**А.Ж.УКАШЕВ**

*преподаватель кафедры защиты информации Военно-инженерного института радиоэлектроники и связи МО РК города Алматы*

**АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ ВОЕНОСЛУЖАЩИМИ**

***Аннотация. Возрастание роли и значения информационной составляющей в структуре военной безопасности и безопасности войск обусловлено общемировой тенденцией продвижения передовых стран к так называемому информационному обществу, где информация и информационные услуги будут основным фактором политического, экономического и социального развития. В этой связи способность государства эффективно использовать накопленные информационные ресурсы и технологии в интересах обороны становится важнейшим показателем его военной мощи.***

  Без широкого применения современных информационных технологий и систем немыслимо формирование эффективной системы управления и воспитания личного состава Вооруженных Сил России. Кроме того, вероятный противник рассматривает эту человеческую компоненту в качестве приоритетного объекта своего воздействия, что также требует принятия известных мер по информационной защите военнослужащих.  
     Информационно-психологическое противоборство давно и прочно стало неотъемлемым компонентом подготовки и проведения боевых операций. Более того, в армиях западных государств усиленно развиваются теория и практика полномасштабной информационно-психологической войны против войск и населения возможного противника, создаются специальные структуры и подразделения.

 На службу такой войне мобилизуются новейшие достижения научно-технического прогресса, разрабатываются и принимаются на вооружение сценарии, способы, средства, системы, способные целенаправленно и эффективно воздействовать на психику и поведение больших масс людей.

  К манипулированию сознанием в своих корпоративных, корыстных целях усиленно стремятся и некоторые политические институты, а также находящиеся под их влиянием средства массовой информации. В сферу их действия неизбежно, а во многом и намеренно попадают военнослужащие. Памятным примером такого жесткого информационного давления может быть недавняя беспрецедентная по масштабу и накалу антиармейская кампания в отечественных средствах массовой информации.

Федеральный закон «Об участии в международном информационном обмене» от 5 июля 1996 года трактует информационную безопасность как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства. Здесь под информационной средой понимается сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Применительно к деятельности Вооруженных Сил России данное определение требует уточнения. Личный состав армии и флота не только обладает информационными ресурсами ограниченного доступа (различными формами документов), информационными технологиями и автоматизированными системами управления оружием и войсками, не только активно участвует в информационном противоборстве с противником, но и сам является объектом непрерывного информационно-психологического воздействия последнего.  
     При этом войска постоянно сталкиваются с так называемыми угрозами информационной безопасности - реальными или потенциально возможными действиями и условиями, приводящими к нарушению нормального режима работы информационных систем (выводу из строя), негативному информационно-психологическому воздействию на личный состав или нанесению материального ущерба.

     **АНАЛИЗ** источников угроз информационной безопасности войск позволяет объединить их в две основные группы: внутренние и внешние.  
     Нестабильная военно-политическая обстановка в регионах и местах дислокации войск и сил флота негативно отражается на информационной политике государства, способствует вовлечению военнослужащих в политическое противостояние, наполнению социально значимой для них информации разного рода слухами, сплетнями, домыслами, версиями. В такой обстановке в информационное поле общества вливаются мощные потоки лженаучной, агрессивной, а порой и антигосударственной (антиармейской) информации. Возникает реальная угроза информационной безопасности войск и морально-психологическому состоянию личного состава.

     Кризисные явления в социально-экономической сфере государства также сужают наши возможности по обеспечению информационной независимости. По мнению специалистов, отставание России от лидирующих государств в области создания компьютерной техники, ее программного обеспечения, локальных и глобальных информационных систем продолжается.  
     Возникла реальная угроза вовлечения страны в информационно-технологическую кабалу от Запада. Вынужденный массовый импорт зарубежной электронно-вычислительной техники ведет не только к дестандартизации собственного производства вычислительной техники и растущей несовместимости (технической и программной) его продукции с иностранными образцами, но и к подрыву информационной безопасности государства.  
     Применение зарубежных ЭВМ в информационных системах Вооруженных Сил снижает их надежность и создает предпосылки к утечке информации, содержащей государственную и военную тайну. Обороноспособность страны при таком развитии событий будет заведомо уязвима от информационных воздействий более развитых государств. Не случайно на Западе активизировались изыскания и разработка оружия, предназначенного для воздействия на противника через информационную инфраструктуру его государства. Учитывая это обстоятельство, Совет Безопасности РФ создал в 1995 году межведомственную комиссию по информационной безопасности, на которую возложил оценку и определение приоритетных задач в сфере обеспечения информационной безопасности государства.

     Серьезные прорехи в системе информационной защиты государства создает неразвитое, противоречивое, запутанное законодательство в области информационной деятельности. В демократическом обществе информация является не только общенародным достоянием, но и обычным товаром, предметом собственности, купли и продажи. Нерегулируемое обращение с ней неизбежно ведет к росту социальной напряженности, нарушению конституционных прав граждан, нанесению им морального и материального ущерба, увеличению опасности манипулирования общественным сознанием недобросовестными субъектами информационной деятельности.

     Угрозу информационной безопасности войск несет нарушение информационного режима жизнедеятельности личного состава и работы различных информационных систем. Необходимо особо подчеркнуть, что нарушение режима работы с закрытой информацией или секретной аппаратурой в частях и на кораблях создает предпосылки для ее утечки, утери или порчи. Кроме того, в ряде случаев трудовая усталость у военнослужащих наступает не из-за физических перегрузок, а в результате грубого нарушения информационного режима. Возникающий при этом информационный голод способствует повышенной внушаемости военнослужащих, создает почву для возникновения негативных слухов, панических настроений и страхов (фобий), особенно в боевой обстановке.  
     Еще одна угроза информационной безопасности войск - усилившаяся в последние годы вероятность применения противником нового информационно-психологического оружия. Широкий спектр новейших образцов такого («несмертоносного») оружия создается сегодня в рамках так называемой технологии «иммобилизующих систем».  
     В работах над таким оружием более или менее четко определились два направления: создание средств, предназначенных для воздействия на психику и здоровье военнослужащих противника; создание средств, направленных на поражение его информационных систем.  
     К первому направлению относится информационно-психологическое оружие, которое основано на применении инфразвука, микроволнового излучения, биоэлектронного воздействия, электромагнитных полей, медико-биологических и химических средств и может быть использовано для контроля над психикой военнослужащих и целенаправленного влияния на их поведение в боевой обстановке.  
     Второе направление связано с разработкой средств поражения систем связи и управления (например, боевых информационно-управляющих систем), радиоэлектронной разведки, радиоэлектронного подавления и т.д. Например, для уничтожения (искажения) программного обеспечения применяемых в войсках ЭВМ «выращиваются» специальные компьютерные вирусы и логические бомбы. Так, если к концу 80-х годов ученым было известно не более десятка вирусов, то в 1990 году их насчитывалось уже около 400, а в наше время еженедельно появляется несколько новых губительных для ЭВМ вирусов.  
     Источником возможных угроз информационной безопасности войск были и остаются силы и средства информационно-психологической борьбы противника. Они показали свою исключительную эффективность в ряде локальных войн и военных конфликтов.  
     Серьезную угрозу информационной безопасности войск по-прежнему представляет подрывная деятельность разведок и спецслужб недружественных России государств. Хотя, как утверждают специалисты, около 70% закрытой военной информации можно почерпнуть из «открытых источников», наиболее ценная информация о военной технике, разработке новых видов вооружения и планах военных операций добывается органами зарубежных разведок. По некоторым данным, противник в настоящее время более 65% развединформации получает через средства радиоэлектронной разведки, осуществляя перехват сообщений, засечку работы систем связи и наблюдения, подключение к информационным каналам (подслушивание), проникновение в информационно-управляющие системы и т.д. Например, в печати упоминалось о программе «троянский конь», предназначенной для скрытого проникновения через информационные сети противника к его информационным ресурсам в целях добывания разведсведений.  
     **В СИСТЕМЕ** информационной безопасности войск важным является вопрос об объектах угроз. Условно их можно разделить на социально-психологические и материально-технические. Необходимо подчеркнуть, что объекты угроз информационной безопасности являются одновременно и приоритетными объектами информационной защиты в армии и на флоте. В зависимости от их специфики определяются пути и особенности обеспечения информационной безопасности войск и сил флота.  
     С учетом изложенного под информационной безопасностью войск можно понимать такое состояние защищенности их информационных ресурсов, систем, технологий и личного состава от внутренних и внешних источников угроз, которое позволяет успешно решать задачи информационного обеспечения повседневной и боевой деятельности частей и подразделений.

     На сегодняшний день, к сожалению, нет единой концепции информационной безопасности войск. Однако научные исследования, зарубежный и отечественный опыт позволяют определить ее основное содержание через структурные компоненты, которые в той или иной мере уже сложились в общей системе информационного обеспечения деятельности войск.

     Центральным ее звеном является надежная информационная защита войск и сил флота. С одной стороны, она предполагает защиту информации, содержащей государственную и военную тайну, защиту информационных систем и средств связи от огневого поражения или проникновения в них противника, радиоэлектронную защиту. С другой - включает в себя защиту здоровья и психики личного состава частей и подразделений от разведывательного информационно-психологического воздействия противника, от попыток подчинить и контролировать массовое сознание военнослужащих, от стремления манипулировать общественным мнением в армейской среде и т.д.  
     Вместе с тем защита должна сочетаться с эффективным информационным противодействием противнику, целью которого является недопущение или максимальное затруднение ведения им информационно-психологической борьбы. Активное противодействие включает не только радиоэлектронное подавление и огневое поражение вражеских информационных систем, но и всевозможное дезинформирование противника (маскировка, демонстративные действия, организованная «утечка важной информации»), а также комплекс мер по нейтрализации или пресечению проводимых противником информационно-психологических акций и операций.

     В ходе военного противоборства информационная безопасность войск в значительной мере будет зависеть от мощности того информационно-психологического воздействия на противника, которое смогут оказать на него спецподразделения психологической борьбы. Оно должно преследовать цели подрыва морально-психологической устойчивости личного состава и населения противника в интересах решения нашими силами стоящих задач.  
     Информационная безопасность тесно связана с оптимальным информационным обеспечением управления войсками. Непрерывный сбор и обработка информации о противнике и театре военных действий (разведка), информационно-аналитическая деятельность органов военного управления, организация связи, информационная поддержка выработки решений, оценка морально-психологического состояния личного состава и воинской дисциплины - все это входит в круг проблем информационного обеспечения управления, которое является базисом и одним из критериев эффективности всей системы информационной безопасности войск.

     *Логически завершающим ее элементом должна стать качественная информационно-воспитательная работа с личным составом частей и соединений. Она формирует у воинов необходимые морально-психологические и боевые качества, верность героическим традициям и воинскому долгу, патриотизм и в конечном итоге - невосприимчивость к негативному информационному воздействию. Именно эти факторы способствуют высокой бдительности, готовности личного состава противостоять духовной агрессии.*

**Литература:**

1. Белозеров В. К. Информационное обеспечение военной политики ФРГ: опыт и возможности его использования в России: дис. ...канд. полит. наук. М.: ВУ, 2003. С. 52.

2. Buch, Klaus. Die neue Zusammenarbeit zwischen Bundeswehr und IT-Industrie // Soldat und Technik. 2001. № 2. Р. 25.

3. Белозеров В. К. Информационное обеспечение военной политики ФРГ: опыт и возможности его использования в России: Автореф. дис. .канд. полит. наук. М.: ВУ, 2003. С. 5.

4. Гриняев С. Особенности информационной войны во время агрессии НАТО против Югославии // Агентура, 2000-2004 гг. [Электронный ресурс]. Режим доступа: http://www.Агентура.ру (дата обращения: 11.04.2009).

5. Путин В. Выступление о мощности пропагандистской машины Запада на встрече с политологами Валдайского клуба от 12 сентября 2008 г. // The Guardian (Великобритания). 2008. 12 сентября.

6. Информационная безопасность и СМИ. Научно-практическая конференция в Университете мировой экономики и дипломатии. 18 Ноября 2006 года [Электронный ресурс]. URL: http://www.mfa.uz/ (дата обращения: 27.02.2008).

7. Паршин С., Горбачев Ю. Концепция «сетецентри-ческой войны» как предпосылка появления новых форм ведения боевых действий // Национальная оборона. М., 2008. № 11. С. 8-22.

8. Жигневский Р. Поле боя — киберпространство // Разведка. М., 2009. № 12. С. 16-19.

9. Мешков Е. П. Социальное управление информационной безопасностью военнослужащих: Монография - Т.: Изд.ТулГУ, 2010. С. 114-146.