Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве

CONCEPTUAL VIEWS ON THE ACTIVITIES OF THE ARMED FORCES OF THE RUSSIAN FEDERATION IN INFORMATION SPACE

extracts in English – translation not certified

14 aprile 2012

Translation: AOSbrief

Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве

CONCEPTUAL VIEWS ON THE ACTIVITIES OF THE ARMED FORCES OF THE RUSSIAN FEDERATION IN INFORMATION SPACE

СОДЕРЖАНИЕ - SUMMARY

"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"
(Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г.).

Введение

Высокие темпы развития информационных систем различного назначения, компьютерных сетей типа Интернет и электронных СМИ привели на рубеже тысячелетий к формированию глобального информационного пространства. Наряду с сухопутным, морским, воздушным и космическим пространством, информационное пространство в армиях наиболее развитых стран стало активно использоваться для решения широкого круга военных задач.

Вследствие уязвимости информационно-коммуникационных систем к радиоэлектронным и программно-аппаратным воздействиям в мире возникло и стало быстро распространяться информационное оружие, обладающее трансграничными поражающими факторами, резко возросла роль информационной войны. Российская Федерация, стремительно продвигающаяся по пути информатизации всех сфер жизнедеятельности общества, оказалась перед лицом новой серьезной угрозы, исходящей из глобального информационного пространства.

Чрезвычайная важность противодействия актам агрессивной информационной войны впервые была отмечена в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 9 сентября 2000 г. В ней определено, что одним из приоритетных направлений противодействия данной угрозе является решение задач “совершенствования приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника. Кроме того, в последнее время вследствие широкого применения в системах управления войсками и оружием компьютерной техники, этот перечень дополнился задачей защиты информационной инфраструктуры Вооруженных Сил Российской Федерации от различного рода компьютерных атак.

Опыт вооруженных конфликтов последнего десятилетия, а также практика оперативной подготовки войск и штабов позволяют констатировать, что в настоящее время в Вооруженных Силах Российской Федерации сложилась цельная система деятельности, призванная обеспечить эффективное сдерживание, предотвращение и разрешение военных конфликтов в информационном пространстве.

Настоящие Концептуальные взгляды раскрывают основные принципы, правила и меры доверия, в соответствии с которыми Вооруженные Силы Российской Федерации используют глобальное информационное пространство для решения задач обороны и безопасности.

1. Основные термины и определения

Для целей настоящего документа используются следующие основные термины и определения:

- Военный конфликт в информационном пространстве - форма разрешения межгосударственных или внутригосударственных противоречий с применением информационного оружия.

- Деятельность вооруженных сил в информационном пространстве – использование вооруженными силами информационных ресурсов для решения задач обороны и безопасности.
- Информационная безопасность вооруженных сил - состояние защищенности информационных ресурсов вооруженных сил от воздействия информационного оружия.
- Информационная война - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.
- Информационная инфраструктура - совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации.
- Информационное оружие - информационные технологии, средства и методы, применяемые в целях ведения информационной войны.
- Информационное пространство - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.
- Информационные ресурсы - информационная инфраструктура, а также собственно информация и ее потоки.
- Кризисная ситуация – этап эскалации конфликта, характеризующийся применением военной силы для его разрешения.
- Международная информационная безопасность - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.
- Система обеспечения информационной безопасности Российской Федерации – часть системы обеспечения национальной безопасности страны, предназначенная для реализации государственной политики в сфере информационной безопасности.

2. Принципы

Деятельность Вооруженных Сил Российской Федерации в информационном пространстве строится исходя из совокупности принципов: законности, приоритетности, комплексности, взаимодействия, сотрудничества, инновационности.

2.1 Законность

Соблюдение принципа законности требует от Вооруженных Сил Российской Федерации в ходе своих действий в информационном пространстве неукоснительно руководствоваться нормами и принципами действующего российского законодательства, а также общепризнанными нормами и принципами международного права.

В частности, в соответствии со ст.20 Военной доктрины Российской Федерации применение Вооруженных Сил Российской Федерации в мирное время осуществляется

по решению Президента Российской Федерации в порядке, установленном федеральным законодательством. Так, решение на применение Вооруженных Сил Российской Федерации за пределами территории Российской Федерации принимается Президентом Российской Федерации на основании соответствующего постановления Совета Федерации Федерального Собрания Российской Федерации. Данное положение следует распространить также и на применение Вооруженных Сил Российской Федерации в информационном пространстве.

Что касается международного права, то Вооруженные Силы Российской Федерации применительно к особенностям военной деятельности в глобальном информационном пространстве руководствуются следующими его нормами и принципами:

- уважение государственного суверенитета,
- невмешательство во внутренние дела других государств,
- неприменение силы и угрозы силой,
- право на индивидуальную и коллективную самооборону.

Кроме того, Вооруженные Силы Российской Федерации руководствуются нормами международного гуманитарного права (ограничение неизбирательного применения информационного оружия; установление особой защиты для информационных объектов, являющихся потенциально опасными источниками техногенных катастроф; запрещение вероломных методов ведения информационной войны).

2.2 Приоритетность

Соблюдение принципа приоритетности требует от Вооруженных Сил Российской Федерации в ходе своей деятельности в информационном пространстве в первоочередном порядке стремиться к сбору актуальной и достоверной информации об угрозах, ее оперативной обработке, глубокому анализу и своевременной выработке мер защиты. Все это в совокупности создает благоприятные условия для эффективного управления войсками и оружием, поддержания необходимого морально-психологического состояния личного состава.

Принятие комплекса мер по защите информационных ресурсов, позволит в условиях информационной войны избежать дезориентации органов военного управления, дезорганизации системы управления войсками и оружием, катастрофического разрушения элементов тыловой и транспортной инфраструктуры, деморализации личного состава и населения в зоне военных действий. В современных условиях необходимость принятия данных мер в приоритетном порядке обуславливается, в том числе тем, что сейчас сотни миллионов человек (целые страны и континенты) вовлечены в единое глобальное информационное пространство, образованное Интернетом, электронными СМИ и системами мобильной связи.

2.3 Комплексность

Соблюдение принципа комплексности требует от Вооруженных Сил Российской Федерации в ходе своей деятельности в информационном пространстве использовать все имеющиеся силы и средства для эффективного решения стоящих перед ними задач.

В целом деятельность в информационном пространстве включает мероприятия штабов и действия войск по разведке, оперативной маскировке, радиоэлектронной борьбе, связи, скрытому и автоматизированному управлению, информационной работе штабов, а также защите своих информационных систем от радиоэлектронных, компьютерных и иных воздействий.

Деятельность в информационном пространстве представляет собой согласованную единую систему, в которой каждый компонент выполняет свои задачи присущими ему способами и приемами, а с другой стороны, интегрируясь в единую систему, повышает возможности всей системы по достижению целей, стоящих перед Вооруженными Силами Российской Федерации.

В организации деятельности в информационном пространстве в мирное, в военное время, при подготовке и в ходе операций (боевых действий) принимают непосредственное участие командование и штабы всех уровней.

Каждый из этих органов управления в соответствии со своими функциями и ответственностью разрабатывает и планирует мероприятия и действия подчиненных войск, объединенные единым замыслом действий в информационном пространстве.

2.4 Взаимодействие

Соблюдение принципа взаимодействия требует от Минобороны России согласовывать свои действия в информационном пространстве с другими федеральными органами исполнительной власти.

Взаимодействие осуществляется в рамках системы обеспечения информационной безопасности Российской Федерации, определенной Доктриной информационной безопасности Российской Федерации (2000 г.).

2.5 Сотрудничество

Соблюдение принципа сотрудничества требует согласования усилий с дружественными государствами и международными организациями.

Основной целью развития сотрудничества на глобальном уровне является установление международно-правового режима, регулирующего, в том числе, военную деятельность государств в мировом информационном пространстве на основе принципов и норм международного права.

Развитие сотрудничества на региональном уровне преследует следующие цели: создание механизмов принятия эффективных коллективных действий, направленных на выявление, предупреждение и пресечение применения информационно-телекоммуникационных технологий для угрозы миру и безопасности, осуществления актов агрессии урегулирование и разрешение международных споров и конфликтных ситуаций, связанных с враждебным использованием информационно-телекоммуникационных технологий, укрепление доверия в области использования информационных систем трансграничного характера и обеспечение безопасности использования единого информационного пространства.

2.6 Инновационность

Соблюдение принципа инновационности требует от Вооруженных Сил Российской Федерации использовать для подготовки и осуществления деятельности в информационном пространстве наиболее передовые технологии, средства и методики, а также привлекать к решению задач по информационной безопасности высококвалифицированный личный состав.

Поэтому для разработки и производства таких средств и технологий может привлекаться научно-производственный потенциал наиболее передовых инновационных центров Российской Федерации, а сама разработка осуществляться в рамках государственных и ведомственных программ и НИОКР.

Подготовка специалистов в сфере организации и осуществления деятельности в информационном пространстве проводится в образовательных учреждениях высшего профессионального образования Министерства обороны Российской Федерации.

Кроме того, для решения задач информационной безопасности Вооруженных Сил Российской Федерации могут привлекаться, в установленном законодательством Российской Федерации порядке, специалисты, закончившие иные образовательные учреждения Российской Федерации.

3. Правила

В ходе своей деятельности Вооруженные Силы Российской Федерации руководствуются совокупностью правил сдерживания, предотвращения и разрешения военных конфликтов в информационном пространстве

“Военная политика Российской Федерация направлена на недопущение гонки вооружений, сдерживание и предотвращение военных конфликтов …” (Военная доктрина Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 февраля 2010 г., ст.17)

3.1 Deterrence and Conflict Prevention

Armed Forces of the Russian Federation in its implementation activities are guided by the following rules of deterrence and prevention of military conflicts in the information space:

.1 Develop a system to ensure security of the Armed Forces of the Russian Federation, designed to contain and resolve armed conflicts in the information space.

.2 To maintain the strength and means to ensure security in constant readiness to repel threats to the military-political nature of the information space.

.3 Cooperate on a priority basis with the countries of the Collective Security Treaty, the Commonwealth of Independent States and the Shanghai Cooperation Organization, to expand the circle of partners and to develop cooperation with them on the basis of common interest in strengthening

international security in accordance with the provisions of the UN Charter and other norms international law.

.4 Seek to conclude a UN treaty on ensuring international information security, extends the application of generally recognized norms and principles of international law on the information space.

.5 Take all possible measures for early detection of potential military conflicts in the information space, as well as exposing the organizers of the conflict, instigators and accomplices.

.6 Identify the factors and the occurrence of an escalation of the conflict and establish control over them so as to avoid emergencies.

.7 To take urgent measures to counter the development (or exacerbation of conservation) of the conflict and its transition into a state which significantly increases the cost of settlement.

.8 Take steps to prevent the spread of conflict in the neighboring areas of international relations and the settlement of the consequences of which will require additional cost and effort.

.9 Take measures to neutralize the factors that gave rise to the conflict in order to direct interaction between the conflicting sides in the direction of constructive cooperation.

.10 Publicly, objectively and in a timely manner to explain the world community causes and origins of the conflict. The formation of the necessary public opinion involves the proper orientation and mobilization, to create a global information space of an environment conducive to limit the possibility of a further escalation of the conflict organized steps.

3.2 Conflict Resolution

"The Russian Federation considers it legitimate to use the Armed Forces and other troops to repel the aggression against it and (or) its allies, and maintaining (recovery) of the world to address the UN Security Council and other institutions of collective security, as well as to protect its citizens, outside the Russian Federation in accordance with generally recognized principles and norms of international law and international treaties of the Russian Federation " (Military Doctrine of the Russian Federation, approved by Presidential Decree of February 5, 2010, p. 20) The Armed Forces of the Russian Federation, guided by the following rules resolve armed conflicts in the information space:

.1 Resolving conflicts in cyberspace to carry out in the first place, by negotiation, conciliation, appeals to the UN Security Council or to regional agencies or arrangements or other peaceful means.

.2 In the case of tensions tend to avoid conflict transition in the extreme, destructive forms of warfare, and especially those which may lead to destabilization of international situation and the emergence of a crisis.

.3 With the escalation of conflict in the information space and its transition into a crisis phase to exercise the right of individual or collective self-defense with any elected ways and means, do not contradict the universally recognized norms and principles of international law.

.4 In order to meet the challenges of individual and collective self-defense to determine the required capacity of the response on the basis of national democratic procedures, taking into account the legitimate interests of the security of other states, as well as the need for international security and stability.

.5 In the interests of individual and collective self-defense to place its forces and means of ensuring security in the territory of other States in accordance with the agreements worked out on a voluntary basis during the negotiations, and in accordance with international law.

.6 During the conflict, keep the domestic and foreign media about the situation and, based on public opinion, more effective de-escalation of its influence on the development and consolidation of results achieved to resolve conflict of contradictions.

4 Measures of trust

Armed Forces of the Russian Federation will seek to develop confidence-building measures in military use of the information space. In particular, such measures include:

.1 Exchange of national security concepts in the information space.

.2 The rapid exchange of information on crisis events and threats in the information space and measures taken with regard to their settlement, and neutralization.

.3 Consultations on the activities in the information space, which may cause concern of the parties, and cooperation in resolving conflicts of a military nature.

Conclusion

In the present conditions of the Russian Federation's defense depends on the effectiveness of the Armed Forces of the information space and is largely determined by their capacity to deter, prevent and resolve conflicts that arise in cyberspace.

Armed Forces of the Russian Federation plan to address the challenges they face defense and security, based on fundamental principles and rules of the Armed Forces of the Russian Federation in the information space, as well as confidence-building measures in the present conceptual views. Realizing the true conceptual view, the Armed Forces of the Russian Federation will seek to maximize the opportunities of the information space to strengthen national defense, deterrence and prevention of military conflicts, military cooperation, as well as the formation of an international information security for the entire world community.