Шушков Георгий Михайлович

Центр перспективного анализа и стратегических исследований, эксперт

Сергеев Илья Витальевич

Центр перспективного анализа и стратегических исследований, эксперт

E-mail: Ilyasergeev1@yandex.ru

Концептуальные основы информационной безопасности Российской Федерации

Библиографическая ссылка на статью: Шушков Г.М., Сергеев И.В. Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл.: Е.А. Куренкова и др. – М.: ИИУ МГОУ, 2016. – С. 69 – 76.

Аннотация

В условиях возрастающей роли информационной сферы значительно увеличивается количество угроз информационной безопасности РФ. Отечественные концепции, при определении указанного рода угроз ориентируются на их обособление, разделяя угрозы информационного характера и «традиционные» угрозы национальной безопасности РФ. В статье предпринята попытка рассмотрения концептуальных основ информационной безопасности РФ с подхода включения информационных угроз в традиционное понимание угроз национальной безопасности РФ.

Ключевые слова

Информационная безопасность РФ, информационные угрозы, информационная сфера, интересы РФ в информационной сфере, информационное противоборство, информационное противодействие.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, являющейся важным фактором

общественной, социальной, политической и военной сфер государственной деятельности. Это обусловлено тем, что продолжается научно-техническая революция в области вычислительной техники и связи, расширяется потребность социально активной части населения в расширении информационного взаимодействия как внутри государства, так и за его пределами. «Расширение информационного обмена происходит в условиях реализации конституционных прав граждан на свободу экономической, информационной и интеллектуальной деятельности» [6, с. 101]. Информационная и интеллектуальная деятельность инициирует геополитическое взаимодействие мирового сообщества, которое осуществляется сегодня, прежде всего, в информационном пространстве. Это порождает значительное количество угроз национальной безопасности, ключевой среди которых является использование данного пространства для проведения операций информационно-психологической войны». По указанной проблеме, в Доктрине информационной безопасности РФ отмечено: «источником внешней угрозы информационной безопасности Российской Федерации является разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним» [1]. Приходится констатировать, что законодатель при определении возможных угроз информационного характера делает акцент на информационных угрозах технического характера, и в недостаточной степени конкретизирует характер иных возможных угроз. Необходимо отметить, что информационное противоборство (война) предполагает использование информации в качестве оружия по трем основным направлениям. Первое направление это воздействие на сознание объекта влияния через информационные технологии. Второе направление ориентировано на подсознание объекта

влияния посредством использования психологических методов воздействия. Третье направление предполагает использование кибертехнологий для воздействия на информационную инфраструктуру в целом. Указанные направления могут использоваться противоборствующими субъектами в информационном конфликте, как по отдельности, так и в комплексе. В рамках настоящей статьи будут рассмотрены концептуальные основы обеспечения информационной безопасности РФ от угроз, возникающих от использования ее политическими оппонентами, террористическими и экстремистскими организациями, криминальными структурами информационных технологий.

Необходимо отметить, что последнее время политические оппоненты России, международные террористические и экстремистские организации, а также криминальные структуры, активно используют методы информационного противоборства для достижения своих целей, что, в свою очередь, свидетельствует о появлении совершенно нового вида угроз национальной безопасности РФ. Данный факт вызывает необходимость формирования российской, адекватной современным реалиям, концепции обеспечения безопасности государства от угроз информационного характера. Это обуславливает потребность в комплексном научно-методическом анализе сущности и природы информационного пространства, процессов, протекающих в нем, специфики информационного конфликта, угроз информационной безопасности РФ в информационной сфере, формулирования понятийного аппарата изучаемой сферы в целях формировании концептуальных основ информационной безопасности РФ.

Несмотря на то, что вопросы информационной безопасности нашли свое отражение в трудах многих отечественных ученых, большинство актуальных положений остается не раскрытыми. Причиной этого является заблуждение большинства исследователей относительно сущности и природы информационных угроз. Практически во всех научных трудах указанные угрозы рассматриваются обособленно от «традиционных» видов

угроз. Они выделяются в самостоятельный вид и исследователи стремятся определить их отличия, классифицировать отдельно от «традиционных» видов угроз национальной безопасности. По нашему мнению, указанная позиция является ошибочной ввиду того, что развитие информационных технологий на сегодняшний день обусловило активное использование информации практически во всех сферах общественной жизни. Террористические организации, организуя террористические акты, преследуют цель устрашения населения и, как следствие, получение влияния. Но информация об организованной, например, в Африке террористической акции, вряд ли бы дошла до населения РФ без использования соответствующих каналов коммуникации. Для этого террористы используют Интернет, а именно социальные сети в Интернете, каналы на видеохостингах в Интернете, которые за считанные часы набирают миллионы просмотров. Усугубляет ситуацию многократное описание во всех деталях террористической акции в новостных лентах по телевидению. Таким образом, о террористическом акте узнает практически все население планеты. Цель террористов достигнута, посеян страх среди населения. Для этого были использованы информационные методы, которые в конкретной ситуации были частью террористической акции, которая, в свою очередь, является одним из видов угроз национальной безопасности РФ. Подобные примеры можно привести ко всем «традиционным» видам угроз национальной безопасности РФ. Приведенное положение вызывает необходимость переосмысления концептуальных основ информационной безопасности РФ с позиций «включения» информационных угроз национальной безопасности РФ в традиционное понимание угроз национальной безопасности.

Большинство современных ученых утверждают, что информационное противоборство протекает в информационном пространстве. Но ни в одном из трудов не дается полное толкование указанного термина. Его определение представляется достаточно сложным в силу обширности охватываемых им

категорий. С точки зрения философии, пространство, не имеет определенных материальных рамок, однако, в свою очередь, имеет определяемую длительность. По нашему мнению, учитывая философскую принадлежность указанного понятия, под ним следует понимать взаимосвязь, возникающую между субъектами информационных отношений, определенную конкретными временными рамками. Очевидно, что в процессе возникновения между субъектами взаимосвязи в информационном пространстве ключевым вопросом является определение цели, преследуя которую субъекты в эту взаимосвязь вступают. Цели могут носить самый различный характер, начиная от взаимодействия субъектов для решения определенных совместных задач и заканчивая конфликтом, который возникает, как правило, в том случае если цели взаимодействующих субъектов разняться друг с другом. В качестве примера можно привести использование некоторыми Западными державами методов информационного противоборства для достижения военно-политических целей, а также целей по установлению однополярного мира. В этом случае, очевидно, что цели Западных держав будут противоречить целям и интересам других государств. Другим примером может послужить использование международной суннитской террористической организацией (ИГИЛ) медиатехнологий в целях устрашения населения, пропаганды идеологических основ своей деятельности. Бесспорно цели, преследуемые ИГИЛ, противоречат целям органов безопасности практически всех государств планеты, учитывая, что целью последних является поддержание стабильной обстановки. Так возникает информационный конфликт. Условно, последний, можно определить как наиболее острый способ разрешения противоречий в интересах, целях, взглядах возникающих в процессе информационного взаимодействия, заключающийся в противостоянии участников этого взаимодействия. В качестве основных признаков информационного конфликта представляется логичным выделить наличие источника конфликта, подразумевающее разность в целях, преследуемых

участниками конфликта, активность участников, заключающуюся в противоборстве друг с другом, а также наличие субъектов конфликта, заключающееся в наличие, как минимум, двух сторон конфликта, между которыми и осуществляется информационное противоборство.

Информационное противоборство следует определить как соперничество субъектов информационного конфликта с целью усиления влияния на те или иные сферы социальных отношений, итогом, которого становится получение преимущества одной противоборствующей стороной и утрата подобных преимуществ другой стороной. Действия участников информационного противоборства могут носить «как наступательный, так и оборонительный характер» [5, с. 40]. С сожалением приходится констатировать, что на сегодняшний день наступательную позицию в информационном противоборстве все чаще занимают субъекты, цели которых разнятся не только с нормами международного права, но и общепринятыми нормами морали. Подобная ситуация сложилась и в Российской Федерации (РФ). Государственные органы, обеспечивающие национальную безопасность РФ, вступают в информационное противоборство постфактум и вынуждены занимать оборонительную позицию. Решение подобной проблемы, по нашему мнению, возможно путем осмысления и научно-методического определения такой категории как информационная безопасность РФ.

Понятие безопасность, как таковое, является относительным. В отличие от многих абсолютных понятий, последнее, приобретает смысловое значение только в контексте конкретной сферы человеческой деятельности. Информационная сфера, как отмечает Н.Н. Гриб, подразумевает трансформацию практически всех структурных элементов цивилизации [2, с. 25]. Исключением не является и понятие безопасности, применительно к данной сфере. Общепринятое понятие «безопасность», подразумевает под собой «отсутствие опасности» [3, с. 67]. Аналогичным образом данное понятие раскрывается и с философской точки зрения: «безопасность есть

состояние сложных социальных систем, обеспечивающих и гарантирующих сохранение их целостности, устойчивого динамического развития и эффективного функционирования на заданные цели» [4, с. 67]. Однако очевидно, что приведенные понятия, характеризующие безопасность как конкретное состояние, которое, в свою очередь, подразумевает защищенность объекта безопасности в связи с отсутствием источника угроз не применимо к понятию информационной безопасности РФ. Это обусловлено тем, что не может быть такой ситуации, в которой на определенный временной промежуток будут отсутствовать угрозы информационной безопасности РФ. Ввиду высокой развитости средств массовой информации, международных телекоммуникационных сетей, отсутствия четких правовых механизмов контроля за последними, осознания государствами-политическими оппонентами РФ, международными террористическими и экстремистскими организациями, криминальными структурами возможности использования методов информационного противоборства, угрозы информационной безопасности РФ возникают постоянно. Соответственно, представляется обоснованным говорить о информационной безопасности РФ как процессе баланса между возникающими и воздействующими угрозами и успешностью процесса противодействия этим угрозам со стороны государственных органов государственной власти, отвечающих за безопасность государства. Важно отметить, что понятие противодействия не должно восприниматься как тождественное понятию защита ввиду того, что последнее является частью понятия противодействия как такового. Следует учитывать, что в случае занятия одной из сторон противоборства позиции защиты от информационных угроз, успешность процесса противодействия с этой стороны снижается во много раз и, вероятнее всего, преимущество будет на стороне, которая проявила информационную агрессию. Более того, арсенал средств информационного противодействия у стороны, занявшей позицию защиты сводится лишь к тем, которые позволяют минимизировать ущерб,

причиненный стороной-агрессором. Соответственно, при выборе государственными органами, осуществляющими защиту РФ от рассматриваемого вида угроз защитной модели информационного противодействия угрозам речь не может идти об обеспечении информационной безопасности т.к. вред уже нанесен, а противодействие осуществляется постфактум. Поэтому, государственным органам, обеспечивающим информационную безопасность РФ в целях успешности процесса ее обеспечения необходимо занимать наступательную модель информационного противоборства, которая будет заключаться в прогнозировании и предотвращении возможных угроз информационного характера.

На основе вышеизложенного представляется возможным сформулировать понятие информационной безопасности РФ – это процесс успешного противодействия государственных органов возникающим угрозам информационного характера, заключающийся в прогнозировании и предотвращении этих угроз. Необходимо уточнить, что говорить об успешности противодействия информационным угрозам возможно только в том случае, если это противодействие осуществляется посредством прогнозирования и противодействия именно возникновению конкретной угрозы.

Из предложенного определения, очевидно, что понятие информационной безопасности РФ непосредственно связано с деятельностью государственных органов, обеспечивающих информационную безопасность государства. На основе этого возникает необходимость толкования понятия обеспечение информационнй безопасности РФ. Под последним следует понимать деятельность органов государственной власти, обеспечивающих безопасность государства направленную на достижение задач по защите личности, общества и государства от угроз информационного характера.

Учитывая тот фак, что информационная безопасность РФ подразумевает под собой процесс, характеризующийся балансом между информационными угрозами и противодействием этим угрозам со стороны государственных органов, необходимо ввести дополнительную категорию, выступающую ориентировочным звеном процесса противодействия угрозам информационной безопасности РФ. В качестве подобной категории предлагается выделить устойчивость информационной безопасности РФ. На последнюю будет влиять множество субъективных и объективных факторов, ключевым среди которых станет эффективность деятельности государственных органов по обеспечению информационной безопасности РФ. Эффективность будет заключаться в успешном и своевременном противодействии угрозам интересам РФ в информационной сфере.

Интересы РФ в информационной сфере заключаются в поддержании гармоничного развития ее информационной инфраструктуры, для реализации конституционных прав граждан на получение и пользование информацией, определенных в ч. 4 ст. 29 Конституции РФ, эффективной защите информационного пространства государства от угроз информационного характера.

Угрозы информационной безопасности РФ можно условно определить как совокупность условий и факторов, создающих опасность посягательства и (или) посягающих на интересы РФ в информационной сфере. Угрозы могут быть как реальные, так и потенциальные, равно как внешние и внутренние.

Угрозы информационной безопасности РФ имеют субъективный характер и возникают, как правило, в связи с конфликтом в интересах и целях участников информационного противоборства. Сначала возникают потенциальные угрозы, а затем реальные. То есть успешное прогнозирование потенциальных угроз позволит предотвращать их на стадии возможности возникновения и исключит, таким образом, наличие реальных угроз. Для прогнозирования потенциальных информационных угроз необходим тщательный и постоянный мониторинг информационного пространства со

стороны органов государственной власти, обеспечивающих безопасность государства.

Определение и классификация угроз интересам РФ в информационной сфере предполагает проведение отдельного исследования, поэтому отметим, что основной из указанного вида угроз на сегодняшний день является широкое внедрение в иностранные средства массовой информации, популярные, в том числе, в РФ, а также в Интернет новых информационных технологий, ориентированных на манипулирование общественным мнением в интересах политических оппонентов России, террористических и экстремистских организаций, а также криминальных структур. Понимание перечисленными категориями субъектов возможности использования информационных технологий для достижения своих целей, носящих деструктивный характер по отношению к интересам РФ в информационной сфере.

Подводя итоги исследования, следует отметить, что оно вносит определенный вклад в разработку вопроса, касающегося функционально-концептуального описания данной темы, но, все же, остается достаточно большое количество вопросов по обозначенной теме, требующих научного обоснования. Относительно формулирования понятийного аппарата темы исследования, в работе предпринята попытка толкования ключевых понятий непосредственно относящихся к вопросу выработки концептуальных основ информационной безопасности РФ, в частности, считаем существенным определение и обоснование понятия информационная безопасность РФ, но большинство из понятий осталось неосвещенными, и предполагают проведение дальнейших исследований, ориентированных на переосмысление концептуальных основ информационной безопасности РФ с позиций подхода «включения» угроз информационного характера в общее понимание «традиционных» угроз национальной безопасности РФ.

ЛИТЕРАТУРА:

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации ПР-1895 от 9 сентября 2000 г. [Текст] // Российская газета.- 2000. - 28 сентября. – С. 3-10.

2. Гриб Н.Н. Информационно-психологическая сфера как ведущее звено системы противодействия терроризму // Правовые вопросы связи. 2006. №1. – С. 25 – 29.

3. Даль В.И. Толковый словарь живого великорусского языка. Т. 1. – М.: Русский язык, 1989. – 699 с.

4. Литвинов Э.П. Философские основы концепции безопасности // Пространство и время. 2012. №1. – С. 66 – 73.

5. Сергеев И.В. Информационно-психологическая война как форма эскалации межгосударственных конфликтов // Информационные войны. 2015. №2 (34). – С. 38 – 41.

6. Сергеев И.В. Социальные сети в Интернете как средство реализации операций информационно-психологической войны // Международный научно-исследовательский журнал. 2015. №9(40). – С. 101 - 104

Reference:

1. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii. Utverzhdena Prezidentom Rossiyskoy Federatsii PR-1895 ot 9 sentyabrya 2000 g. [Tekst] // Rossiyskaya gazeta.- 2000.-28 sentyabrya. – S. 3-10.

2. Grib N.N. Informatsionno-psihologicheskaya sfera kak veduschee zveno sistemyi protivodeystviya terrorizmu // Pravovyie voprosyi svyazi. - #1, 2006. – S. 25 – 29.

3. Dal V.I. Tolkovyiy slovar zhivogo velikorusskogo yazyika. T. 1. – M.: Russkiy yazyik, 1989. – 699 s.

4. Litvinov E.P. Filosofskie osnovyi kontseptsii bezopasnosti // Prostranstvo i vremya. - #1, 2012. – S. 66 – 73.

5. Sergeev I.V. Informatsionno-psihologicheskaya voyna kak forma eskalatsii mezhgosudarstvennyih konfliktov // Informatsionnyie voynyi. - #2 (34), 2015. – S. 38 – 41.

6. Sergeev I.V. Sotsialnyie seti v Internete kak sredstvo realizatsii operatsiy informatsionno-psihologicheskoy voynyi // Mezhdunarodnyiy nauchno-issledovatelskiy zhurnal. - #9(40), 2015. – S. 101 - 104