во всех перечисленных документах и одинаковы по своему содержанию – универсальны, то основания их возможного ограничения и прямые ограничения, устанавливаемые государствами, существенно различаются.

Несмотря на существование достаточно разработанных положений международного и национального механизмов правового регулирования в области информации и коммуникации, этот механизм во многом отстает от тех задач, которые имеются в сфере распространения информации, осуществления коммуникации и информационного противоборства.

Так, в современных условиях требуют дальнейшей научной и практической разработки следующие основные проблемы публично-правового и частноправового регулирования информационной сферы:

– координация международно-правового и национального механизмов правового регулирования информационной сферы, в первую очередь – сферы новых ИКТ;

– исследование структуры и содержания национальных правовых моделей регулирования реализации права на сочетание свободы информации и свободы информировать в условиях информационного противоборства;

– установление и определение баланса публичного и частного интересов в доступе к источникам информации;

– мониторинг правоприменения (в рамках международной и национальной юрисдикций) в сфере обеспечения информационной безопасности государства, личности и общества;

– создание системы подготовки кадров для реализации моделей правового обеспечения информационной безопасности и противоборства.

Таким образом, анализ проблем правового регулирования обеспечения информационной безопасности показывает, что оно должно осуществляться на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности органов государственной власти Российской Федерации во взаимодействии с органами местного самоуправления, организациями различных форм собственности, общественными организациями и гражданами. Публично-правовые и частноправовые аспекты информационной безопасности и информационного противоборства нуждаются в дальнейшей научной разработке, для эффективного ее функционирования необходима система международного (преимущественно для стран, входящих в интеграционные объединения постсоветского пространства) и межведомственного взаимодействия, а также интеграции в системе подготовки кадров [9] и повышения квалификации.

Литература

1. Указ Президента Российской Федерации от 31 декабря 2015 года № 683 «О Стратегии национальной безопасности Российской Федерации».

2. Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 № Пр-2976).

3. http://www.comss.info/page.php?al=Evrosoyuz_podgotovil_pervyj_normativno_pravovoj_akt_v_sfere_IB

4. Воронцова Л.В., Фролов Д.Б. История и современность информационного противоборства. – М. : Горячая линия – Телеком, 2006.

5. Электронный ресурс: http://www.scrf.gov.ru/documents/ 6/135.html

6. Электронный ресурс: https://rg.ru/2016/06/24/sovbez-opublikoval-novuiu-doktrinu-informbezopasnosti-rf.html

7. Электронный ресурс: http://www.kommersant.ru/doc/2961578

8. Тыртышный А.А. Методология исследования теории права и государства как мировоззренческой основы формирования правосознания юристов // Вестник Российского нового университета. – 2013. – Выпуск 3. – С. 7–11.

9. Тыртышный А.А., Понаморенко В.Е., Коровяковский Д.Г. О правовом исследовании интеграционных процессов на постсоветском пространстве // Вестник Российского нового университета. – 2010. – Выпуск 4. – С. 5–6.

10. GA Res. 2200 A/XXI/, 21 UN GAOR, Supp. 16 and 49, UN Doc. A./6316.

11. Council of Europe // European Treaty Series. – No. 5.

12. GA Res. 2200 A/XXI/, 21 UN GAOR, Supp. 16 and 49, UN Doc. A. /6316.

13. Круглов Е.В. Массовая коммуникация в Восточной и Юго-Восточной Азии: тенденции развития накануне XXI века // От книги до Интернета. Журналистика и литература на рубеже нового тысячелетия. – М. : МГУ, 2000.

14. http://nvo.ng.ru/concepts/2016-04-22/1_flowers.html

15. https://m.lenta.ru/news/2016/02/04/electronic/