# Правовые проблемы информационной войны.

# Военный Университет

# Москва 2000

# Выполнил: Старостин В.И.

# Научный руководитель: Крылов Г.А.

# Правовые проблемы информационной войны.

Информационное противоборство ранее присутствовало практически во всех войнах в таких основных формах, как ведение разведки и противодействие ей, распространение дезинформации, слухов и борьба с ними (в т.ч. через цензуру) и т.п.

С появлением новых информационных технологий и организацией международного информационного обмена на новом уровне, информационная составляющая в стратегии обеспечения национальной безопасности, по оценке Совета Безопасности РФ, руководителей российских спецслужб и МО РФ вышла на первый план. По данным ФАПСИ, за последние 15 лет расходы на приобретение средств информационной борьбы увеличились в США в 4 раза и занимают сейчас там 1 место среди всех программ по вооружению.

Информационное противоборство в ходе ведения обычной войны начало переходить в свою новую, более высокую стадию -информационную войну.

**Термин "Информационная война"** (далее ИВ) появился в середине 1980-х годов в связи с новыми задачами Вооруженных Сил США после окончания "холодной" войны (разработка группы военных теоретиков США в составе: Экклз Г.Е., Саммерз Г.Г. и др.); начал активно употребляться после проведения операции "Буря в пустыне" в 1991 г., где новые информационные технологии впервые были использованы как средства ведения войны; официально впервые закреплен в директиве МО США от 21.12.1992 г. и в директиве Комитета начальников штабов ВС США Т9 3600.1. (12.1992 г.); детально разъяснен в Меморандуме № 30 (1993 г.) заместителей МО и Комитета начальников штабов ВС США. В военных кругах США **под информационной войной** понимаются - "действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии **посредством воздействия на информацию и информационные системы** противника, при одновременном обеспечении безопасности и защиты собственной информации и информационных систем".

К особенностям информационной войны можно отнести следующие:

* - охватывает в качестве самостоятельных объектов все виды информации и информационных систем, отделяя информацию от среды использования;
* - объекты могут выступать и как оружие и как объект защиты;
* - расширяет территорию и пространство ведения войн, ведется как при объявлении войны, так и в кризисных ситуациях в различных сферах жизнедеятельности;
* - ведется как специализированными военными, так и гражданскими структурами.

Концепция "*информационной войны*" по оценке российских спецслужб, предусматривает:

* - подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);
* - электромагнитное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба);
* - получение разведывательной информации путем перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счет специально внедренных в помещения и технические средства электронных устройств перехвата информации (радиоэлектронная разведка);
* - осуществление несанкционированного доступа к информационным ресурсам (путем использования программно-аппаратных средств прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением либо нарушением нормального функционирования этих систем ("хакерная" война);
* - формирование и массовое распространение по информационным каналам противника или глобальным сетям информационного взаимодействия дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения (психологическая война);
* - получение интересующей информации путем перехвата и обработки открытой информации, передаваемой по незащищенным каналам связи, циркулирующей в информационных системах, а также публикуемой в средствах массовой информации.

Эти оценки основных направлений ведения информационной войны подтверждаются выделением в программах Университета национальной обороны США таких форм информационной войны, как: радиоэлектронная борьба (РЭБ), война с использованием средств разведки, психологическая война, война с хакерами, кибернетическая война.

В целях реализации этой концепции (как в наступательном, так и оборонительном плане) в США проведены также и осуществляются следующие основные мероприятия:

1. Создана объединенная (МО и ЦРУ) Комиссия по безопасности, которая с 06.1993 г. по 02.1994 г. исследовала эту проблематику и пришла к выводу, что вторжение в информационные системы и сети - это "важнейшая угроза безопасности в этом десятилетии и, вероятнее всего, в следующем столетии...", 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".

2. Разработана и апробирована стратегия подготовки и ведения ИВ. Во всех видах Вооруженных Сил США созданы специализированные центры по ведению ИВ (Центр информационных боевых действий ВВС США - АFIWC (расположен в штате Техас на базе ВВС Келли);

Служба наземных информационных боевых действий Армии США -LIWA (расположен в штате Вирджиния в форте Белвуар).

При этом в Пентагоне каждый из видов войск имеет свою рабочую группу по этому проблематике. В уставах ВС США и нормативных документах изложены принципы и способы ведения ИВ.

3. Во всех видах ВС США созданы спецподразделения ведения ИВ и введены должности офицеров по проблемам ИВ. Во всех военных учебных заведениях введены спецкурсы по ИВ и идет подготовка специалистов ведения ИВ (в 1995 г. - первый выпуск).

4. В ВС США проводятся учения и штабные игры по этой проблематике (опыт учений 1994-1995 гг. обобщен в Пентагоне). Вовремя практических боевых действий за пределами США отраба­тываются конкретные операции ИВ с применением информацион­ного оружия.

5. Проведено 5 международных конференций по проблемам ИВ под эгидой Правительства США.

6. Принимаются меры по ежегодному совершенствованию национальной информационной инфраструктуры, где по оценкам представителей Правительства США, циркулирует до 80% конфиденциальной информации, в т.ч. особо важной.

Администрация Б.Клинтона в 02.1998 г. приняла решение о развертывании проекта по созданию новой сети Internet (Next Generation Internet) на территории США с новыми качественными характеристиками.

7. Ежегодно увеличиваются ассигнования на разработку новых видов информационного оружия (в МО, АНБ, ЦРУ США) и оснащение им национальных структур в объеме, превышающем с 1994 г., по оценкам экспертов, затраты на ракетно-ядерные и космические программы.

Информационное оружие, как и информационное противоборство по мере развития общества и информационных технологий претерпевало изменения. В современной практике под информационным оружием, по определению американских экспертов, понимается комплекс программно-информационных средств, созданных для поражения информационных ресурсов противника.

Однако сопоставляя это понятие с определением ИВ, принятым Комитетом Начальников штабов ВС США, надо признать, что это понятие является неполным, т.к. не включает в себя информационные системы, как цель поражения в ИВ.

Определение, данное российскими учеными и экспертами, представляется более точным.

**Информационное оружие** (далее ИО) - это "средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всего высокотехнологического обеспечения жизни общества и функционирования государства".

Информационное оружие от обычных средств поражения отличает:

* - скрытность - возможность достигать цели без видимой подготовки и объявления войны;
* - масштабность - возможность наносить невосполнимый ущерб не признавая национальных границ и суверенитетов, без привычного ограничения пространства во всех средах жизнедеятельности человека;
* - универсальность - возможность многовариантного использования как военными так и гражданскими структурами страны нападения, как против военных, так и гражданских объектов страны поражения.

По оценкам СВР РФ, приведенным на парламентских слушаниях в Государственной Думе РФ "Угрозы и вызовы в сфере информационной безопасности" (июль 1996 г.), сфера применения ИО включает, как военную область, так и экономическую, банковскую, социальную и иные области потенциального использования с целью:

* - дезорганизации деятельности управленческих структур, транспортных потоков и средств коммуникации;
* - блокирования деятельности отдельных предприятий и банков, а также целевых отраслей промышленности путем нарушения много­звенных технологических связей и системы взаиморасчетов, прове­дения валютно-финансовых махинаций и т.п.;
* - инициирования крупных техногенных катастроф на территории противника в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии;
* - массового распространения и внедрения в сознание людей определенных представлений, привычек и поведенческих стереотипов;
* - вызова недовольства или паники среди населения, а также провоцирования деструктивных действий различных социальных групп.
* При этом, в качестве основных объектов применения ИО, как в мирное, так и в военное время выступают:
* - компьютерные и связные системы, используемые государственными организациями при выполнении своих управленческих функций;
* - военная информационная инфраструктура, решающая задачи управления войсками и боевыми средствами, сбора и обработки информации в интересах вооруженных сил;
* - информационные и управленческие структуры банков, транспортных и промышленных предприятий;
* - средства массовой информации, и в первую очередь электронные (радио, телевидение и т.д.).

Это подтверждается и дополняется представителями Правительства США применительно к определению наиболее уязвимых объектов в национальной информационной инфраструктуре США для возможного применения ИО. К ним в США отнесены: телекоммуникационные узлы, центры спутниковой связи и каналы международного информационного обмена. ИО подразделяется по области применения на ИО военного и невоенного назначения.

ИО, применение которого возможно в условиях открытой войны **(радиоэлектронное подавление),** включает в себя средства со следующими функциями:

* - поражение обычными боеприпасами по целеуказаниям средств радио и радиотехнической разведки и частичным самонаведением на конечном участке;
* - поражение высокоточными боеприпасами нового поколения -интеллектуальными боеприпасами, самостоятельным поиском цели и самонаведением на ее уязвимые элементы;
* - радиолокационное подавление средств связи маскирующими помехами;
* - создание имитирующих помех, затрудняющих вхождение в связь, синхронизацию в каналах передачи данных, инициирующих функции переспроса и дублирования сообщений;
* - подавление с помощью средств силовой РЭБ (с помощью мощного электромагнитного излучения, создающего подавляющие помехи за счет паразитных каналов приема);
* - выведение из строя радиоэлектронных компонентов за счет воздействия больших уровней электромагнитных или ионизирующих излучений;
* - силовое воздействие импульсом высокого напряжения через сеть питания;
* нарушение свойств среды распространения радиоволн (например, срыв КВ-радиосвязи за счет модификации параметров ионосферы);
* - с помощью специальных методов воздействия на ЭВМ систем связи;
* - средства генерации естественной речи конкретного человека.

 Особую опасность ИО представляет сегодня для информационных компьютерных систем органов государственной власти, управления войсками и оружием, финансами и банками, экономикой страны, *а также для людей при информационно-психологическом воздействии на них с целью изменения и управления их индивидуальным и коллективным поведением.*

При этом по своей результативности информационное оружие сопоставимо с оружием массового поражения.

К ИО, применение которых возможно, как в военное, так и в мирное время, могут быть отнесены, средства поражения информационных компьютерных систем и средства поражения людей (их психики).

**К средствам поражения информационных компьютерных систем относят:**

1. Компьютерные вирусы - среди многообразия которых различают следующие основные группы:

- загрузочные (бутовые) вирусы, заражающие загрузочные сектора дискет и винчестеров;

- файловые вирусы;

- загрузочно-файловые вирусы;

- вирусы, заражающие файлы данных.

2. Программные закладки (типа "Логическая бомба", "Троянский конь") - программные закладные устройства, заранее внедренные в информационные системы и приводимые в действие по сигналу (в т.ч. со спутника) или в установленное время с целью уничтожения (модификации), получения информации или поражения ЭВМ.

3. Средства подавления информационного обмена в телекоммуникационных сетях, его фальсификации, передачи по каналам государственного и военного управления противника нужной для себя информации.

4. Средства, позволяющие внедрять программные закладки в государственные и корпоративные информационные системы (особенно постоянно действующие в режима реального времени) и управлять ими на расстоянии (от внедрения микропроцессоров и других компонентов в электронную аппаратуру и линии связи противника до создания международных сетей и систем, курируемых заинтересованными организациями). К таким средствам относят, например, нейтрализатор тестовых программ, обеспечивающий невозможность выявления естественных и искусственных недостатков программных средств специальными тестовыми программами.

Средства поражения компьютерных систем эксперты классифицируют по следующим критериям:

* - управляемость (возможность или невозможность дистанционного или непосредственного управления);
* - происхождение (самостоятельные, специально созданные или модифицированные программные средства);
* - объект воздействия (поражают системные или прикладные программы, дезорганизуют работу средств управления и др.);
* - время действия (разового или длительного действия);
* - способ ввода в действие (немедленного или отложенного действия);
* - способность к самовоспроизводству;
* - целевое предназначение (для поражения объектов информационного воздействия или для перераспределения данных).

**Средства поражения (воздействия) на людей и их психику** различают в зависимости от целей их применения в психологической войне. К таким целям относят:

* - искажение получаемой политическим руководством, командованием и личным составом вооруженных сил противника информа­ции и навязывание им ложной или бессодержательной информации, лишающей их возможности правильно воспринимать события или текущую обстановку и принимать верные решения;
* - психологическую обработку войск и населения;
* - идеологические диверсии и дезинформацию;
* - поддержание благоприятного общественного мнения;
* - организацию массовых демонстраций под ложными лозунгами;
* - пропаганду и распространение ложных слухов;
* - изменение и управление индивидуальным и коллективным поведением.

Наряду с использованием традиционных средств (печатные и электронные средства массовой информации) идет активная разработка и апробирование специальных средств воздействия на человека как через СМИ, так и через компьютерные сети: средства информационно-психологического (психофизического) воздействия (в т.ч. в рамках программ МК-Ультра - ультрамозговой контроль, МК-Дельта - дистанционное изменение поведения человека, Блю-берд, Артишок).

В числе таких разработок, уже получивших применение, называют голографические изображения в пространстве, вирус № 666 (выдает на экране ЭВМ особую цветовую комбинацию, вызывающую измененное состояния психики человека, вплоть до блокирования сосудов головного мозга у оператора ЭВМ).

Применение этих и других видов информационного оружия в условиях открытости и роста международного информационного обмена определяет особенности защиты информационных систем от его воздействия.

# Особенности правовой охраны и защиты прав на информационные системы

Следует различать правовую охрану и защиту прав на информацию в информационных системах и защиту прав в отношении самих информационных систем.

Правовая охрана прав собственника (владельца) на информационную систему возникает с момента ее создания (приобретения) и действует в объеме и порядке предусмотренном в ГК РФ (II раздел), что подтверждено ФЗ "Об участии в международном информационном обмене", где указано, что информационные системы используются только по волеизъявлению их собственника или уполномоченного им лица (ст.9), а доступ физических и юридических лиц к этим системам осуществляется по правилам, установленным собственником или владельцем этих систем в соответствии с законодательством РФ (ст. 12). В то же время такая правовая охрана в каждом конкретном случае будет иметь свою специфику в зависимости от вида информационных систем:открытые (для общего пользования) или закрытые (для ограниченного круга пользователей); государственные или негосударственные (корпоративные); внутрироссийские или международные и т.д.

Многообразие объектов и субъектов права в этой области требует от государства определить свой интерес и степень своего участия в их охране и защите.

Роль государства должна быть определена прежде всего в решении следующих проблем:

**Во-первых, - организация научных исследований** и разработка в этой сфере, где при общем сокращении объемов финансирования отсутствует должная координация, в результате чего даже немногочисленные средства распыляются и не дают должного эффекта. В сравнении с другими странами в 1997 г. в России объем расходов на научные исследования и разработки составил:

**а) в млн.долларов США**

1. США 170765.0
2. Япония 75165.8
3. ФРГ 36245.2
4. Франция 26164.1
5. КНР 22240.0
6. Великобритания 20792.0
7. Италия 12393.5
8. Канада 9446.1
9. Корея 7615.0
10. Индия 7100.0
11. Чехия 117б.5
12. Россия 800

**б) в процентах от ВВП**

1. Израиль 3.50
2. Швеция 3.05
3. Япония 2.90
4. Корея 2.62
5. США 2.45
6. Швейцария 2.44
7. Франция 2.38
8. Финляндия 2.31
9. ФРГ 2.27
10. Великобритания 2.19
11. КНР 0.82
12. Чили 0.56
13. Турция 0.46
14. Россия 0.33
15. Аргентина 0.30

**Во-вторых, - это установление льгот по инвестированию** в сферу информационных технологий, в сферу развития информационных систем. Если у государства нет достаточно средств для создания таких систем, то по крайней мере, нужно установить льготный режим кредитования, льготный режим для инвесторов, как отечественных, так и зарубежных. В то же время национальные интересы России в обеспечении приоритета производства и эксплуатации отечественных средств связи и обеспечения информационной безопасности требуют установления ряда ограничений. К их числу можно отнести:[[1]](#footnote-1)

* - при привлечении иностранных инвестиций - сохранение государственного контроля и участия в управлении предприятиями этой отрасли индустрии и дальнейшей эксплуатации произведенной продукции (например - для космической отрасли);
* - при использовании иностранных технологий, элементной базы и отдельных видов оборудования и средств связи - проведение их обязательной экспертизы и сертификации государственными органами России с точки зрения обеспечения безопасности;
* - при разработке, производстве и эксплуатации средств обеспече­ния информационной безопасности, включая программное обеспе­чение, использовать только отечественные технологии и средства защиты.

**В-третьих, - подготовка кадров,** без чего трудно реализовать задачи обеспечения информационной безопасности в информационных системах. Приказом Министерства общего и профессионального образования РФ № 1781 от 20.08.1997 г., наряду с существующими учебными заведениями по подготовке специалистов в этой области в системе МО, ФСБ, МВД, ФАПСИ была создана сеть из 14 региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы, где головным определен МИФИ (технический университет).

Требуется специальная федеральная целевая программа, предусматривающая подготовку специалистов (на условиях госзаказа) с учетом потребности как для государственных, так и негосударственных структур в этой сфере. Актуальность подтверждается тем, что новая глава 28 УК РФ о компьютерных преступлениях не будет в ближайшее время работать в полном объеме из-за отсутствия соответствующих специалистов среди оперативных работников, следователей, судей, прокуроров и т.д.

**В-четвертых,** необходимо определить перечень информационных систем, где государство должно нести 100% ответственность за их охрану и защиту (системы управления федеральных органов государственной власти, управления войсками и оружием, обеспечения банковской и финансовой стабильности и т.п.), критерии безопасности таких систем.

Так, например, в США компьютерные системы по критериям безопасности распределены по 7 классам:

* Д - с минимальной защитой;
* С-1 - с раздельным доступом (ограничение доступа пользователей на индивидуальной основе);
* С-2 - с раздельным и контролируемым доступом (регистрация любого ввода в систему, контроль операций каждого пользователя и изоляция массива данных);
* В-1 - с контролируемым доступом и с регулируемым уровнем безопасности (категории секретности всех данных, принудительный контроль доступа конкретных лиц к конкретным данным или операциям);
* В-2 - со структурированной защитой (четко определенная, задокументированная модель обеспечения безопасности по "критическим" и "некритическим" элементам защиты, дополнительные звенья контроля и управления);
* В-3 - со специальными комплексами безопасности внутренний механизм регистрации доступа любого пользователя к любым данным с полным исключением возможного несанкционированного доступа к данным при одновременном снижении до минимума сложности и размеров системы);
* А-1 - с доказуемым и проверяемым уровнем безопасности. Наличие такого рубрикатора позволяет легче осуществлять государственное регулирование при сертификации средств защиты и лицензировании деятельности в этой сфере.

Примером такой закрытой, со стопроцентным участием государства информационной системы может стать создаваемая в соответствии с Указом Президента РФ от 3.04.1995 № 334 информационно-телекоммуникационная система специального назначения в интересах органов государственной власти (ИТКС).

**В-пятых,** одновременно с этим, государство должно определить степень своего участия в регулировании процессов создания и функционирования закрытых негосударственных (корпоративных) систем, а также открытых систем, прежде всего, в интересах защиты прав граждан." Примером этому может служить нынешняя ситуация, когда банки, предприятия и организации устанавливают у себя импортное оборудование цифровых АТС с встроенным блоком полицейских функций, позволяющим вести запись в автоматическом режиме всех телефонных переговоров. Это, по мнению собственников таких систем позволяет им защитить более надежно свои права на коммерческую, банковскую, служебную тайну, но сточки зрения закона это грубо нарушает конституционные права граждан на тайну переговоров, в т.ч. тех, кто не является

работником данной организации. Другим примером неблагополучия в этой области может служить ситуация с цифровыми телефонными станциями общего пользования, ответственность за которые несет Госкомсвязи РФ. За пять лет число цифровых телефонных станций возросло с 2 до 76, а цифровых каналов до 70 тыс. В этом импортном оборудовании, по оценке спецслужб России, не исключены закладки обратной связи, позволяющие бесконтрольно снимать информацию в любое удобное время для поставщиков без ведома российских пользователей. А это уже не только нарушение конституционных прав граждан на тайну переговоров, но и с учетом возможностей информационного оружия - прямая угроза для безопасности всей страны.

**В-шестых,** государство должно установить более четко правовые регуляторы, запреты и ограничения при осуществлении международного информационного обмена.

В действующем ФЗ "Об участии в международном информационном обмене" ряд таких ограничений установлен:

* - включение информационных систем в состав средств международного обмена осуществляется при наличии международного кода в порядке, устанавливаемом Правительством **РФ,** а в отношении систем с особыми правилами доступа к информации - с разрешения Гостехкомиссии при Президенте РФ и ФАПСИ (ст. 10);
* - средства международного информационного обмена для обработки информации с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации в порядке, определяемом ФЗ "О связи" (ст. 17);
* - деятельность при вывозе (ввозе) информации государственных информационных ресурсов подлежит лицензированию (ст. 18);
* Выдача сертификатов и лицензий возложена законом на Гостехкомиссию и ФАПСИ (ст.9).
* -при обнаружении нештатных режимов функционирования информационных систем, т.е. возникновении ошибочных команд, а также команд, вызванных несанкционированными действиями обслуживающего персонала или иных лиц, либо ложной информации собственник или владелец этих средств должен своевременно сообщить об этом в органы контроля за осуществлением международного информационного обмена и собственнику или владельцу взаимодействующих средств международного информа­ционного обмена, в противном случае он несет ответственность за причиненный ущерб (ст.9);
* в случае противоправных действий органы исполнительной власти (РФ и субъектов РФ), осуществляющие контроль за между­народным информационным обменом, могут приостановить его на любой стадии до 2-х месяцев, что может быть обжаловано в суде (ст. 16, 19);
* - за противоправные действия нарушители несут гражданско-правовую, административную или уголовную ответственность (ст. 20).

Защита прав может осуществляться по выбору собственника (владельца) в административном порядке (в случаях, установленных прямо в законе: например, для пресечения монополистической деятельности и недобросовестной конкуренции - жалоба в федеральный антимонопольный орган), либо по общему правилу - в судеб­ном порядке (суд, арбитражный суд или третейский суд)

Только в УК РФ (глава 28) предусмотрена ответственность за правонарушения в этой области (ст. 272 - неправомерный доступ к компьютерной информации; ст.273 - создание, использование и распространение вредоносных программ для ЭВМ; ст.274 -нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети). Наряду с совершенствованием действующего законодательства РФ по вопросам международного информационного обмена необходимо объединение усилий всего международного сообщества по решению ряда проблем, являющихся специфическими для открытых информационных систем при таком обмене.

1 .Требуется унификация законодательства, т.к. киберпространство не признает национальных границ. Нужны единые подходы в борьбе с компьютерными преступлениями. Предпосылки для такой единой правовой политики создаются в странах Европейского Союза, Совета Европы и СНГ.

2.Сети международного информационного обмена резко расширяют возможности использования информационного оружия, добиться полного запрещения которого вряд ли удастся. Но ввести ограничения на производство и оборот этого оружия, международный запрет на ведение информационных войн можно и нужно.

В прошлом году автор выступил с инициативой, которая была поддержана парламентскими комитетами Госдумы, а в декабре 1997 года превратилась в политическую инициативу девяти государств СНГ. МПА СНГ приняла обращение в ООН, ОБСЕ, к странам Межпарламентского Союза с предложением включить в повестку дня Генеральной ассамблеи вопрос о подготовке и заключении международной конвенции «О предотвращении информационных войн и ограничении оборота информационного оружия». Это необходимо, чтобы мы не тратили средства, сначала на разработку информационного оружия, затем на защиту от него, а потом на его уничтожение, как это было ранее с ядерным, химическим и бактериологическим оружием в XX веке.

3. Нужен «кодекс чести» собственников, владельцев и пользователей открытых информационных систем (в т.ч. Internet - сообщества), как клятва Гиппократа у врачей, Кодекс поведения в Internet (Канада), хартия Internet (Франция). Основой для выработки такого Кодекса может стать Национальный кодекс деятельности в области информатики и телекоммуникаций, принятый Торгово-Промышленной Палатой РФ.[[2]](#footnote-2)

Безусловно, названные правовые проблемы и пути их решения не являются исчерпывающими. Актуальность темы требует объедине­ния усилий ученых и практиков, политиков и общественности, представителей всех ветвей государственной власти по дальнейшему исследованию этих вопросов, поиску путей эффективного обеспечения национальных интересов России в системе информационной безопасности.

1. Лопатин В.А. На спутниковую связь не хватает денег. Распыление средств ведет к технологическому отставанию \Независимая газета 0т 13.11.1997 [↑](#footnote-ref-1)
2. Копылов В.А. Информационное право М,1997г. с. 306-308 [↑](#footnote-ref-2)