

**УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

*ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и  
Ю.А. Гагарина» (г. Воронеж)*

*Tishin M.A., Polunin E.S.*

**THREATS OF INFORMATION SECURITY OF THE RUSSIAN  
FEDERATION**

*MESC AF «N.E. Zhukovsky and Y.A. Gagarin  
Air Force Academy» (Voronezh)*

**Реферат:** *Статья посвящена анализу существующих и потенциальных угроз информационной безопасности Российской Федерации. Акцентируется внимание на том, что на сегодняшний день информационная война может быть крайне эффективным средством для борьбы с противниками. Основной целью государственной политики по обеспечению информационной безопасности является нейтрализация потенциальных и реальных информационных угроз, ограничение всего спектра негативного информационного влияния на страну. Государственная политика РФ в области информационной безопасности нуждается в совершенствовании: при сохранении генеральных целей, задач и принципов необходимо изменить механизмы ее реализации, особенно, по отдельным направлениям.*

**Ключевые слова:** *Российская Федерация; информационная война; национальная безопасность; угроза.*

---

<sup>1</sup>Тишин Максим Андреевич – младший научный сотрудник 14 ОНИ НИЦ (ППО и УА ВВС) ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

<sup>2</sup>Полунин Евгений Сергеевич – к.и.н., старший научный сотрудник 14 ОНИ НИЦ (ППО и УА ВВС) ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

**Abstract:** *The article is devoted to the analysis of the existing and potential threats of information security of the Russian Federation. The attention is focused that today information war can be extremely effective remedy for fight against opponents. The main purpose of the state policy of Russia is information security. Policy needs to be improved.*

**Keywords:** *Russian Federation; information war; national security; threat.*

В истории Российской Федерации (как и других стран мира) первые элементы угроз информационного характера появились достаточно давно, и вплоть до XX в. главными из них оставались различные формы пропагандистского воздействия (в частности, пропаганда Смутного времени). После Первой мировой войны и Октябрьской революции в России, а, особенно, с началом «Холодной войны», информационное противоборство разворачивалось, в первую очередь, как идеологическая война. Советское руководство много внимания уделяло защите информационного пространства страны от влияния извне, в основном, используя механизмы фильтрации входящей информации. Однако в современных условиях бурного развития информационных технологии, формирования глобального информационного пространства и превращения информационной сферы в важнейший фактор развития страны Россия не может изолиро-

ваться от мировых информационных процессов и должна искать альтернативные и в то же время эффективные способы обеспечения своей информационной безопасности [2].

Для современной Российской Федерации опасность представляют следующие угрозы в информационной сфере: распространение идей и концепций, направленных на разжигание национальной, социально-политической, религиозной вражды; призывы к нарушению суверенитета и территориальной целостности государства; опасность кибератак на важнейшие информационно-технические системы страны (военные системы управления и связи, ВПК, транспортные системы и другие); нарушение прав в информационной сфере (например, авторского); террористическая активность в информационном пространстве; разведывательно-подрывная деятельность иностранных спецслужб; разглашение секретной информации (составляющих государственную тайну сведений и прочей конфи-

циальной информации, значимой для обеспечения национальных интересов); дискредитация политики России и авторитета отдельных российских государственных деятелей; ограничение прав граждан на доступ к информации (если это не предусмотрено законом); распространение в СМИ культуры жестокости и насилия; неразвитость информационной инфраструктуры и рынка высокотехнологической продукции; научно-техническая отсталость страны и многое другое [7].

Исходной точкой для предотвращения и пресечения угроз информационного характера является выработка учеными, аналитиками, общественными и политическими деятелями концептуальных основ российской политики по обеспечению информационной безопасности. Общая стратегия информационной политики должна базироваться на результатах глубокого научного осмысления современного состояния как национальной, так и глобальной информационной безопасности. На этом пути предстоит сделать еще многое, к тому же на фоне бурного развития информационной сферы и быстрого появления в этой связи все новых угроз их научное исследование должно продолжаться постоянно.

В целом эксперты и политики сходятся в том, что основной целью государственной политики по обеспечению информационной безопасности является нейтрализация потенциальных и реальных информационных угроз, ограничение всего спектра негативного информационного влияния на страну. В связи с этим выделяется спектр задач государства в данной области: обеспечение неприкосновенности прав и свобод граждан относительно распоряжения информацией, защита национального рынка информационных и высоких технологий [9], расширение информационно-аналитических возможностей государства; информационное обеспечение системы национальной безопасности; выявление и пресечение подрывной и антироссийской информационной деятельности внутри страны и за ее пределами; борьба с активностью террористических группировок в информационном пространстве; предотвращение, выявление и пресечение киберпреступлений и правонарушений на рынке высокоточных технологий и информации; мониторинг информационной безопасности и информационной среды; противодействие несанкционированному проникновению в информационную инфраструктуру и базы данных органов национальной безопасности и государ-

ственных органов Российской Федерации; охрана конфиденциальной информации государственной тайны и другие.

Разнообразные задачи государственной политики в сфере обеспечения информационной безопасности могут быть условно объединены в группы: нормативно-правовые, финансово-экономические и организационно-методические. Сама стратегия и приоритеты усилий государства в данной сфере находят свое оформление в нормативных документах. Источником и базой законодательства в области информационной безопасности являются основные положения Конституции РФ, в которой закреплено право граждан на тайну переписки и переговоров (ст. 23), принцип неприкосновенности личных данных (ст. 24), право свободного использования информации (за исключением охраняемых государством сведений) и на доступ к данным об экологической ситуации (ст. 42)[3]. Эти основополагающие идеи получили развитие в прочих законодательных актах, регулирующих вопросы обеспечения информационной безопасности. Например, ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006г. регламентирует отношения, связанные с правами на поиск, полу-

чение, обработку, хранение, передачу, производство и распространение информации; а также отношения, возникающие при использовании информационных технологий и при защите информации[11]. Важнейшим событием в ходе формирования концептуальных основ информационной политики России стало принятие 5 декабря 2016 г. Доктрины информационной безопасности Российской Федерации. В этом документе были сформулированы цели, задачи, принципы, направления обеспечения государством информационной безопасности страны. Доктрина для дальнейшего определения конкретных очертаний политики в данной области предлагает три генеральные цели: защита конституционных прав и свобод граждан в сфере информации; развитие информационного и телекоммуникационного пространства; охрана информационных и телекоммуникационных систем.

Наряду с правовыми методами государство много внимания уделяет организационно-технической защите информации. За последние десятилетия созданы специализированные информационно-телекоммуникационные системы в органах власти, различные системы защиты государственной тайны и информации. Ввиду постоянного

появления все новых технических возможностей в сфере информационных технологий, инженерно-техническая защита информационных ресурсов государства требует особого внимания и больших капиталовложений [10] для создания и применения новых и эффективных технических средств защиты информации от несанкционированного доступа (сооружения, аппаратные средства, программное обеспечение). Организационные меры защиты информации связаны с урегулированием отношений между исполнителями (используют информацию), с организацией режима охраны информации (работа с документами, техническими средствами сбора, обработки, передачи и хранения данных)[4].

Информационная сфера, по сравнению с другими, по ряду причин особенно подвержена процессам глобализации, поэтому Российская Федерация много внимания уделяет налаживанию международного сотрудничества по предупреждению и устранению угроз информационной безопасности. Приоритеты соответствующей политики государства определены в принятых в соответствии с положениями Конституции РФ, Доктрины информационной безопасности и Закона об информации Основых государственной политики

РФ в области международной информационной безопасности на период до 2020 г. В этом документе сформулированы следующие важнейшие цели: создание системы международной информационной безопасности, предотвращение противоправного использования информационных и коммуникационных технологий с целью нанесения вреда обществу, формирование и совершенствование международного сотрудничества суверенных государств в информационной сфере. В российской политике обеспечения глобальной информационной безопасности выделяются такие направления как: утверждение российских инициатив по разработке и принятию мировым сообществом решений в сфере информационной безопасности; осуществление международных многосторонних совещаний экспертов в области информационной безопасности (БРИКС, «Группа двадцати» и другие) и развитие диалога о перспективах использования экспертного потенциала государств-партнеров; интернационализация управления сетью Интернет и выдвижение соответствующих инициатив РФ; совершенствование кадровой политики занимающихся обеспечением международной информационной безопасности органов; развитие глобальной методологической базы

информационной безопасности и прочие [8].

Несмотря на существенный прогресс в обеспечении национальной информационной безопасности в последние годы государственная политика в этой сфере не лишена недостатков и требует дальнейшего совершенствования. Так, ее нормативно-правовая база сохраняет свою противоречивость, к тому же действующие законы полностью не охватывают все актуальные проблемы информационной безопасности. Недостаточно внимания получает информационно-аналитическая деятельность: развитие здесь идет медленными темпами и, по большей части, экстенсивным путем [5]. Ощущается нехватка четкой координации действий центральных органов и властей регионального уровня в сфере обеспечения информационной безопасности (в целом проблеме регулирования региональных информационных рынков уделяется мало внимания). Требуется улучшение кадровой политики в информационной области (профессиональный уровень занятых в сфере защиты информации работников нередко требует повышения). Одной из центральных проблем остается техническое отставание отечественной информационной инфраструктуры и ее зависимость от поступле-

ний иностранной техники, недостаточное развитие российского телекоммуникационного производства. Остро стоит вопрос недостаточного финансирования: ввиду непростой общей экономической ситуации инвестирование информационных структур (как государственных, так и частных), новых технологий в сфере информации и связи проводится по остаточному принципу. Многие проблемы в рассматриваемой области связаны со слабыми позициями России на международном рынке информации и информационных технологий. Допускается экспансия в РФ зарубежных производителей информационной продукции, а они при этом реализуют агрессивную рыночную стратегию при недостаточной информационной инициативе России на международной арене. Недостаточно внимания уделяется задаче информирования о нашей стране в международных СМИ и информационном пространстве (зачастую за рубежом информация о нас либо не доходит, либо сохраняются устаревшие и традиционные клише) [6].

Таким образом, государственная политика РФ в области информационной безопасности нуждается в совершенствовании: при сохранении генеральных целей, задач и принципов необходимо изменить механиз-



мы ее реализации, особенно, по отдельным направлениям. Обратимся к некоторым рекомендациям экспертов. Необходимо провести оптимизацию правового, научно-технического, методического и организационного сопровождения системы обеспечения информационной безопасности России. Среди правовых мероприятий особенно актуальной для нас остается защита интеллектуальной собственности. Особого внимания заслуживает кадровый вопрос, в частности, важно сформировать единую систему кадровой работы и подготовки специалистов в области информационных технологий и информационной безопасности. Непременным условием, как нашей безопасности, так и прогресса в целом является развитие отечественных информационных продуктов, телекоммуникаций – все это требует усиленных инвестиций. Особенно уязвимым остается интернет-пространство. Чтобы изменить положение здесь, требуется совершенствовать нормативную базу обеспечения информационной безопасности в сети Интернет, включая борьбу

с киберпреступлениями, например, шпионажем, распространением компьютерных вирусов.

На фоне развернувшейся против нашей страны в последние годы информационной войны важно в мировом информационном пространстве задействовать все возможности российской «мягкой силы» (в Интернете, через вещающие за рубежом государственные каналы (RussiaToday), чтобы довести до внутренней и международной аудитории достоверную и полную информацию о нашей стране, государстве, политике РФ: официальную позицию государства по принципиальным для нас вопросам, нашу интерпретацию тех или иных событий. Не менее значима популяризация за рубежом российских национальных культурных продуктов (фильмы, музыка, различные национальные бренды); она позволяет формировать общее положительное впечатление о России в сознании иностранцев; защищать национальные ценности и идеив глазах и самих россиян, и мировой общественности [1].

### ***Список литературы***

1. Зорина Е.Г. Информационный суверенитет современного государства и основные инструменты его обеспечения // Известия Саратовского университета. Серия Социология, Политология. 2017. Т. 17. Вып. 3. С. 345-348.

2. Караванская А. Информационная политика РФ на современном этапе. М.: LAP LambertAcademicPublishing, 2014. 112 с.
3. Конституция РФ от 12.12.1993 с изм. и доп. от 21.07.2014. СПб.: Питер, 2015. 64 с.
4. Литвинов В.А. Основы национальной безопасности России. М.: Ленанд, 2014. 328 с.
5. Лишманова Н.А. Информационная безопасность Российской Федерации //Гуманитарные знания и естественные науки: современные проблемы и перспективы развития. Материалы III Межвузовской научно-практической конференции / под общ.ред. Е.В. Корлюк. Минск: БГУ, 2014. С. 094-097.
6. Марков А. Процессы формирования информационной безопасности общества. М.: LAP LambertAcademicPublishing, 2011. 532 с.
7. Назмутдинова Р.Р. Информационная безопасность как вид безопасности в информационном обществе //Управление человеческими ресурсами. 2014. № 1(6). С. 51-54.
8. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. URL: <http://www.scrf.gov.ru/documents/6/114.html> (дата обращения: 11.11.2018).
9. Панарин И.Н. Информационная война, PR и мировая политика. Курс лекций. М.: Горячая линия – Телеком, 2014. 352 с.
10. Чеботарева А.А. Человек и электронное государство. Право на информационную безопасность. Чита: Изд-во ЧитГУ, 2011. 159 с.
11. Федеральный Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149–ФЗ. М.: Омега–Л, 2007. 66 с.

### *References*

1. Zorina E.G. Informacionnyjsuverenitetsovremennogogosudarstva i osnovnyeinstrumenty ego obespecheniya // IzvestiyaSaratovskogouniversiteta. Seriya-Sociologiya, Politologiya. 2017. T. 17. Vyp. 3. S. 345-348.
2. Karavanskaya A. Informacionnayapolitika RF nasovremennomehtape. М.: LAP Lambert Academic Publishing, 2014. 112 s.
3. Konstituciya RF ot 12.12.1993 s izm. idop. ot 21.07.2014. SPb.:Piter, 2015. 64 s.



4. Litvinov V.A. Osnovynacional'nojbezopasnostiRossii. M.: Lenand, 2014. 328 s.
5. Lishmanova N.A. Informacionnayabezopasnost' RossijskojFederacii //Gumanitarnyeznaniya i estestvennyenauki: sovremennyyeproblemy i perspektivyrazvitiya. Materialy III Mezhvuzovskojnauchno-prakticheskoykonferencii / pod obshch. red. E.V. Korolyuk. Minsk: BGU, 2014. S. 094-097.
6. Markov A. Processyformirovaniyainformacionnojbezopasnostiobshchestva. M.: LAP Lambert Academic Publishing, 2011. 532 s.
7. Nazmutdinova R.R. Informacionnayabezopasnost' kak vid bezopasnosti v informacionnomobshchestve //Upravleniechelovecheskimiresursami. 2014. № 1(6). S. 51-54.
8. OsnovygosudarstvennojpolitikiRossijskojFederacii v oblastimezhdunarodnojinformacionnojbezopasnostina period do 2020 goda. URL: <http://www.scrf.gov.ru/documents/6/114.html> (data obrashcheniya: 11.11.2018).
9. Panarin I.N. Informacionnayavojna, PR i mirovayapolitika.Kurslekcij. M.: Goryachyaliniya – Telekom, 2014. 352 s.
10. Chebotareva A.A. Chelovek i ehlektronnoegosudarstvo. Pravonainformacionnuyubezopasnost'. CHita: Izd-voCHitGU, 2011. 159 s.
11. Federal'nyjZakon RF «Ob informacii, informacionnyhtekhnologiyah i o zashchiteinformacii» ot 27.07.2006 № 149–FZ. M.: Omega–L, 2007. 66 s.