Модель информационного противоборства в Российской Федерации

Сироткин Д. В.[1], Мартьянов А. Н.[2]

[1]Сироткин Дмитрий Викторович / Sirotkin Dmitry Viktorovich – кандидат технических наук, преподаватель;
[2]Мартьянов Анатолий Николаевич / Martyanov Anatoly Nikolaevich – доктор технических наук, профессор, командно-инженерный факультет, кафедра № 37,
Военная академия ракетных войск стратегического назначения имени Петра Великого, г. Москва

Аннотация: *в данной статье раскрываются аспекты информационного противоборства Российской Федерации, затрагивающие интересы государства, общества, личности. В настоящее время мировые державы меняют тактику завоевания мирового господства. Статья написана в рамках гранта Президента РФ на 2016-2017 г. г.*

Abstract: *this article reveals aspects of information warfare of the Russian Federation affecting the interests of the state, society, personality. Currently, the world powers are changing their tactics for world domination. The article was written within the grant of the RF President in 2016-2017.*

Ключевые слова: *информация, противоборство.*
Keywords: *information, warfare.*

Современный период развития информационного противоборства 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;

недостаточно развитым механизмом правового регулирования в сфере информационного противоборства, в том числе норм международного права, устанавливающих международную ответственность государств-инициаторов информационно-психологической агрессии.

Данные факторы придали импульс для разработки модели информационного противоборства. Модель состоит из четырех компонентов: модель устройства государства в виде концентрированных кругов, источники угроз в области ИПб, обьекты защиты, утвержденные в НПА, и как пример правовые основы информационного противоборства США. В центре находится глава государства, вокруг него располагаются политические элиты. Следующим кругом является экспертное сообщество, формирующее политические смыслы и интерпретации, и медиапространство, переводящее все на язык масс. Далее - это сами массы: общество, население страны. А снаружи – внешний круг – вооруженные силы как средство защиты всей этой концентрической конструкции. При таком подходе основой стратегии является осуществление агрессии в отношении государства извне, то есть не против вооруженных сил, не напрямую «лобовым образом». Более эффективной становится так называемая концепция ведения войны «изнутри наружу» [1, с. 7]. Эта модель позволяет установить эффективный контроль над всеми возможными участниками информационного противоборства: «противник», «партнер». При этом цели каждая из сторон выбирает в соответствии со своими планами. Особенностью ведения такой войны является то, что невидимые границы информационного пространства позволяют не соблюдать нормы международного права.

Как в любом противоборстве модель предусматривает источники угроз и объекты защиты.

Внешние источники угроз:

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

обострение международной конкуренции за обладание информационными технологиями и ресурсами;

деятельность международных террористических организаций;

увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

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.

Закон РФ «О безопасности» определяет безопасность как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». В связи с этим к основным объектам безопасности следует отнести:

личность - ее права и свободы;

общество - его материальные и духовные ценности;

государство - его конституционный строй, суверенитет и территориальная целостность.

Взяв США, как наиболее опытную державу, проводящую информационные операции, можно увидеть, сколько нормативно-правовых документов в данной области у них принято [2, с. 15]:

1. Комплексная национальная инициатива кибербезопасности 2008 г.
2. Единый устав КНШ № 3-13 от 1998 г.
3. «Доктрина информационных операций КНШ ВС» США.
4. ДР МО США от 1992 г. № TS 3600.1 «Информационная война».
5. Директива Президента США 2008 г. № 23 «Обеспечение внутренней безопасности», № 54 «Обеспечение национальной безопасности».
6. ДР председателя КНШ МОР от 1993 г. № 30-93.
7. «Концепция информационных операций объединённых группировок ВС» КНШ № 3210.01.
8. Документ КНШ ВС США «Единая перспектива-2020».
9. «Концепция информационных операций объединённых группировок ВС» КНШ № 3210.01.

Особенностью правовой системы США является то, что оператором проведения любой военной операции может являться организация не имеющая отношения к МО США.

Основные цели, которые преследуют зарубежные государства [2]:

1. Подмена у граждан традиционных нравственных ценностей и ориентиров, создание атмосферы бездуховности, разрушение национальных духовно-нравственных традиций и культивирование негативного отношения к культурному наследию противника.

2. Манипулирование общественным сознанием и политической ориентацией социальных групп населения страны по осуществлению так называемых «демократических преобразований» в интересах создания обстановки политической напряженности и хаоса.

3. Дезорганизация системы госуправления, создание препятствий функционированию государственных институтов.

4. Дестабилизация политических отношений между партиями, объединениями в целях провокации конфликтов, нагнетания атмосферы недоверия органам госуправления.

5. Обострение политической борьбы, провоцирование репрессий против оппозиции – сети неправительственных организаций (так называемых «демократических сил») и отдельных «независимых» активистов.

6. Снижение уровня информационного обеспечения органов власти и управления в целях затруднения принятия важных решений.

7. Дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления и др.

Литература

1. *Буренок В. М., Горгола Е. В., Викулов С. Ф.* Национальная безопасность России в эпоху сетевых войн, 2015.
2. *Новиков В. К., Галушкин И. Б., Аксёнов С. В.* Организационно-правовые основы информационной безопасности (защиты информации), 2015.