ИНФОРМАЦИОННОЕ ОРУЖИЕ

Выполнила студентка факультета

агрономии и биотехнологии

405 группы

Крюкова Екатерина

ИНФОРМАЦИОННОЕ ОРУЖИЕ И ИНФОРМАЦИОННЫЕ ВОЙНЫ

Сейчас много говорят об информационном оружии и новом лице войны. Основной тезис состоит в том, что войну можно вести более профессионально и "цивилизованно". Вместо того, чтобы вводить в стан противника танки врага можно ослабить более эффективно, аккуратно нарушая его информационный механизм управления, вскрывая финансовые коммуникации, направляя в желатемое русло развитие информационной сферы путем внедрения устаревших информационных технологий.

С переходом от индустриального общества к информационному и соответствующим развитием информационных технологий значительное внимание уделяется новейшим видам так называемого *“гуманного оружия”*. К ним относятся *информационное, психотронное, экономическое, консциентальное оружие и пр*. Особое место среди них занимает информационное оружие и технологии ведения информационной войны. Об их значимости свидетельствует то, что США создали информационные войска и уже третий год выпускаются подразделения кибервоинов. По своей результативности информационное оружие сопоставимо с оружием массового поражения. Спектр действия информационного оружия может простираться от нанесения вреда психическому здоровью людей до внесения вирусов в компьютерные сети и уничтожения информации. Пентагон на суперкомпьютерах моделирует варианты возможных войн в XXI столетии с использованием методов и технологии “несмертельного оружия”.

В вооруженных силах НАТО значительное внимание уделяется роли “несмертельного оружия” и технологий, которые существенно изменяют характер применения сухопутных, военно-воздушных и военно-морских сил на ТВД и геополитического и цивилизационного противоборства основных центров мира.

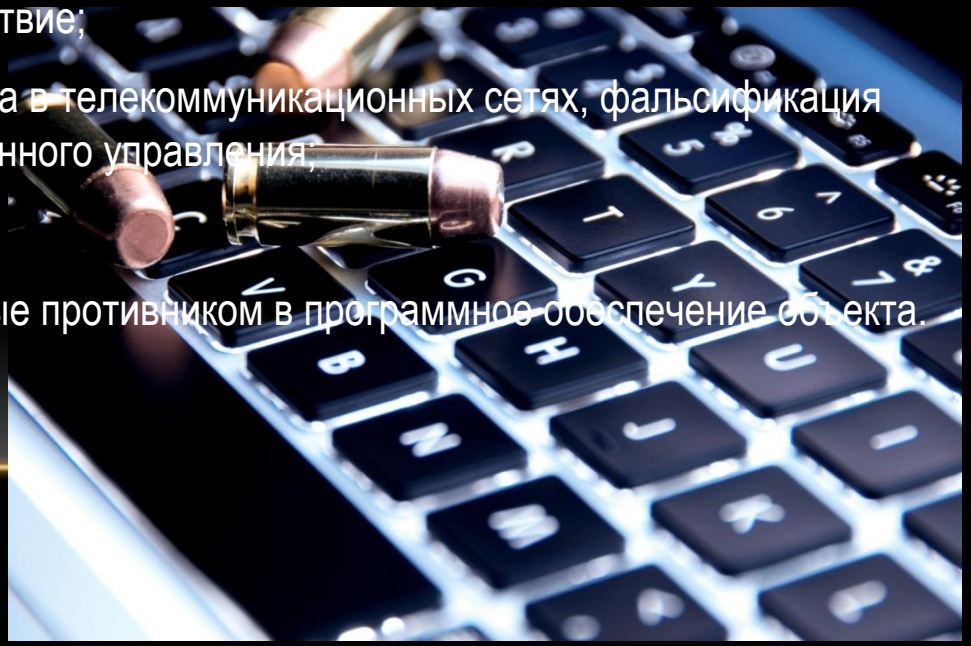
Отличие видов и технологий “несмертельного оружия” от обычного военного оружия: *оно акцентирует внимание на использовании алгоритмов и технологий, концентрирующих в себе базовые знания, направленных на поражение противника. Информационная война* олицетворяет собой войну цивилизаций за выживание в условиях постоянно сокращающихся ресурсов. Информационное оружие поражает сознание человека, разрушает способы и формы идентификации личности по отношению к фиксированным общностям, оно трансформирует матрицу памяти индивида, создавая личность с заранее заданными параметрами, удовлетворяющих требования агрессора, выводит из строя системы управления государства-противника и его вооруженных сил.

Информационным оружием называются средства:

- уничтожения, искажения или хищения информационных массивов;
- преодоления систем защиты;
- ограничения допуска законных пользователей;
- дезорганизации работы технических средств, компьютерных систем.

Атакующим информационным оружием сегодня можно назвать:

- компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т. п.;
- логические бомбы - программные закладные устройства, которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;
- средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;
- средства нейтрализации тестовых программ;
- различного рода ошибки, сознательно вводимые противником в программное обеспечение объекта.



Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, достаточный выбор времени и места применения, наконец, экономичность делают информационное оружие чрезвычайно опасным: оно легко маскируется под средства защиты, например, интеллектуальной собственности; оно позволяет даже вести наступательные действия анонимно, без объявления войны.

Нормальная жизнедеятельность общественного организма целиком определяется уровнем развития, качеством функционирования и безопасностью информационной среды. Производство и управление, оборона и связь, транспорт и энергетика, финансы, наука и образование, средства массовой информации - все зависит от интенсивности информационного обмена, полноты, своевременности, достоверности информации. Именно информационная инфраструктура общества - мишень информационного оружия. Но в первую очередь новое оружие нацелено на вооруженные силы, предприятия оборонного комплекса, структуры, ответственные за внешнюю и внутреннюю безопасность страны. Высокая степень централизации структур государственного управления российской экономикой может привести к гибельным последствиям в результате информационной агрессии. Темпы совершенствования информационного оружия превышают темпы развития технологий защиты. Поэтому задача нейтрализации информационного оружия, отражения угрозы его применения должна рассматриваться как одна из приоритетных задач в обеспечении национальной безопасности страны.

МИРОВЫЕ ИНФОРМАЦИОННЫЕ СЕТИ И ИНФОРМАЦИОННОЕ ОРУЖИЕ

Во всем мире стоит вопрос защиты национальных информационных ресурсов в связи с расширением доступа к ним через открытые информационные сети типа Internet. Кроме того, что повсеместно увеличивается число компьютерных преступлений, реальной стала угроза информационных атак на более высоком уровне для достижения политических и экономических целей.

Пропаганда информационного оружия активно ведется в США, и эти пропагандистские мероприятия связаны со стратегическими инициативами создания Национальной и Глобальной информационных инфраструктур, так как основу практически всех направлений международной и внутренней политики США составляет идея лидерства этой страны в мире. Технологические достижения США совместно с сильной и динамичной экономикой позволяют демонстрировать могущество страны. Информационное оружие, базирующееся на самых передовых информационных и телекоммуникационных технологиях, способствует решению этой задачи. Уязвимость национальных информационных ресурсов стран, обеспечивающих своим пользователям работу в мировых сетях, - вещь обоюдоострая. Информационные ресурсы взаимно уязвимы. В докладе Объединенной комиссии по безопасности, созданной по распоряжению министра обороны и директора ЦРУ в США в июне 1993 года и завершившей свою работу в феврале 1994 года, говорится: "...Уже признано, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться с "электронными скоростями" при обороне и нападении. Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Наша политика обеспечения национальной безопасности и процедуры ее реализации должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести такие войны..."

Для предотвращения или нейтрализации последствий применения информационного оружия необходимо принять следующие меры:

- защита материально-технических объектов, составляющих физическую основу информационных ресурсов;
- обеспечение нормального и бесперебойного функционирования баз и банков данных;
- защита информации от несанкционированного доступа, искажения или уничтожения;
- сохранение качества информации (своевременности, точности, полноты и необходимой доступности).

Создание технологий обнаружения воздействий на информацию, в том числе в открытых сетях, - это естественная защитная реакция на появление нового оружия. Экономическую и научно-техническую политику подключения государства к мировым открытым сетям следует рассматривать прежде решив вопрос национальной информационной безопасности. Будучи открытой, ориентированной на соблюдение законных прав граждан на информацию и интеллектуальную собственность, эта политика должна предусматривать защиту сетевого оборудования на территории страны от проникновения в него скрытых элементов информационного оружия. Это особенно важно сегодня, когда осуществляются массовые закупки зарубежных информационных технологий. Без подключения к мировому информационному пространству страну ожидает экономическое отставание. Оперативный доступ к информационным и вычислительным ресурсам, поддерживаемым сетью Internet дает возможность преодоления международной экономической и культурной изоляции, преодоления внутренней дезинтеграции, развития социальной инфраструктуры.

Практические мероприятия программного характера по защите от информационного оружия:

- Организация мониторинга и прогнозирования потребностей экономических и других структур в различных видах информационного обмена через международные сети. Возможно создание специализированной структуры для контроля трансграничного обмена, в том числе посредством Internet; координация мер государственных и негосударственных ведомств по предотвращению угроз информационной безопасности в открытых сетях; организация международного сотрудничества.
- Разработка государственной программы совершенствования информационных технологий, обеспечивающих подключение национальных и корпоративных сетей к мировым открытым сетям при соблюдении требований безопасности информационных ресурсов.
- Организация системы комплексной подготовки и повышения квалификации массовых пользователей и специалистов по информационной безопасности для работы в мировых информационных сетях.
- Разработка национального законодательства в части правил обращения с информационными ресурсами, регламента прав, обязанностей и ответственности пользователей открытых мировых сетей. Установление перечня информации, не подлежащей передаче по открытым сетям, и обеспечение контроля за соблюдением установленного статуса информации. Активное участие в разработке международного законодательства и нормативно-правового обеспечения функционирования мировых открытых сетей.

КОНСЦИЕНТАЛЬНАЯ ВОЙНА

Мир вступил в новый этап борьбы - конкуренции форм организации сознаний, где предметом поражения и уничтожения являются определенные типы сознаний. В результате консциентальной войны определенные типы сознаний просто должны быть уничтожены, перестать существовать, их не должно быть. А носители этих сознаний, наоборот, могут быть сохранены, если они откажутся от форм сознания - предметов разрушения и поражения. Типы сознаний - предметы поражения в консциентальной войне - должны быть вытеснены за рамки цивилизационно допустимых и приемлемых форм.

Уничтожение определенных типов сознания предполагает разрушение и переорганизацию общностей, которые конституируют данный тип сознания.

Можно выделить пять основных способов поражения и разрушения сознания в консциентальной войне:

- 1. Поражение нейро-мозгового субстрата, снижающее уровень функционирования сознания, может происходить на основе действия химических веществ, длительного отравления воздуха, пищи, направленных радиационных воздействий;
- 2. Понижение уровня организации информационно-коммуникативной среды на основе ее дезинтеграции и примитивизации, в которой функционирует и "живет" сознание;
- 3. Оккультное воздействие на организацию сознания на основе направленной передачи мыслеформ субъекту поражения;
- 4. Специальная организация и распространение по каналам коммуникации образов и текстов, которые разрушают работу сознания;
- 5. Разрушение способов и форм идентификации личности по отношению к фиксированным общностям, приводящее к смене форм самоопределения и к деперсонализации.

- *Основная цель консциентальной войны:* диаспоризация российского народа, фрагментация региональных и социально-стратовых общностей на основе слома всех существующих имиджидентификаций
- *Конечная цель использования консциентального оружия* это изымание людей из сложившихся форм мегаобщностей. Разрушение народа и превращение его в население происходит за счет того, что никто больше не хочет связывать и соотносить себя с тем полиэтносом, к которому до этого принадлежал. Разрушение сложившихся имиджиндентификаций нацелено на разрушение механизмов включения человека в естественно сложившиеся и существующие общности и замена этих эволюционно-естественно сложившихся общностей одной полностью искусственной - общностью зрителей вокруг телевизора. Неважно, как человек при этом относитесь к тому, что он видит и слышит с экрана телевизора, важно, чтобы он был постоянным телезрителем, поскольку в этом случае на него можно направленно и устойчиво воздействовать.

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Задачи построения гражданского общества в РФ как общества информационного, возрастание роли информации, информационных ресурсов и технологий в развитии граждан, общества и государства в XXI веке, выводят вопросы информационной безопасности на первый план в системе обеспечения национальной безопасности.

Понятие и структура информационной безопасности

- Соотнося определение информационной безопасности, данное в Федеральном законе “Об участии в международном информационном обмене” (ст. 2) с понятием “безопасность”, данном в Законе РФ “О безопасности” (ст. 1) под информационной безопасностью понимается: “состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз”. В соответствии с Конституцией РФ (ст. 84) Президент РФ определяет основные направления внутренней и внешней политики, в том числе в области информационной безопасности. Исходя из анализа Программы действий на 1996-2000 годы, ежегодных Посланий Президента Федеральному Собранию РФ (1994-1998 гг.) и Концепции национальной безопасности РФ, утвержденной Указом Президента РФ № 1300 от 17.12.1997 г., определены основные интересы и угрозы им в информационной сфере, основные задачи и принципы государственной политики по обеспечению информационной безопасности.

Жизненно важными интересами в информационной сфере являются:

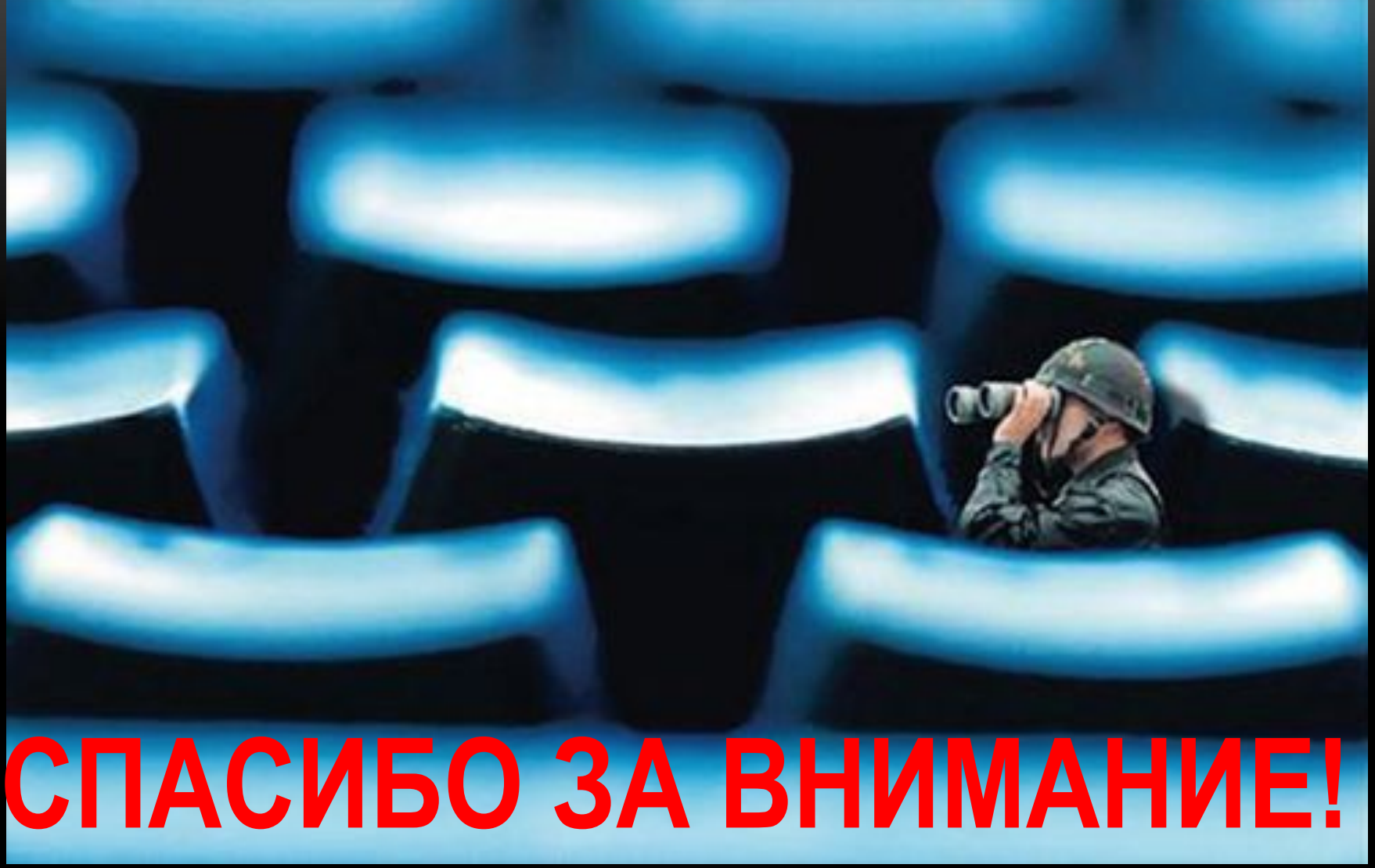
- а) *для личности:*
- соблюдение конституционных прав и свобод граждан на поиск, получение, передачу, производство и распространение объективной информации;
- реализация права граждан на неприкосновенность своей частной жизни;
- обеспечение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации.
- б) *для общества:*
- построение информационного общества;
- защита национальных духовных ценностей, пропаганда национального культурного наследия, норм морали и общественной нравственности;
- предотвращение манипулированием массовым сознанием;
- приоритетное развитие современных телекоммуникационных технологий, сохранение и развитие отечественного научного и производственного потенциала;
- в) *для государства:*
- защита интересов личности и общества;
- формирование институтов общественного контроля за органами государственной власти;
- формирование системы подготовки, принятия и реализации решений в органах государственной власти, обеспечивающей баланс интересов личности, общества и государства;
- защита государственных информационных систем, в том числе государственных информационных ресурсов.

Основные угрозы жизненно важным интересам личности, общества и государства в информационной сфере включают в себя:

- а) *внутренние:*
- отставание России от ведущих стран мира по уровню информатизации;
- ослабление роли русского языка как государственного языка Российской Федерации;
- размывание единого правового пространства страны вследствие принятия субъектами РФ нормативных правовых
- актов, противоречащих Конституции РФ и федеральному законодательству;
- разрушение единого информационного и духовного пространства России, активизация различного рода религиозных сект, наносящих значительный ущерб духовной жизни общества, несущих прямую опасность для жизни и здоровья граждан;
- отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам;
- б) *внешние:*
- целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем РФ;
- стремление сократить использование русского языка как средства общения за пределами России;
- попытки не допустить Россию участвовать на равноправной основе в международном информационном обмене;
- подготовка к информационным войнам и использование информационного оружия.

К *основным задачам в сфере обеспечения информационной безопасности* можно отнести следующие:

- формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере;
- совершенствование законодательства Российской федерации в сфере обеспечения информационной безопасности;
- координация деятельности органов государственной власти по обеспечению информационной безопасности;
- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;
- совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;
- развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;
- защита государственных информационных ресурсов и, прежде всего, в федеральных органах государственной власти, на предприятиях оборонного комплекса;
- духовное возрождение России;
- обеспечение сохранности и защиты культурного и исторического наследия (в том числе музейных, архивных, библиотечных фондов, основных историко-культурных объектов);
- сохранение традиционных духовных ценностей при важнейшей роли в этой деятельности Русской православной церкви и церквей других конфессий;
- пропаганда через средства массовой информации национальных культур народов России, духовно-нравственных, исторических традиций и норм общественной жизни и передового опыта такой работы;
- повышение роли русского языка как государственного языка и языка межгосударственного общения народов России и государств - участников СНГ;
- создание оптимальных экономических условий для осуществления важнейших видов творческой деятельности.



СПАСИБО ЗА ВНИМАНИЕ!