*УДК 327.8*
*ГРНТИ 11.25.25*

# ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА В СОВРЕМЕННЫХ НАУЧНЫХ ИССЛЕДОВАНИЯХ

*Е.С. ПОЛУНИН, кандидат исторических наук*
*ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)*

Статья посвящена анализу научной литературы по теме информационной безопасности государства. Особое внимание уделено особенностям понятийного аппарата исследований, оценкам политической и научной актуальности и значимости проблемы, мнению отечественных исследователей об угрозах информационной безопасности России и их рекомендациям по защите информационного пространства страны.

*Ключевые слова:* информационная безопасность, информационное пространство, информационные угрозы, информационное оружие, информационные войны.

## THE STATE INFORMATION SECURITY ISSUE IN CONTEMPORARY SCIENTIFIC RESEARCH

*E.S. POLUNIN, Candidate of Historical Sciences*
*MESC AF «N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh)*

The article is devoted to the analysis of scientific literature on the topic of the state information security. Particular attention is paid to the peculiarities of the conceptual research apparatus, assessing the political and scientific relevance and significance of the problem, the opinion of domestic researchers about threats to Russia's information security and their recommendations for protecting the country's information space.

*Keywords*: information security, information space, information threats, information weapons, information wars.

**Введение.** В настоящее время в научных кругах, среди политиков, государственных и военных деятелей все чаще обсуждаются проблемы информационной безопасности государства как одной из составляющих более широкого понятия национальной безопасности. Возрастание интереса к этому вопросу обусловлено как воздействием долговременных факторов, в первую очередь, связанных с бурным развитием информационных технологий, так и влиянием последних политических событий, заставивших говорить о своего рода втором издании «Холодной войны» между западными государствами и Россией. Ввиду этих внешнеполитических обстоятельств много внимания уделяется геополитическому измерению проблемы, поэтому наряду с техническими и юридическими активизировались также политологические и социально-философские исследования на тему информационной безопасности.

**Актуальность.** Так как положения, сформулированные в научных и публицистических трудах по проблемам информационной безопасности оказывают влияние на формирование общественного мнения и на выработку политической линии по соответствующим вопросам, предпринятый в настоящей статье анализ основных идей их авторов представляется научно значимым и актуальным.

**Задачи.** Объектом изучения в данной работе выступает безопасность государства в информационной сфере, а предметом – российские исследования в этой области. В частности, предлагается обратиться к анализу понятийного аппарата рассматриваемых научных публика-



СОДЕРЖАНИЕ

ций (спектр применяемых понятий, расхождения в интерпретации устоявшихся терминов и введение новых), к оценкам их авторами актуальности и значимости проблемы в политическом и военном измерениях, к особенностям восприятия зарубежного опыта защиты информационного суверенитета, к обсуждению в отечественной научной и публицистической литературе актуальных для России информационных угроз и возможных мероприятий по их предупреждению и устранению. В основе методологии предпринятого исследования лежат методы научного анализа и обобщения (синтеза), кроме того, активно применялись общелогические и сравнительный методы, в частности, при сопоставлении позиций различных авторов по отдельным аспектам проблемы.

Для введения в проблематику вначале следует рассмотреть основные понятия, используемые в анализируемой научной и публицистической литературе. Многие из них по форме и содержанию в той или иной степени соотносятся с устоявшимися в общественно-политической практике категориями, другие только пробивают себе дорогу в научный и политический лексикон. Центральное для рассматриваемой проблематики понятие информационной безопасности относится к числу сравнительно новых для России. В советский период истории страны оно не получило широкого распространения [1, с. 71]; и лишь с 1990-х гг. внедрялось вначале в понятийный аппарат теории национальной безопасности, а уже оттуда перешло в официальный язык общения политиков и экспертов [2, с. 206]. В общих чертах информационная безопасность государства понимается как защищенность национальных интересов в информационной сфере. Таким образом, исходным понятием для его определения выступают национальные интересы (баланс интересов личности, общества и государства) [3, с. 48–49]. Их реализация, как и в случае с национальными интересами и национальной безопасностью в целом, считается целью государственной политики по обеспечению информационной безопасности [4, с. 12]. В качестве примеров конкретного содержания этой политики исследователи называют предотвращение несанкционированного доступа к защищаемой информации; защита государственных информационных ресурсов, обеспечение реализации прав и свобод граждан и государства в информационной сфере [12, с. 206]. Ни у кого не вызывает сомнений важность технических аспектов защиты информационного пространства государства. Однако в России практически с самого начала обеспечение информационной безопасности трактовалось шире, и предполагало также недопущение вмешательства внешних сил в определение приоритетов и в реализацию внутренней и внешней политики государства через средства массовой информации и коммуникаций [5, с. 82–83]. Поэтому в научной литературе проблема ввиду ее важности для политических, юридических, социальных и философских наук зачастую выводится за рамки технической [1, с. 72, 75].

В условиях глобализации информационное пространство отдельно взятой страны не может существовать изолировано, информационные угрозы также приняли международный характер. Поэтому наряду с национальным измерением рассматриваемой темы в литературе также активно обсуждается понятие международной информационной безопасности как состояния системы взаимоотношений между государствами, предусматривающего защищенность отдельных стран и мирового сообщества от исходящих из глобального информационного пространства угроз безопасности [6, с. 55–56].

Некоторые исследователи активно поддерживают идею внедрения в теорию и практику информационной безопасности понятия национального информационного суверенитета [5, с. 82]. В частности, М.М. Кучерявый, понимая под ним верховенство и независимость государственной власти в формировании и проведении политики в национальном и глобальном информационном пространстве, предлагает использовать этот термин наряду с понятиями идеологического, экономического и военного суверенитета [4, с. 11–12, 9–10]. А Д.Л. Сивоволов отмечает необходимость применения понятия национального информационного суверенитета ввиду того, что информационная безопасность в настоящее время стала неотъемлемой составляющей почти всех видов человеческой деятельности [5, с. 82]. В рамках такого подхода может исполь-



СОДЕРЖАНИЕ

зоваться набор более узких понятий, например, цифрового суверенитета (в сфере информационно-коммуникативных технологий), ментального суверенитета (защита национальной идеи и культурной самоидентификации нации), государственной политики информационного суверенитета [4, с. 12–13].

Одно из важнейших понятий рассматриваемой проблематики – угрозы в информационной сфере жизни общества, то есть условия и факторы, представляющие опасность для личности, социума, государства и их интересов в информационном пространстве. Угрозы информационной безопасности связывают с объективными проявлениями противоречий и разногласий между отдельными индивидуумами, социальными общностями и странами [6, с. 56]. В этой связи под информационными угрозами понимаются действия стран, преступных и террористических групп с целью ущемления национальных интересов России, нарушения конституционного строя, подрыва идеологических устоев, подмены ценностей российского общества [7, с. 51]. По своим источникам угрозы подразделяются на внешние и внутренние. К первым относят, например, противодействие реализации национальных интересов в глобальном информационном пространстве, вытеснение российских компаний из мирового рынка информационных технологий; а к внутренним информационным угрозам – отставание страны по уровню и темпам информатизации, в развитии информационных систем [4, с. 11–12]. По объектам и форме воздействия угрозы информационной безопасности подразделяются на информационно-технические (хакерские и вирусные атаки) и информационно-психологические (информационные кампании, пропаганда).

Ввиду бурного развития современных информационно-коммуникативных технологий к угрозам в информационно-технической области неизменно сохраняется высокий интерес. Проблемы киберпреступлений и кибербезопасности, защищенности информационных систем от преступлений в сфере и с применением новейших информационных технологий, постоянно обсуждаются учеными, политиками и общественными деятелями [5, с. 85–86]. В частности, отмечается углубление и расширение угроз в этой области: внедрение незащищенной зарубежной информационной техники, увеличение объема научно-технических публикаций (что затрудняет контроль утечки информации ограниченного доступа), активизация международного сотрудничества фирм и предприятий, рост числа пользователей Интернета и социальных сетей, увеличение объема памяти и скорости обработки информации [8, с. 787–789]. Отмечается постоянно появление их новых форм – кибершпионаж, хищение информации у производителей SIM-карт, киберкражи у банков и т.д. [6, с. 60–66].

Особую актуальность в последнее время приобрели и информационно-психологические угрозы, ведь, с одной стороны, наблюдается увеличение роли политической составляющей в обеспечении национальной безопасности, а с другой – усиление влияния информационных факторов на политические процессы [4, с. 8]. Поэтому все большие опасения вызывают возможные последствия информационного воздействия на психику и сознание отдельных людей и социальных групп, на общественные настроения и мнение масс, на национальное самосознание и идеологические установки [3, с. 51; 9, с. 108]. Нельзя не согласиться с общепризнанным мнением, что современные государства заинтересованы в формировании в глобальном информационном пространстве положительного образа страны, что является немаловажным условием успеха внешней политики.

Как уже отмечалось выше, субъектами борьбы в информационном пространстве выступают не только государства, но и различные негосударственные формирования: от отдельных личностей и групп до транснациональных корпораций, международных террористических и преступных организаций [3, с. 53; 5, с. 87]. В этой связи особое внимание приковано к террористическим угрозам в глобальном информационном пространстве. Международные террористические организации успешно осваивают широчайший спектр возможностей, предоставляемый им современными информационно-коммуникативными технологиями: организация кибератак, нападения на информационные системы различных объектов инфраструктуры, пропаганда идей



СОДЕРЖАНИЕ

и рекрутирование новых сторонников. В частности, в распространении своей идеологии и мобилизации новых кадров через Интернет-ресурсы особенно преуспела запрещенная в России террористическая организация Исламское государство (ИГ) [8, с. 792; 6, с. 55–60].

С информационной безопасностью и угрозами тесно связаны понятия информационного противоборства и войны. Под информационным противоборством понимается разворачивающееся в информационном пространстве соперничество государств, их борьба за ресурсы и за преимущества дальнейшего развития [3, с. 50]. Как и в случае с информационными угрозами, выделяется информационно-техническое (радиоэлектронная, акустическая, компьютерная борьба [3, с. 51]) и информационно-психологическое противоборство (пропаганда, информационные кампании) [10, с. 26].

Все чаще в научной литературе и в общественно-политическом дискурсе встречается понятие информационных войн в их техническом и политическом понимании. В первом случае речь идет о борьбе за своевременность, достоверность, полноту; скорость получения, переработки и доведения информации [7, с. 55]. Так называемые кибервойны сопровождаются целенаправленными массированными атаками на компьютерные серверы, сети, базы данных. Такие кибератаки могут проводить мобильные, небольшие строго засекреченные группы, нередко с территории третьих стран; что существенно затрудняет их обнаружение и организацию противодействия их активности [8, с. 791]. Целью информационных войн в политической области являются переформатирование общественного мнения, дискредитация суверенитета и политического режима, нарушение общественного порядка, разжигание вражды в ее различных проявлениях [6, с. 55–58].

Явление информационного противоборства не ново. Борьба за умы масс имела место и в войнах прошлого, например, в форме пропаганды и агитации. По мере развития средств массовой информации (СМИ) и коммуникаций они все активнее использовались для воздействия на убеждения масс. Одной из таких стратегий влияния на общественные настроения была так называемая общественная дипломатия, практикуемая странами НАТО [10 с. 27–28]. Однако лишь благодаря революционному развитию средств массовых коммуникаций, Интернета, изобретению социальных сетей на современном этапе истории человечества информационные войны приобрели глобальный и сетевой характер, были перенесены в глобальную виртуальную реальность, значительно расширили состав участников (одновременно сделав его менее прозрачным) [5, с. 84–85].

Войны в информационном пространстве ведутся при помощи информационного оружия, в этом понятии исследователи объединяют самый широкий спектр средств уничтожения, искажения, хищения информации, получения или ограничения доступа к информационным системам, нарушения функционирования информационной техники и сетей [7, с. 51]. Так, в кибератаках применяются компьютерные вирусы, логические бомбы, программы-оборотни и убийцы информации, средства несанкционированного доступа к информационным ресурсам и подавления информационных систем и т.д. [7, с. 55]. А для политической борьбы в информационной сфере используются методы трансформации информационного пространства, механизмы воздействия на взгляды отдельных людей и на общественное мнение [3, с. 48]. Как отмечает, например, К.Ю. Чугунова, средством информационно-психологического воздействия выступают сами люди и культура в ее различных проявлениях [11, с. 60]. Современная наука предложила немало новейших способов влияния на настроения, взгляды и убеждения масс, например, нейролингвистическое программирование. С другой стороны, в этой области до сих пор широко и эффективно используются давно проверенные методы – дезинформация, замалчивание и искажение фактов (в современных исследованиях такое явление иногда называют «фейковая война» [2, с. 206–207]), обеспечение монополии на производство и распространение информации. К тому же в информационных войнах нашего времени большую роль продолжают играть традиционные средства массовой информации [12]. Базовым элементом любого информационно-психологического оружия остается специально разработанный контент, который распространя-



СОДЕРЖАНИЕ

ется различными доступными средствами с целью заданного воздействия на взгляды населения той или иной страны или мировой аудитории в целом [6, с. 55–58]. Показательный пример приводит А.Ю. Маруев: во время войны в Югославии при участии американских специалистов создавались специальные сайты с целью добиться поддержки местным населением военных действий, поэтому в размещаемых там текстах широко использовались слова «беженцы», «этнические чистки», «массовые убийства» [3, с. 52–53].

Таким образом, понятийный аппарат отечественных исследований проблемы безопасности в информационной сфере до сих пор находится в стадии становления: пересматривается содержание устоявшихся определений, предлагаются новые понятия, заимствуются термины из зарубежной науки и практики. Такое положение вещей связано с бурным развитием современных информационных технологий и информационно-коммуникативного пространства, в котором постоянно возникают новые реалии, требующие научного описания и встраивания либо в существующую, либо в новую систему представлений. На основе выше изложенных представлений о важнейших понятиях в рассматриваемых исследованиях обратимся к анализу их основных идей по поводу актуальности, научной и политической значимости проблемы, а также состояния защищенности информационного пространства России.

Политическая актуальность и даже злободневность темы информационной безопасности последние несколько лет зачастую увязывается с информационной кампанией против России, стартовавшей в западных и украинских средствах массовой информации на фоне развития украинского кризиса [2, с. 206]. События на Украине считаются точкой отсчета для полномасштабной информационной войны против России. Предпринимаемые в ходе нее прозападными информационными агентствами попытки дискредитировать политику России в регионе и на международной арене в целом [13, с. 75, 77] способствовали привлечению внимания к проблеме защиты национальных интересов в информационном пространстве. С другой стороны, не упускается из виду и тот факт, что сами западные страны, несмотря на свое лидерство в области информационно-коммуникативных технологий, оказались уязвимы перед угрозами в информационной сфере. В качестве примера можно назвать многочисленные скандалы с утечкой личной и конфиденциальной информации политиков, видных представителей бизнеса и культуры [13]. Таким образом, актуальность отечественных исследований проблемы информационной безопасности объясняется, в первую очередь, значимыми для России процессами в глобальном информационном пространстве, однако учитываются и международные события в этой области.

Несмотря на востребованность проблемы в общественно-политическом дискурсе, многие авторы отмечают ее слабую изученность в научной литературе. Если в технических и экономических дисциплинах информационной безопасности в последние годы уделяется достаточно много внимания, то в социальных и гуманитарных науках фиксируется нехватка соответствующих исследований [5, с. 82–83]. В частности, некоторые авторы указывают на почти полную неисследованность информационных войн как одной из форм международных конфликтов [3, с. 51]. Тем не менее, уже сформировался определенный массив отечественных исследований проблемы информационной безопасности, что позволяет выделить в них ряд общих моментов и главные идеи, определить особенности изучения темы в России.

В рассматриваемых работах много места отводится обоснованию военно-политической значимости обеспечения информационной безопасности государства с учетом как исторического опыта, так и современных реалий. Одним из наиболее часто встречающихся исторических примеров для иллюстрации разрушительной силы информационного оружия является обращение к итогам идеологической войны между Соединенными Штатами и Советским Союзом. Распространено мнение, что распад СССР и блока социалистических стран во многом оказался подготовлен воздействием западной массовой потребительской культуры на умы населения [3, с. 49]. Кроме того, встречаются ссылки на эффективность американских информационно-психологических операций в вооруженных конфликтах конца XX – начала XXI вв. (в Югославии, Ираке, Ливии и Сирии), а также на успехи западного воздействия на протестные настрое-



СОДЕРЖАНИЕ

ния в самых разных странах мира (например, в Грузии и на Украине) [2, с. 207]. В этих событиях западные специалисты прибегали как к традиционным формам информационного воздействия (агитация и пропаганда), так и к новейшим (использование средств массовой коммуникации для формирования общественного мнения) [3, с. 52–53].

Гораздо больше внимания уделяется роли информационной сферы на современном этапе развития общества, из этого положения выводится идея особого значения защиты информационного пространства для обеспечения национальной безопасности в целом. Практически все исследователи значимость проблемы информационной безопасности увязывают с активным проникновением информационно-коммуникативных технологий в основные виды человеческой деятельности [4, с. 11], с качественной трансформацией всех сфер жизни современного общества под воздействием информационных факторов (например, во многом, под влиянием новейших информационных технологий сформировалась новая система управления [8, с. 785]), с определяющей ролью информации и информационных технологий в мировом развитии. Отмечается зависимость экономических, политических, военных и прочих успехов современного государства от уровня развития национального информационного пространства. Из этих положений делается вывод о том, что защищенность информации в наши дни превратилась в одно из важнейших условий политической, экономической, финансовой, военной и других видов безопасности [3, с. 47] (неслучайно даже предлагается ставить информационную безопасность в один ряд с экономической [1, с. 72]). Кроме того, в литературе можно также встретить интересную мысль о том, что информационно-коммуникативные технологии не только существенно изменили традиционные сферы жизни и деятельности общества, но и создали параллельную виртуальную реальность, глобальное информационное пространство, функционирующее по своим собственным законам [4, с. 8]. Одним словом, исследователи проблемы информационной безопасности научную значимость своей темы неизменно связывают с тем, что на современном этапе истории информационный фактор превратился в один из важнейших для развития человеческого общества в целом, а значит и для обеспечения его безопасности, в частности.

Еще одним аргументом в пользу чрезвычайной важности защиты информационного пространства государства является мощный разрушительный потенциал информационного оружия как в его техническом (например, хакерские атаки), так и в информационно-психологическом понимании (агитация, пропаганда, дезинформация). В первом случае объектами информационных атак могут выступать различные виды инфраструктуры; системы связи, управления и разведки; базы информации; компьютерные сети [3, с. 51]. По мнению американских специалистов, наиболее уязвимы перед кибератаками объекты энергетики, телекоммуникации, авиационные диспетчерские системы, государственные информационные структуры, системы автоматизированного управления войсками и оружием [8, с. 792]. Кибероперации приносят не только серьезный материальный ущерб, но и могут привести к человеческим жертвам [6, с. 55–59].

В последнее время все больше внимания привлекает к себе информационно-психологическое оружие, что не в последнюю очередь связано, как уже упоминалось выше, с обострением информационного противоборства западных стран и России. Его активнейшее использование в современном геополитическом противостоянии государств мира в научной литературе объясняется малыми издержками, широкими возможностями и высокой эффективностью данного типа оружия. Информационно-психологические средства воздействия на противника, не требуя привлечения огромных материальных и человеческих ресурсов, позволяют решать масштабные политические задачи [3, с. 47]. Их действие направлено не на материальные объекты, а на умы и образ мыслей населения. Их цель – дискредитация государственной идеологии, режима, политической системы, приоритетов внутренней и внешней политики [2, с. 207]. Информационно-психологическое оружие способно повлиять на настроения и предпочтения масс, привести к размыванию их политической и национальной самоидентификации, способствовать их культурной дезинтеграции [11, с. 62]. Результаты целенаправленного вмешательства в информационное пространство той или иной страны могут быть самыми значимыми – от ос-



СОДЕРЖАНИЕ

лабления политических противников до их подчинения воли внешних сил и даже полной смены правительств и режимов [3, с. 51] (в этой связи иногда отмечается, что информационные атаки опасны не столько своим прямым воздействием, сколько возможными масштабными последствиями [1, с. 75]). Многие исследователи указывают также на следующие обстоятельства, определяющие преимущества информационно-психологического оружия: высокая проницаемость государственных границ для информационных потоков [4, с. 11], оперативность информационного воздействия и возможность охватить самую широкую аудиторию [3, с. 48], способность действовать скрытно [11, с. 59], слабость нормативно-правового регулирования сферы информационной безопасности (что касается как ведения информационных войн [3, с. 50], так и совершения киберпреступлений [6, с. 55–60]), перманентный характер информационного противоборства [1, с. 75].

Мысль об огромной разрушительной силе информационного оружия, которое некоторые эксперты предлагают относить, ни много ни мало, к оружию массового поражения [11, с. 61], зачастую подкрепляется также обращением к современной политике и прогнозам западных стран в области информационных войн. Передовые зарубежные страны активно финансируют как разработку новой информационной техники и технологий [8, с. 786], так и развитие средств воздействия на общественное сознание (так называемых технологий «управляемого хаоса» [6, с. 67–68] и «цветных революций» [2, с. 207], а также прочих механизмов реализации политики «мягкой силы» [10, с. 27]). Эти два магистральных направления тесно связаны. Не вызывает сомнений, что бурный прогресс информационно-коммуникативных технологий, в частности, Интернета и социальных сетей, открыл новые огромные возможности для управления настроениями масс [5, с. 84–85].

Ввиду выше сказанного, отечественные исследователи склонны соглашаться с западными специалистами, прогнозирующими дальнейшее увеличение роли защиты информационного пространства в обеспечении национальной безопасности [1, с. 74], постепенное вытеснение информационной экспансией прочих форм геополитической борьбы между государствами, превалирование в войнах будущего информационных средств воздействия на противника (военные действия в будущем, возможно, будут ограничиваться подавлением жизненно важных информационных систем врага) [3, с. 47], ускорение развития именно наступательных видов информационного оружия [8, с. 790].

Рассмотренные нами положения отечественных исследований проблем информационной безопасности, в конечном счете, призваны проиллюстрировать чрезвычайную важность вопроса защиты информационного пространства для России. Достаточно широко распространено мнение о том, что информационная война западных стран против Российской Федерации с самого начала была связана с геополитической борьбой за контроль над пространствами бывшего Советского Союза. По мере вступления России на путь ориентированной на национальные интересы внешней политики это противоборство начало усиливаться, в том числе, в информационной сфере [3, с. 49]. Ученые и политики сходятся в том, что с невероятной силой информационная война против России развернулась после государственного переворота в Киеве. В западном освещении событий на Украине Россия предстает агрессором [13, с. 76–77], обвиняется в империализме, в приверженности жестких действий на международной арене, в поддержке правых политических сил [2, с. 208]. Широко обсуждается и то, что отдельным направлением дискредитации образа России стали попытки пересмотра на западе роли нашей страны в истории, прежде всего, Второй мировой войны и советской эпохи [13, с. 78].

Исследователи выделяют широкий спектр внутренних и внешних угроз информационной безопасности Российской Федерации. Примерами первых могут выступить нарушения прав и свобод в информационной сфере, несовершенство правовой базы функционирования средств массовой информации. К внешним информационным угрозам относят распространение за рубежом искаженных и заведомо ложных сведений о политике России, иностранное влияние на выработку внешнеполитической линии страны, раскрытие зарубежными разведывательными



СОДЕРЖАНИЕ

службами государственной тайны и конфиденциальных сведений [1, с. 73; 9, с. 110], распространение пропагандируемых западными средствами массовой информации и несвойственных российскому обществу ценностей [9, с. 114], усиление зависимости духовной и общественной жизни России от зарубежных информационных структур [10, с. 31].

Уязвимость России перед угрозами информационного характера в литературе связывается с политическими, экономическими и социальными проблемами страны. В 1990-е гг. Российская Федерация не уделяла должного внимания всему комплексу вопросов обеспечения национальной безопасности ввиду глубокого политического и социально-экономического кризиса в государстве [4, с. 8]. Обозначившееся тогда отставание в организации информационной безопасности со временем все больше усугублялось превосходством некоторых передовых стран мира (США, Япония, Франция, ФРГ) в области информационно-коммуникативных технологий. В этой сфере у данных государств уже накопился огромный потенциал для дальнейшего упрочения своего политического, экономического и военного лидерства [8, с. 786]. Слабая защищенность российского общества от информационно-психологических угроз зачастую объясняется нерешенностью некоторых социально-экономических проблем, неразвитостью институтов гражданского общества, неэффективностью образовательной системы и органов управления [9, с. 109–110], открытостью российского информационного пространства влияниям извне, и даже безыдейностью и низким культурным уровнем населения [1, с. 74]. В этой связи высказываются особые опасения по поводу возможности использования внешними силами потенциала социального недовольства населения России [5, с. 87].

При анализе проблемы информационной безопасности и выработке рекомендаций по ее обеспечению в России многие отечественные исследователи обращаются к соответствующему западному опыту. В настоящее время отмечается активизация усилий США и их союзников по продвижению западных ценностей и политического мировоззрения в самых разных регионах мира [3, с. 48]. Корни этой политики следует искать в истории «Холодной войны» с ее идеологическим противостоянием капиталистической и социалистической систем. Хотя в 1990-е гг. в самих Соединенных Штатах интерес к информационному противоборству несколько угас, все же приемы и технологии информационных войн продолжали развиваться. К примеру, в НАТО в середине 1990-х гг. прошло обновление содержания политики общественной дипломатии. В частности, особое внимание было решено уделять формированию общественного мнения относительно блока и его политики, в первую очередь, в странах-партнерах, в 2001 г. при альянсе возникло даже специальное Управление общественной дипломатии. В США финансирование проектов и программ в сфере информационной безопасности активизировалось с начала 2000-х гг. А после терактов 11 сентября 2001 г. американские эксперты сформулировали весьма показательные основные принципы информационной политики США: добиваться понимания иностранной аудиторией американской политики как она есть (на самом деле, а не в соответствии с мнением о ней); интерпретировать политические шаги США с упором на их рациональность и обоснованность фундаментальными ценностями; соблюдать последовательность, правдивость и убедительность при обращении в мировых средствах массовой информации; подготавливать целевые обращения с учетом особенностей аудитории; проявлять активность в коммуникации с мировой общественностью всеми доступными средствами, интенсивно привлекать партнеров для повышения убедительности сообщений; активно проводить обмены делегациями [10, с. 27–29]. В современных Соединенных Штатах информационные угрозы ставятся в один ряд с терроризмом и распространением оружия массового поражения. К защите информационной безопасности привлекаются американские силовые ведомства: Агентство национальной безопасности (АНБ) и Министерство обороны. Еще в 2009 г. в рамках Стратегического командования США было сформировано Киберкомандование, что говорит о том, что вопросу придается стратегическое значение. Хотя в США действуют специальные войска психологической борьбы, все же приоритет в защите национальной информационной безопасности отдается ее техническим аспектам, а не информационно-психологическим [12; 5, с. 86]. И все-таки, несмот-



СОДЕРЖАНИЕ

ря на огромные ресурсы и большое внимание к проблеме, Соединенные Штаты не добились неуязвимости перед информационными угрозами [8, с. 790].

У исследователей не возникает сомнения, что для обеспечения информационной безопасности России необходима самая активная государственная политика на этом направлении [3, с. 51], и даже более того – консолидация всех сил государства и общества [12]. Как отмечает А.Ю. Маруев, глобально может быть два пути защиты национального информационного пространства – обеспечение превосходства над противниками в информационной сфере или поиск ассиметричных ответов. Нельзя также не согласиться с мыслью о том, что универсальных рецептов в этой области нет, каждый раз к решению проблем нужно будет подходить творчески [3, с. 52, 54].

Предлагаемые исследователями мероприятия по обеспечению информационной безопасности страны могут быть объединены в группы: политические, организационные, правовые, технические, экономические и прочие меры [12]. Исходным пунктом в информационной политике, по мнению многих авторов, является выработка стратегических приоритетов, определение национальных интересов и основных путей их реализации [4, с. 13; 3, с. 49]. Большинство авторов сходятся во мнении, что базовым принципом национальной информационной политики должно стать сохранение и упрочение в общественном сознании национальных ценностей, патриотизма и гуманизма [7, с. 52–53]. Исходя из этого, предлагается, например, создать механизмы контроля над внутренними и поступающими извне информационными потоками и системы защиты от пропаганды чуждых ценностей, выработать меры защиты информационного суверенитета страны на международной арене [4, с. 13], развивать возможности государственных средств массовой информации по своевременному и качественному доведению информации о политике России, создавать государственные электронные информационные ресурсы [7, с. 53]. Кроме того, одной из важнейших задач для государства в этой области считается развитие образования и повышение культурного уровня населения [1, с. 75].

Много места в литературе отводится необходимости выстроить четкую и эффективную нормативно-правовую базу защиты информационной безопасности России [11, с. 63; 7, с. 56]. Наличие в Российской Федерации специальной доктрины информационной безопасности признается важнейшим условием для дальнейшего развития правового регулирования соответствующих вопросов [12], однако, по замечанию К.Ю. Чугуновой, ощущается нехватка создаваемых на базе доктрины законов [11, с. 61]. Нередко можно услышать о необходимости достаточно жестких мер защиты информационного пространства России, например: введения электронных биометрических паспортов, развития сети видеонаблюдения, ограничения свободы слова для противодействия террористической пропаганде, организации слежения за абонентами через систему сотовой связи [1, с. 72]. Однако при этом большинство авторов предостерегают от опасности нарушения прав (свобода получения и распространения информации, соблюдение тайны личной жизни и переговоров, право на защиту чести и доброго имени, свобода совести, мысли и слова [11, с. 60]) и несоблюдения интересов граждан в информационной сфере. В качестве решения предлагается обеспечить баланс между защитой государства от информационных атак и обеспечением прав граждан на доступ к открытой информации [6, с. 67–68; 4, с. 9–10]; между интересами отдельных личностей, общества и государства [7, с. 52]; между безопасностью и свободой [1, с. 72]. Условием этого, по мнению большинства авторов, является строгое соблюдение слова и духа Конституции страны при разработке нормативно-правовых документов по защите информационной безопасности [7, с. 52; 1, с. 74; 8, с. 794].

Как и следовало ожидать, важным условием безопасности России в информационной сфере считается развитие отечественных информационно-коммуникативных технологий и производства информационной техники в стране [5, с. 82–83; 3, с. 50]. В рамках обеспечения информационно-технической защищенности российского информационного пространства предлагается, в частности, усилить государственную поддержку исследований и производств в информационной сфере (причем с выходом на международные рынки) [7, с. 53], обеспечить защи-



СОДЕРЖАНИЕ

щенность национальных информационных и телекоммуникационных систем (прежде всего, военных и важнейших инфраструктурных) [3, с. 50], активизировать разработку отечественных аппаратных и программных средств защиты информации, совершенствовать систему защиты государственной тайны [7, с. 53–54], создавать национальные государственные защищенные информационные сети [4, с. 13], развивать систему подготовки специалистов в области информационной безопасности [3, с. 50]. На пути развития собственной информационной техники и технологий не представляется возможным отказываться от сотрудничества с передовыми зарубежными производителями в данной области [3, с. 50, 52]. Однако оно, разумеется, должно быть организовано таким образом, чтобы не создавать угрозу безопасности национального информационного пространства. Отдельной важной задачей является обеспечение информационной безопасности в военной области (например, создание собственных информационных войск, развитие средств и приемов информационного противоборства) [4, с. 13].

Еще одним важнейшим условием обеспечения информационной безопасности считается научное исследование угроз в этой сфере, причем как информационно-технического, так и информационно-психологического характера. Например, предлагается развивать базу данных об информационных угрозах [6, с. 69], создать систему мониторинга настроений населения по поводу важнейших вопросов безопасности [9, с. 108–109]. А уже на основе подобных исследований должны вырабатываться приемы и механизмы ведения информационных войн и обеспечения информационной безопасности [3, с. 50] (например, методики повышения мотивации и морально-психологической устойчивости, в особенности, обеспечивающего защиту информации персонала [7, с. 57]).

Наконец, многие авторы отмечают, что в условиях развития глобального информационного пространства ни одна страна не в состоянии в одиночку справиться со всеми исходящими из него информационными угрозами [6, с. 56]. Отсюда выводится мысль о необходимости активнейшего участия России в усилиях международного сообщества по обеспечению глобальной информационной безопасности. В литературе предлагается развивать сотрудничество в этой области как с ближайшими союзниками, так и с другими странами, невзирая на существующие противоречия [8, с. 795–796; 6, с. 69]. В частности, речь идет об участии российских специалистов в формулировке принципов и норм международного права в сфере информационной безопасности [4, с. 13], в международных программах исследования информационных угроз, в организации коллективных действий международного сообщества против атак в информационном пространстве и т.д. [6, с. 55–56].

**Выводы.** Таким образом, тема информационной безопасности государства все чаще привлекает внимание отечественных исследователей, причем на фоне активизации информационной войны западных стран против России особый интерес в последние годы стала вызывать проблема защищенности информационного пространства страны не только от чисто технических, но и от информационно-психологических угроз. Понятийный аппарат теории информационной безопасности постоянно пополняется новыми терминами ввиду бурного развития как информационно-коммуникативных технологий, так и появления новых вызовов и угроз в киберпространстве. Научная и политическая значимость проблемы защиты информационного пространства страны исследователями связывается с ростом роли информационных факторов в развитии всех сфер жизни современного общества, а также с бурной эволюцией методов и приемов ведения информационных войн, которые по прогнозам специалистов, если и не вытеснят остальные формы войны, то, во всяком случае, займут важное место в конфликтах будущего. В исследовательской литературе уязвимость информационной сферы России перед внешними и внутренними атаками связывается с отставанием от ведущих стран в информационной технике и технологиях, с нерешенностью в стране некоторых социально-экономических проблем, с неразвитостью нормативно-правового регулирования в области СМИ и массовых коммуникаций. Для обеспечения информационной безопасности России исследователи призывают государство активнейшим образом заняться формированием и реализацией четкой информаци-



СОДЕРЖАНИЕ

онной политики, нацеленной на обеспечение соответствующих национальных интересов, предупреждение и пресечение угроз информационного характера.

## СПИСОК ЛИТЕРАТУРЫ

1. Лазарев А.Ю., Скопец П.С. Информационная безопасность в системе национальной безопасности государства // Вестник Российской правовой академии. 2006. № 4. С. 71–75.

2. Кузина С.И., Мякинченко Д.А. Информационное насилие: аспекты национальной безопасности // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 3. С. 205–209.

3. Маруев А.Ю. Информационная безопасность России и основы организации информационного противоборства // Контуры глобальных трансформаций: политика, экономика, право. 2010. Вып. 1. Том 3. С. 47–54.

4. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2014. № 9(69). С. 7–13.

5. Сивоволов Д.Л. Новые угрозы национальному суверенитету России в сфере национальной безопасности // Социум и власть. 2015. № 6(56). С. 82–88.

6. Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность». 2016. № 1(3). С. 54–72.

7. Лопатин Ю.Н. Информационная безопасность в России. Проблемы, поиски решений // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. 2008. № 2. С. 51–57.

8. Богачев В.Я., Редин В.В. Информационная безопасность как составная часть национальной безопасности Российской Федерации // Стратегия гражданской защиты: проблемы и исследования. 2012. № 2. Т. 2. С. 785–797.

9. Сарычев Н.В., Мельниченко Д.В. Внешние и внутренние угрозы информационной безопасности России // Российский психологический журнал. 2010. Том. 7. № 5–6. С. 108–114.

10. Рогозин А.Д. «Общественная дипломатия» НАТО: информационная безопасность России // Власть. 2008. № 9. С. 26–32.

11. Чугунова К.Ю. Информационное оружие как угроза национальной безопасности Российской Федерации // Актуальные проблемы российского права. 2015. № 7(56). С. 59–64.

12. Сизьмин М.А. Информационная (информационно-психологическая) безопасность в структуре национальной безопасности (на примере США и России) [Электронный ресурс] // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). Электронный научный журнал. 2014. № 3. Режим доступа: http://eizvestia.isea.ru (дата обращения: 14.08.2018).

13. Фролкин П.П., Шишкин Д.П. Информационная война против России и национализм на Украине как актуальная угроза национальной безопасности РФ // Информационная безопасность регионов. 2014. № 2(15). С. 75–79.

## REFERENCES

1. Lazarev A.YU., Skopets P.S. Informatsionnaya bezopasnost' v sisteme natsional'noy bezopasnosti gosudarstva // Vestnik Rossiyskoy pravovoy akademii. 2006. № 4. P. 71–75. (in Russian).

2. Kuzina S.I., Myakinchenko D.A. Informatsionnoe nasilie: aspekty natsional'noy bezopasnosti // Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski SKAGS. 2015. № 3. P. 205–209. (in Russian).



СОДЕРЖАНИЕ

3. Maruev A.YU. Informatsionnaya bezopasnost' Rossii i osnovy organizatsii informatsionnogo protivoborstva // Kontury global'nyh transformatsiy: politika, ehkonomika, pravo. 2010. Vyp. 1. Tom 3. P. 47–54. (in Russian).

4. Kucheryavyy M.M. Gosudarstvennaya politika informatsionnogo suvereniteta Rossii v usloviyah sovremennogo global'nogo mira // Upravlencheskoe konsul'tirovanie. 2014. № 9(69). P. 7–13. (in Russian).

5. Sivovolov D.L. Novye ugrozy natsional'nomu suverenitetu Rossii v sfere natsional'noy bezopasnosti // Sotsium i vlast'. 2015. № 6(56). P. 82–88. (in Russian).

6. Kazarin O.V., Skiba V.YU., SHaryapov R.A. Novye raznovidnosti ugroz mezhdunarodnoy informatsionnoy bezopasnosti // Vestnik RGGU. Seriya «Dokumentovedenie i arhivovedenie. Informatika. Zashhita informatsii i informatsionnaya bezopasnost'». 2016. № 1(3). P. 54–72. (in Russian).

7. Lopatin YU.N. Informatsionnaya bezopasnost' v Rossii. Problemy, poiski resheniy // Gumanitarnye issledovaniya v Vostochnoy Sibiri i na Dal'nem Vostoke. 2008. № 2. P. 51–57. (in Russian).

8. Bogachev V.YA., Redin V.V. Informatsionnaya bezopasnost' kak sostavnaya chast' natsional'noy bezopasnosti Rossiyskoy Federatsii // Strategiya grazhdanskoy zashhity: problemy i issledovaniya. 2012. № 2. V. 2. P. 785–797. (in Russian).

9. Sarychev N.V., Mel'nichenko D.V. Vneshnie i vnutrennie ugrozy informatsionnoy bezopasnosti Rossii // Rossiyskiy psihologicheskiy zhurnal. 2010. Tom. 7. № 5–6. P. 108–114. (in Russian).

10. Rogozin A.D. «Obshhestvennaya diplomatiya» NATO: informatsionnaya bezopasnost' Rossii // Vlast'. 2008. № 9. P. 26–32. (in Russian).

11. CHugunova K.YU. Informatsionnoe oruzhie kak ugroza natsional'noy bezopasnosti Rossiyskoy Federatsii // Aktual'nye problemy rossiyskogo prava. 2015. № 7(56). P. 59–64. (in Russian).

12. Siz'min M.A. Informatsionnaya (informatsionno-psihologicheskaya) bezopasnost' v strukture natsional'noy bezopasnosti (na primere SSHA i Rossii) [EHlektronnyy resurs] // Izvestiya Irkutskoy gosudarstvennoy ehkonomicheskoy akademii (Baykal'skiy gosudarstvennyy universitet ehkonomiki i prava). EHlektronnyy nauchnyy zhurnal. 2014. № 3. Rezhim dostupa: http://eizvestia.isea.ru (data obrashheniya: 14.08.2018). (in Russian).

13. Frolkin P.P., SHishkin D.P. Informatsionnaya voyna protiv Rossii i natsionalizm na Ukraine kak aktual'naya ugroza natsional'noy bezopasnosti RF // Informatsionnaya bezopasnost' regionov. 2014. № 2(15). P. 75–79. (in Russian).



Полунин Евгений Сергеевич, кандидат исторических наук, старший научный сотрудник 14 отдела научно-исследовательского 1 управления научно-исследовательского научно-исследовательского центра (проблем применения, обеспечения и управления авиацией Военно-воздушных сил), Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А, evgeny.polunin1989@yandex.ru.



СОДЕРЖАНИЕ