Потенциальные возможности развития основных сфер жизни общества и соответствующих компонентов обороноспособности определяются состоянием информационных процессов. В настоящее время информация считается стратегическим национальным ресурсом, одним из основных богатств страны. Под воздействием информатизации все сферы жизни общества приобретают новые качества:
 - гибкость;
 - динамичность.
Но одновременно возрастает и потенциальная уязвимость общественных процессов от информационного воздействия.

Так по мнению как отечественных, так и иностранных учёных по информации, на смену опасности возникновения ядерной катастрофы может прийти угроза развязывания войны, которая примет новые формы. Это будет борьба, направленная против стран, обладающих передовой технологией, для создания хаоса в государственном, военном управлении и порождения экономической катастрофы. В военном деле наступает новый, постядерный этап развития. Эффективность современного оружия всё больше определяется не столько огневой мощью, сколько степенью информационной обеспеченности. Информатизация армии стала приоритетной задачей военно-технической политики. В содержании военных действий возросла значимость информационно-технического противоборства. Превосходство в степени информированности-неприменное условие победы в воздушном, морском, и даже в сухопутном бою, залог успеха в противовоздушной обороне. Об этом свидетельствует опыт вооруженных конфликтов и локальных воин современности. Возрастание роли информационно-технической борьбы стирает границу между войной и миром. Вооружённые силы ряда государств находятся в постоянном информационном противоборстве, а военная информатика и в мирное время решает задачи, характерные для войны. В настоящее время в военно-политическом противоборстве государств, другого рода внешних и внутренних конфликтах сейчас на тенденция смещения центра тяжести с традиционных силовых методов и средств борьбы к нетрадиционным, в том числе информационным.

Итак, информация и информационные технологии сегодня становятся реальным оружием. Оружием не только в метафорическом смысле, но и в прямом. Естествен вопрос: что является объектом информационного воздействия?

Основным объектом информационного воздействия является сознание и психика человека. В зависимости от преследуемых целей, масштабов действий, характера и содержания решаемых задач, привлекаемых сил и средств этими людьми могут быть как конкретные лица(государственные и политические лидеры, сотрудники спецслужб, военнослужащие, ученые, члены политических движений),так и определённые социальные группы (рабочие, предприниматели, молодёжь, домохозяйки и т.д.).А в условиях когда нарушено функционирование системы государственного управления, создана обстановка общественно-политической и социально-экономической нестабильности в стране или в конкретном регионе, объектом воздействия может стать всё население.

Таким образом, информационные войны сегодня уже не мифы-реальность.И чем дальше, тем больше информационное оружие будет выступать в качестве фактора скрытого военно-политического давления, способного нарушить сложившийся в мире стратегический паритет. Чтобы не допустить этого, России надлежит предпринять целый ряд принципиальных шагов.

ПЕРВОЕ. Нужна грамотная оценка состояния и перспектив развития информационного оружия, способов применения и противодействия ему.

ВТОРОЕ. Необходимо выявить источники негативного информационного воздействия как на индивидуальном, так и на стратегическом уровнях и создавать адекватные средства противодействия,своеобразные"фильтры",позволяющие блокировать, в крайнем случае сводить к минимуму негативное влияние атакующих средств информационного воздействия.

ТРЕТЬЕ. Готовить психику индивидуумов и общества в целом к отражению негативных информационных воздействий, что в итоге поможет поддерживать духовное равновесие на индивидуальном уровне и информационный баланс на стратегическом Следовательно для выполнения этих задач необходимо создать систему обеспечения информационной безопасности. Таким образом, по мере развития научно-технического прогресса роль информационной безопасности Вооружённых Сил увеличивается, и её обеспечение должно занять подобающее место в военной политике государства. И чем выше уровень интеллектуализации и информатизации

Вооружённых Сил, тем надёжнее её информационная безопасность, поскольку реализация интересов всё более осуществляется информационных, а не вещественно-энергетических воздействий. На Западе стал популярен афоризм "Кто владеет информацией, тот владеет миром."

Так что же такое информационная безопасность?

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - способность государства защитить все сферы общественной жизни, сознание и психику граждан от негативного информационного воздействия, обеспечить субъекты политического и военного руководства данными для успешной модернизации общества и армии, не допустить утечки закрытой, общественно ценной информации и сохранить постоянную готовность к информационному противоборству внутри страны и на мировой арене, способствовать достижению социальной стабильности и согласия в обществе.

Исходя из данного определения можно охарактеризовать информационную безопасность Вооружённых Сил как степень их защищённости и, следовательно, устойчивости основных сфер деятельности по отношению к опасным информационным воздействиям, причём как к внедрению, так и к извлечению информации. Информационная безопасность личности воина характеризуется защищённостью психики и сознания от опасных информационных воздействий: манипулирования, дезинформирования, побуждению к самоубийству, оскорблений и т.п.

 Необходимо отметить, что информационные воздействия опасны (или полезны) не столько сами по себе, сколько тем, что "запускают" мощные вещественно-энергетические процессы, управляют ими. Суть влияния информации как раз и заключается в её способности "запускать "вещественно-энергетические процессы, параметры которых на порядок выше самой информации. Системный подход к информационной безопасности войск требует определения её субъектов, средств и объектов, принципов обеспечения, источников опасности, направленности информационных потоков. Источники информационных опасностей могут быть естественными (объективными) и умышленными. Первые возникают в результате непреднамеренных ошибок и неисправностей, случайных факторов, стихийных бедствий и др. Известно, например, что системы ПВО переодически выдают ложные сигналы тревоги из-за разнообразных технических сбоев, но по этим сигналам приводятся в высокую степень боеготовности стратегические носители ядерного оружия. Умышленные информационные воздействия осуществляются сознательно и целенаправленно. При этом часто используются средства массовой информации, РЭБ, специальные программные средства для компьютеров. Они настолько эффективны, что их можно выделить как новый класс оружия-информационный. Объектами опасного информационного воздействия и, следовательно, информационной безопасности, выступают: сознание, психика воина; информационно-технические системы; информационные ресурсы.

 ИНФОРМАЦИОННЫЕ РЕСУРСЫ - отдельные документы и отдельные массивы документов, документы, и массивы документов в информационных системах. Если же говорить о социальных объектах информационной безопасности, то к ним можно отнести личность воина, воинский коллектив. Субъектами информационной безопасности войск следует считать те военные органы и структуры, которые занимаются её обеспечением.

Основные информационные воздействия следует разделить на два вида.

ПЕРВЫЙ ВИД связан с утратой ценной информации, что либо снижает эффективность собственной деятельности, либо повышает эффективность деятельности противника. Если объектом такого воздействия является сознание воина, то речь идёт о разглашении военных тайн, вербовке агентов, специальных мерах и средствах подслушивания, использования медикаментозных, химических и других воздействий на психику человека. Появились сообщения о вирусе 666,который способен негативно воздействовать на психофизиологическое состояние оператора ПЭВМ, вплоть до его смерти. Принцип действия вируса-убийцы в следующем: он выдаёт на экран специально подобранную цветную комбинацию, погружающую человека в своего рода гипнотический транс. Всё рассчитано так, чтобы подсознательное восприятие вызвало резкое изменение деятельности сердечно-сосудистой системы, вплоть до блокирования сосудов головного мозга и смерти. Если же источником информации служат технические системы, то речь уже идёт о технической разведке, или шпионаже(перехват телефонных переговоров, радиограмм, сигналов других систем коммуникаций),проникновении в компьютерные сети, банки данных.

ВТОРОЙ ВИД информационного воздействия связан с внедрением негативной информации, что может не только привести к опасным ошибочным решениям, но и заставить действовать во вред, даже подвести к самоубийству, а общество к катастрофе.