Министерство образования Российской Федерации

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра радиоэлектроники и защиты информации (РЗИ)

# ГРАЖДАНСКОЕ ОБЩЕСТВО И ИНФОРМАЦИОННОЕ ОРУЖИЕ

Курсовая работа по дисциплине

"Теория и методология защиты информации"

## РТФ КР.000000.002

Студент гр.\_\_\_\_\_\_\_\_\_\_\_

Руководитель

Доцент кафедры РЗИ,

В.В. Загоскин

# РЕФЕРАТ

Курсовая работа 32 с., 7 источников, 1 приложение.

ИНФОРМАЦИОННОЕ ОРУЖИЕ, ГРАЖДАНСКОЕ ОБЩЕСТВО, ИНФОРМАЦИЯ, ЗАЩИТА ИНФОРМАЦИИ, МОРАЛЬНО – ПСИХОЛОГИЧЕСКАЯ ЗАЩИТА, ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ, НАПАДЕНИЕ, ПСИХОТЕХНИКА, УПРАВЛЕНИЕ, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ПСИХИЧЕСКАЯ ЗАЩИТА, СИСТЕМА ВЕРОВАНИЙ, КОМПЛЕКСНАЯ СИСТЕМА БЕЗОПАСНОСТИ.

Объектом исследования являются влияние морально – психологических средств и методов, как видов информационного оружия, на личность и гражданское общество в целом.

Цель работы – обзор и анализ способов и результатов применения некоторых видов информационного оружия и методов защиты от него.

В данной работе, главным образом, были рассмотрены основные способы влияния на человека морально – психологическими средствами, способы защиты от такого влияния и методы обнаружения такого влияния.

Данная работа может быть полезной как отдельным лицам для ознакомления с видами и способами воздействия информационного оружия, так и при построении комплексной системы защиты информации и подборке сотрудников при формировании кадрового аппарата.

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра радиоэлектроники и защиты информации (РЗИ)

УТВЕРЖДАЮ

### Зав. Кафедрой РЗИ, профессор

\_\_\_\_\_\_\_\_\_\_\_В. Н. Ильюшенко

"\_\_\_\_" \_\_\_\_\_\_\_\_\_г.

## ЗАДАНИЕ

**на курсовую работу**

**по дисциплине "Теория и методология защиты информации"**

**Тема работы:** Гражданское общество и информационное оружие

**Исполнитель:** ст-т гр.189 Ли Д.Р.

**Цель работы:** обзор и анализ способов и результатов применения информационного оружия и методов защиты от него.

**Содержание работы**

##### 1. Психическое нападение

2. Способы психологического воздействия и противодействия ему

3. Возможные объекты нападения

# 4. Организационные, технические и правовые методы обеспечения морально – психологической информационной безопасности

**Источники разработки:**

1. Терминология в области защиты информации. Справочник. – М.: ВНИИстандарт, 1993.

2. Данченко В. Принципы современной психической самозащиты. Электронный вариант.

3. Пимкин Д.Е. Морально-психологические средства и методы обеспечения информационной безопасности. Журнал "БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ" 1998г. 1/3

4. Левин А.А. Секрет фирмы. – М.: Сириус, 1992.

5. Ивонин М. В. Средства и методы защиты от информации. Журнал "БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ" 1998г. 1/3

6. Кулагин Ю. В. Доклад на 2-й Северо-Западной международной конференции "Бизнес и безопасность", 22 октября, Санкт-Петербург

7. Алдер Х. НЛП: современные психотехнологии. – СПб.: Издательство "Питер", 2000.-160 с.

#### Руководитель работы

#### Задание получил

Дата выдачи "\_\_\_"\_\_\_\_\_\_\_ г.

Срок сдачи работы "\_\_\_"\_\_\_\_\_\_\_ г.

# Содержание

Введение 6

1. Психическое нападение 7

2. Возможные объекты нападения 30

3. Организационные, технические и правовые методы обеспечения морально – психологической информационной безопасности 36

Заключение 40

Список использованных источников 41

Приложение А 42

# Введение

На протяжении последних десяти лет наша страна пытается перестроиться на новый лад развития. Этот путь перемен неразрывно связан с проведением реформ. Но понятие реформ не должно восприниматься узко - лишь как проведение экономических, либо политических преобразований. Это комплексная и трудоемкая задача. Перед Россией стоит проблема не только перестроить и стабилизировать политическую систему государства, внедрить новые приемы и методы в экономическом управлении страной, но более важной и базовой задачей является построение демократического общества, такого общества, которое можно было бы назвать гражданским.

Что же мы понимаем под термином гражданское общество? В первую очередь, - это сфера жизнедеятельности индивидов, не контролируемая государством.

При демократии общество контролирует выбор средств, которые

используют люди в процессе своей деятельности, в том числе и средств информационной борьбы. Только в том случае, если намерения людей имеют под собой как моральную основу, так и технологическую, этот выбор будет разумен.

Сейчас уже имеются средства, позволяющие создать информационное оружие, а так как информационное оружие является очень мощным оружием, то гражданское общество должно быть защищено от него не менее, чем от «традиционного» оружия. К воздействию информационного оружия уязвимы все. Всем известно, если возникает какое-либо «действие», то обязательно возникает «противодействие». Поэтому в данной работе была предпринята попытка осветить проблему «Гражданского общества и информационного оружия» как одной неразрывно связанной системы, в контексте морально-психологической защиты единицы гражданского общества-личности, индивидуума – от информационного оружия. Также рассматриваются виды информационного оружия.

# 1. Психическое нападение

## 1.1 Патогенные системы верований

На человека может быть совершено психическое нападение. Психические нападения - это различные отрицательные психофизиологические состояния, рассматриваемые пострадавшими как наведенные извне, как исходящие от другого человека, с которым пострадавший в момент нападения не находился в непосредственном контакте. Феномен психического нападения наблюдается лишь в тех случаях, когда потенциальная жертва разделяет ту или иную патогенную (болезнетворную) систему верований, то есть систему верований, которая предполагает возможность психического нападения, способного повлиять на здоровье человека. Таким образом, психическая защита представляет собой по существу защиту от патогенных систем верований. Сразу же следует уточнить, что всецело патогенных систем верований не существует. Системы верований могут быть патогенными в своих частных аспектах, предполагающих принципиальную возможность нападения.

Можно выделить три основные патогенные системы верований: народную (в ней циркулируют такие патогенные понятия, как, например, «дурной глаз» и «наведение порчи»), оккультную («астральные шнуры», «лярвы», «инвольтация») и биопольную («телепатическое воздействие», «лучи», «пучки энергии», «заряды отрицательной информации» и т.д., и т.п.).

Народная система патогенных верований отличается отсутствием собственной концептуальной основы: это система верований в прямом смысле слова, - хотя для объяснения эффектов производимых, скажем, «дурным глазом», могут привлекаться оккультные и биопольные толкования.

Оккультная система патогенных верований, напротив, основана на огромном массиве оккультных теорий и становится их логическим следствием: чтобы испытать на себе патогенное воздействие оккультной системы верований, человеку предварительно необходимо освоить эти теории.

Особенность биопольной системы патогенных верований состоит прежде всего в том, что фактический материал, истолкованием которого она является, относится к ощущениям в теле (соматической и висцеральной природы) и колебаниям общего психофизиологического тонуса организма, а не к визуализациям, как в традиционной оккультной системе верований. Особенность этой системы состоит также в том, что она апеллирует не к анимистическим «потусторонним» силам и сущностям, а к объективным биофизическим процессам. И, наконец, биопольная система верований, в отличие от традиционно-оккультной не противопоставляет себя привычной нам научно-популярной картине мира и не «надстраивается» над ней, но органично из нее вырастает. И поэтому ее, в отличие от оккультной системы верований, гораздо труднее рассматривать как систему верований.

#

## 1.2 Как это происходит. Абсолютная защита и ее относительность

Как же происходит нападение? Итак, исходная задача нападающего («экстрасенса») при работе с обычным человеком («не экстрасенсом») состоит в том, чтобы овладеть его воображением, суметь внушить ему мысль о возможности экстрасенсорного воздействия. Это достигается за счет приобщения, «подключения» человека к специальной системе верований.

«Вновь подключенный», ощущая превосходство экстрасенса как профессионала, причастного к «скрытому знанию» данной системы верований, открывает свою психику для манипуляций со стороны индуктора и превращается тем самым в жертву. В зависимости от поставленной задачи и квалификации, воздействие нападающего может положительным или отрицательным образом сказываться на здоровье и самочувствии жертвы, а также не отражаться на нем вовсе.

«Абсолютной защитой» против патогенных факторов любой системы верований служит принципиальное неверие и, в особенности, насмешка.

Следует заметить, однако, что пассивно используемая абсолютная защита неверия не всегда эффективна и может давать пробои. Известна, например, история одного журналиста, собиравшего материал о шаманах. Однажды, присутствуя на церемонии, он неожиданно почувствовал, что входит в измененное состояние, что шаман, имеющий безраздельную власть над умами своих суеверных соплеменников, каким-то непостижимым образом коснулся и его собственного цивилизованного сознания. Неизвестно, чем бы все это кончилось, если бы у журналиста не оказался под рукой портативный магнитофон, на транзисторах, конденсаторах, пассиках и валиках которого он сосредоточил все свое внимание. Эти детальки были в тот момент воплощением величия и мощи нашей технократической цивилизации и порожденной ею системы верований, в рамках которой бормочущий нелепые заклинания шаман был всего лишь невежественным дикарем.

В данном случае магнитофон послужил не чем иным, как инструментом активации неверия, обеспечив тем самым требуемую защиту. Очевидно, что если бы этот журналист знал кое-что о биополях, магнитофон вряд ли смог бы ему помочь. Ведь магнитофон действует, так сказать, посредством полей, электромагнитных полей, и шаман действует посредством полей, - в том числе и электромагнитных.

Как частная система верований, концепция биополя органично вписывается в целостную картину мира, выстраиваемую современной наукой, - картину мира, которая сегодня для преобладающего большинства людей составляет предельную, абсолютную систему верований, тождественную «реальности». Осуществляя в рамках биологических объектов фактически ту же функцию, которую в случае физических объектов выполняет гипотетическое гравитационное поле, биологическое поле представляется чем-то не менее «реальным».

Однако наряду с концепцией биополя право на «реальное» существование неизбежно получает и логическое следствие этой концепции: принципиальная возможность дистантного (полевого) взаимодействия между биологическими объектами, а отсюда и возможность оперирования биополями. А когда человеку кажется, что его полями оперируют, хвататься за магнитофон в поисках защиты от «средневекового мракобесия» уже бесполезно.

Итак, существует ряд традиционных патогенных верований, насмеяться над которыми (то есть применить абсолютную психическую защиту) не составляет особого труда, - в крайнем случае достаточно три раза поплевать через левое плечо или повернуть картуз на голове козырьком назад. С современной биопольной системой верований, однако, дела обстоят сложнее и картузом здесь не отвертишься. В связи с выходом данной системы верований на просторы СМИ абсолютная защита от нее крайне затруднена, «не верить вообще» становится все труднее.

Не легче удерживаться и в рамках не вовлеченной «малой веры»: к моим, мол, биополям ваши никакого отношения не имеют. Имеют, и самое непосредственное! Поэтому в настоящее время возрастает значение таких форм защиты, которые бы не просто пытались откреститься от этой системы верований, но разрабатывались на ее основе.

Существует две формы «защиты от биополя»: с изменением объекта восприятия и с изменением субъекта восприятия. Однако прежде, чем перейти к описанию принципиальных механизмов психической защиты, необходимо сказать несколько слов о механизмах психического нападения, - о том, что подвергается нападению и как это нападение происходит. Инструмент психического нападения будем далее условно называть отрицательным зарядом, а для описания механизма нападения воспользуемся условной «пространственной» моделью внутреннего мира.

Когда агрессор посылает возможной жертве отрицательный заряд, процесс этот протекает на самом внешнем из внутренних уровней – «энергетическом». Отрицательный заряд внедряется в эту оболочку и вызывает, как теперь говорят, резкое нарушение ее «энергетического баланса», десинхронизацию ее «силового каркаса» и т.д. Жертва субъективно переживает это событие как падение общего психофизиологического тонуса, чувство общей слабости, упадка сил или, если его чувствительность достаточно развита, как специфические ощущения в различных областях переживаемой им «схемы тела» (то есть в так называемых «центрах» или Чакрах).

Следует особо подчеркнуть, что в абсолютном большинстве случаев резкое снижение тонуса происходит в результате естественного несовпадения индивидуальных полевых характеристик, а не в результате злонамеренного психического нападения. При таком несоответствии более сильное поле на некоторое время десинхронизирует более слабое.

Итак, объективным симптомом первой фазы психического нападения - внедрения отрицательного заряда в энергетическую оболочку - служит снижение общего психофизического тонуса или какие-то отрицательные ощущения в «схеме тела». Надо сказать, что эта яркая в своей очевидности фаза психического нападения для жертвы совершенно безопасна. Энергетическая оболочка очень подвижна, она непрерывно регистрирует изменения в энергетике окружающей среды, причем эта ее информационная функция выполняется тем более эффективно, чем более чутко и полно она реагирует на любые формы внешних воздействий вне зависимости от характера последних. И если внутренние оболочки - эмоциональная и интеллектуальная - не задеты, то никакое внешнее воздействие не может на сколько-нибудь продолжительный срок патологически изменить ее структуру, нарушить стабильность, произвести «разрушение» и т.д. Если более глубокие оболочки не затронуты, то даже при отсутствии какой-либо специальной защиты результат психического нападения сводится исключительно к падению физического тонуса и общей слабости, которая может продолжаться от двух часов до двух дней.

Однако беда в том, что люди, как правило, неспособны различать свои оболочки, неспособны невовлечённо наблюдать жизнь своих более поверхностных оболочек. Поэтому отрицательный заряд беспрепятственно проникает сквозь энергетическую оболочку в оболочку эмоциональную.

Это проявляется в том, что у человека портится настроение, он становится раздражительным или подавленным, он проецирует свои эмоции вовне или во внутрь, - короче говоря, проникновение отрицательного заряда в эмоциональную оболочку субъективно переживается во всем диапазоне отрицательных эмоциональных состояний, особенности которых определяются темпераментом жертвы и другими индивидуальными факторами, причем эмоции разворачиваются на фоне отрицательного физического состояния (которое возникло в результате имевшего место прободения энергетической оболочки).

В конце концов, жертва начинает волноваться: он обеспокоен своим состоянием и пытается выяснить, с чем оно связано. Это свидетельствует о том, что из эмоциональной (витальной) оболочки отрицательный заряд проник в оболочку интеллектуальную (ментальную).

Жертва начинает размышлять о своем состоянии, он начинает искать его причины. И тут до него доходит: «Да на меня ведь совершено психическое нападение!!» (хотя не исключено, что он просто слишком плотно пообедал). Он начинает со всех сторон обыгрывать эту тему: включилось ВООБРАЖЕНИЕ. Если же он при этом еще испугался.

Все. Можно считать, что нападение было успешным: цель поражена. Следует заметить, что «отрицательный заряд» сам по себе еще не приносит болезни и т.п., хотя и может быть ориентирован на выполнение той или иной конкретной задачи. Сам по себе он лишь создает соответствующую патогенную «отрицательную доминанту» - очаг господствующего возбуждения в психике жертвы на трех ее уровнях - ментальном, эмоциональном, и «энергетическом». Эта отрицательная доминанта нарушает равновесие и приводит к общей десинхронизации функций на всех трех уровнях, то есть создает идеальные условия для заболевания.

1**.3 О природе отрицательной доминанты**

Итак, что питает отрицательную доминанту? Обычно картина представляется следующим образом. Экстрасенс устанавливает с жертвой некую связь, так называемый «раппорт». В конце XIX в. раппорт описывали как нечто вроде «психического кабеля», - шланга, по которому индуктор может нагнетать в бедную жертву (или отсасывать у него) все, что ему заблагорассудится, причем в неограниченных количествах. Тут уж вся надежда на «опытного оккультиста», способного кабель «перекусить». Сегодня говорят о полевых взаимодействиях: индуктор якобы «впечатывает» в полевую структуру жертвы некое «деструктирующее клише отрицательной информации», так называемого «вампира.

Секрет заключается в том, что вас все это не так. Между нападающим и жертвой действительно устанавливается раппорт, в каких бы терминах он не описывался; не важно, какова концептуальная модель, - раппорт есть, это психологический факт. Да, раппорт - это действительно инородное тело в «тонком теле» жертвы, «наведенная» структура в его «энергетическом каркасе». Но энергосистема этой наведенной структуры бесконечно более слаба, чем целостная энергосистема организма жертвы.

Да, раппорт - это действительно своеобразный паразит, получающий подпитку от жертвы, «живущий его соками»; но в масштабном отношении по сравнению с жертвой он подобен клопу. А много ли наших соков удается выпивать клопу? Да, раппорт действительно создает «отрицательную доминанту», но НЕ ОН ЕЕ ПИТАЕТ, - ОН ЕЮ ПИТАЕТСЯ!

Ее питает наше воображение. Задача раппорта - обрушить на нас нашу собственную силу, включить лавинообразный каскад нашего воображения. Именно воспаленное воображение заставляет человека усматривать в клопе вампира, и именно в воображении находится ядро «отрицательной доминанты». А механизм доминанты в том и состоит, что питает себя она сама. Заодно доминанта питает и исподволь стимулирующий ее раппорт. Если бы не эта обратная связь, если бы раппорт не получал своей минимальной подпитки, - а нужно ему совсем немного, - то в самом скором времени он бы усох и отпал.

Наводка и внедрение отрицательного заряда, устанавливающего раппорт, служит лишь «затравкой» в механизме психического нападения. Жертва «переваривает» этот заряд очень быстро, а затем, если нападение было успешным, начинает посредством отрицательной доминанты переваривать самого себя - и, кстати говоря, вполне может довести этот процесс до летального исхода.

В случае, когда возникает возможность неконтролируемой реакции психического самопереваривания, возникает, естественно, и необходимость в психической самозащите, то есть в защите от самого себя.

Однако, если отрицательный заряд не проникает глубже энергетической оболочки, естественное назначение которой - взаимодействовать с любыми влияниями (как положительными, так и отрицательными, как сильными, так и слабыми), то необходимости в защите не возникает. Йоги, например, развивающие свое сознание и разотождествленные со своими оболочками, вообще не пользуются защитой, поскольку любая защита закрывает нас от мира и делает менее сознательными. Но если человек не властен над своим внутренним миром, в определенных ситуациях у него возникает необходимость от этой «части себя» защищаться.

## 1.4 Общие принципы концентративной защиты

В результате успешного психического нападения в сознании жертвы возникает патогенная отрицательная доминанта. Задача *защиты с изменением объекта восприятия* сводится к тому, чтобы «выбить» эту доминанту другой доминантой. Существует два основных вида защиты «с изменением объекта», условно рассчитанных на людей концентративного и медитативного типа.

Принцип концентративной защиты очень прост: при первых симптомах «нападения» необходимо резко сосредоточить внимание на заданном «объекте-хранителе», представляющем собой по существу не что иное, как активатор дополнительной системы защитных верований. Действительно, при невозможности отказаться от принятой патогенной системы верований борьба с ее нежелательными эффектами может производиться лишь посредством создания в рамках основной системы некой дополнительной, нейтрализующей ее системы защитных верований.

Иногда в поисках «защиты от биополя» обращаются к традиционным оккультным формам защиты «с изменением объекта». Однако традиционные приемы могут эффективно выполнять свою функцию лишь в том случае, если человек включен в сложную систему специальных оккультных верований и поэтому вряд ли могут быть рекомендованы «непосвященным»: ведь для того, чтобы иметь возможность ими воспользоваться, человек должен был бы предварительно принять в себя тот легион оккультных фобий (страхов), от которых потом можно было бы защищаться. Игра здесь явно не стоит свеч.

Современные, биопольные методы концентративной защиты характеризуются простотой методикой и дополнительной системой верований. Речь идет прежде всего о создании всякого рода «защитных оболочек», об «уплотнении индивидуального поля» и т.д., а по существу - об экстериоризации тактильной (осязательной) чувствительности. В отличие от оккультной, биопольная дополнительная система верований ориентирована не на потусторонние анимистические силы и не на антропоморфно-сознательную помощь «оттуда» по типу ангелов-хранителей, или Оккультной Полиции, а на естественные биоэнергетические процессы. Другими словами, ориентация этой системы защитных верований не мистична, а научна, поскольку «научны» и биоэнергетические страхи, порождаемые нашим временем.[2]

2.**Способы психологического воздействия и противодействия ему**

Люди в ряду источников информации занимают особое место как активный элемент, способный выступать не только источником, но и субъектом злонамеренных действий. Люди являются и обладателями, и распространителями информации в рамках своих функциональных обязанностей. Кроме того, что люди обладают информацией, они еще способны ее анализировать, обобщать, делать соответствующие выводы, а также, при определенных условиях, скрывать, продавать и совершать иные криминальные действия, вплоть до вступления в преступные связи со злоумышленниками как добровольно, так и посредством оказанного на него давления.

Воздействовать на ум и поведение человека можно различными путями, одни из которых требуют лишь специфичной подготовленности специалиста (внушение), а другие - еще и специальной аппаратуры (технотронные приемы, зомбирование). Методы прицельного влияния могут быть щадящими (внушение) и изощренными (зомбирование), трудноуловимыми (нейро - лингвистическое программирование) и дополняющими (фармакоуправление).

Еще раз повторимся, одним из важнейших атрибутов психологического воздействия на личность является то, что человек зачастую не подозревает о происходящих в его сознании изменениях. И поэтому овладеть навыками психологической защиты может только человек, знакомый с техникой атаки.

## 2.1 Внушение

Под внушением подразумевается передача информации с внедрением заключенных в ней идей без какой-либо критической оценки и логической переработки предлагаемого. О том, что сработало внушение, а не осознанный выбор говорит сугубо эмоциональная реакция на малейшую попытку обсуждения "заветной истины", причем все противоречащее ей отвергается с порога, и чем убедительнее доводы, тем сильнее возмущение.

**Методы внушения используют**:

* для блокировки нежелательного поведения или мышления человека;
* для склонения индивида к требуемому действию;
* для быстрого распространения полезной информации и(или) необходимых слухов.

**Хорошо подвержены внушению те, кто**:

* проявляют себя слабой личностью (робкие, стеснительные, пугливые);
* некритично воспринимают других (простодушные, доверчивые);
* склонны зависеть от других (ищут себе хозяина, исключительно услужливые...).

**Трудно поддаются внушению те, кто**:

* обладают деловой активностью (энергичные и инициативные);
* являются сильной личностью (а также самолюбивые и высокомерные);
* противопоставляют себя другим (замкнутые и угрюмые);
* исключительно активно проявляют свои чувства (эксцентричные и откровенные);
* не зависят от других, а наоборот, имеют кого-то в своей зависимости

**Проведению внушения способствуют**:

* полное отсутствие, или чрезвычайная противоречивость текущей информации;
* очень авторитетный (как живой, так и печатный) и при этом "свой" источник;
* внутреннее ощущение зависимости;
* сильное психофизическое истощение и переутомление объекта;
* некая психологическая напряженность (гнев, экстаз, страх, поиск выхода из сложной ситуации);
* явная желательность или приятность внушаемого;
* жесткая категоричность заявлений и требований;
* шоковая неожиданность сообщения;
* повторяемость подсовываемой информации;
* абсолютная логичность и особая эмоциональность сообщаемого;
* некоторые болезни и особенности личности (психопатия, импотенция, слабость логического мышления, суеверность, наркомания).

**Проведению внушения иной раз мешают специфические внутренние барьеры, таковые, как**:

* критически-логический (отвержение всего, что кажется логически необоснованным);
* интуитивно-аффективный (отметание всего, что не вызывает подсознательного доверия или уверенности);
* этический (неприятие того, что противоречит нравственно-этическим воззрениям личности).

Преодоление барьеров подразумевает лишь умелое подстраивание под них. Так, для воздействия на лиц со слабым интеллектом, нужное внушение лучше сочетать с усиленными отрицательными эмоциями, а ежели данное лицо вполне интеллектуально или же заведомо внушаемо - то использовать положительные эмоции. В случае, когда объект подавлен или слишком неуверен в себе, должное внушение выполняют эмоциональным повелительным тоном с привлечением мимики и жестов, оформляющих неоднократно повторяемые резкие, короткие, как бы "вколачиваемые" фразы. Если объект излишне возбужден и значительно обеспокоен, то внушают успокаивающим тоном, с применением неоднократно повторяемых мягких, убаюкивающих, длинных фраз. Главное - не вызвать ни малейшей настороженности, но очаровать и словно бы заворожить персону. Когда обрабатываемый избыточно тщеславен, то имеет смысл "атаковать" его любовью, безудержно расхваливая и высказывая комплименты, способствующие представлению объекта о своей значительности; параллельно с этим удается косвенно внушать нужные идеи. Так как эффективное внушение обусловливается подсознанием, перспективной является попытка разбудить фантазию (к примеру, эротическую) у человека, каковой при этом погружается в себя так, что грани между подсознанием и сознанием стираются. Психика в подобном случае становится податливой ко всяким изменениям и к восприятию любого знания. О вхождении в такое состояние говорит расслабленность лица со всецело отрешенным и остановившимся взглядом.

В некоторых ситуациях применяют незаметное для окружающих подпороговое внушение, каковое осуществляется тихим шепотом, не воспринимаемым сознанием объекта. Превосходным каналом передачи нужного внушения служат тщательно отобранные слухи. Здесь работает тот факт, что подслушанные или вскользь уловленные идеи часто действуют сильнее тех, что навязываются впрямую.

## 2.2 Гипноз

Под гипнозом подразумевают состояние специфического сна, или же зауженного осознания с совершенным отключением критического восприятия и повышенной чувствительностью к внешнему внушению.

Слабой стороной гипнотического воздействия является то, что его невозможно применять против желания объекта. Исключение составляет гипнотическая обработка спящего человека.

**Техника гипноза может быть использована**:

* для получения информации (гипнодопрос);
* при секретной пересылке сообщений;
* для внедрения дезинформации;
* с целью программирования на желаемое поведение.

**Хорошо гипнотизируются**:

* лица художественного типа;
* социально адаптированные общительные личности;
* очень тревожные и значительно потеющие люди;
* все хронические алкоголики и наркоманы;
* те, кто болен энурезом (ночным недержанием мочи) или страдает астмой.

**Трудно загипнотизировать**:

* лиц мыслительного типа;
* психастеников, зацикленных на всяческих сомнениях и перетасовывании своих переживаний.

**Различают три стадии гипноза**:

* легкую (сонливость): объект может с легкостью и тотчас же, как пожелает оборвать сеанс;
* среднюю (гипотаксия): полная расслабленность при сохранении уверенности в том, что есть возможность побороть сонливость, правда делать этого совсем не хочется;
* глубокую (сомнабулизм): человек не реагирует ни на какие раздражения, и поддерживает речевой контакт (раппорт) только со своим ведущим; в данном состоянии кодируют на действие (сроком до одного года), а подчас расщепляют личность на несколько отдельных "Я", каждое из коих в состоянии жить своей особой жизнью, не подозревая о существовании других: все переживания в этой фазе четко амнезируются (как бы забываются).

Для введения объекта в гипнотический транс требуется создавать условия, благоприятствующие последнему и, ориентируясь на ситуацию, применять подходящие приемы, тщательно отслеживая внешние признаки вхождения в трансовое состояние.

**Хорошо содействуют, а порой и сами по себе вводят человека в транс**:

* сильная усталость и сонливость;
* пасмурная и дождливая погода;
* полусумрак вечера и тишина;
* поза удобная для сна или же, наоборот, предельно неудобная и непривычная позиция;
* ритмичные раскачивания и вращательные движения всего тела и головы;
* полное отсутствие реальных раздражителей (сенсорный голод) либо монотонные ритмичные воздействия физической природы (зрительные, тактильные и слуховые);
* ритмичная "шаманская" или "космическая" музыка;
* резкий и сверхмощный раздражитель (удар гонга, вспышка света, неожиданная пощечина, выкрик-приказ...);
* интенсивный эмоциональный подъем, в том числе половое возбуждение;
* состояние страха и ярости;
* пережимание сонных артерий и надавливание на глазные яблоки или прочие фрагменты тела (ухо, локоть, лоб, запястье).

Для углубления гипнотического состояния нужно очень тихим голосом внушать красочные образные представления покоя, мышечной расслабленности и полного отключения от окружающих с восприятием лишь слов внушения.

Проще всего, вызвать гипнотический транс у нормально спящего, ибо у последнего отсутствует какая-либо воля к сопротивлению. Это осуществляют в фазах специфического "быстрого сна", первая из коих наступает через 45-90 минут после засыпания. Данных фаз в течение ночи отмечают несколько, и перед началом их индивид каждый раз поворачивается в постели.

Все внушения в гипнозе делают негромким голосом, с помощью коротких, повторяемых по несколько раз фраз с незначительными паузами между ними. Ключевые слова подают в тот момент, когда человек делает очередной вдох. Весь сеанс обычно длится не более 15-20 минут.

Чтобы индивид впоследствии не вспомнил о происшедшем, ему следует внушить, что перед пробуждением он увидит яркий сон, но как только сновидение появится, он незамедлительно проснется; сон при этом хорошо ему запомнится, а все что было до того - забудется.

**Частные методики решения специальных задач с применением гипноза таковы**:

**Гипнодопрос**. Человека вводят тем, или иным способом в гипнотический транс и, установив раппорт, настраивают отвечать на задаваемые вопросы, причем первые из них должны быть самые простые (о погоде, имени, профессии), чтобы не возбудить даже легкой настороженности. Профессиональному солдату или служащему хорошо внушить, что перед ним его начальник, ждущий самого подробного доклада. Иногда используют методику свободных ассоциаций, при которой произносят ключевое слово и желают, чтобы визави сообщил то, что придет ему на ум. Следует воздерживаться от вопросов, явно настраивающих на конкретные ответы, ибо под гипнозом индивид способен выдать вымышленную информацию даже при легком непреднамеренном давлении со стороны допрашивающего.

**Пересылка тайной информации**.

Человека вводят в гипнотический транс и сообщают некоторую информацию, развивая амнезию на представленное. После этого он окажется способен передать услышанное только будучи опять же погружен в гипноз и в этом состоянии уловит установленное в основном сеансе кодовое слово (или фразу) как пароль, вскрывающий его память.

**Сотворение дезинформации**.

Загипнотизированному субъекту тщательно внушают, что он якобы участвовал в какой-то акции, видел некое событие, слышал закулисную беседу, добыл ту, или иную информацию. Выйдя из кодируемого состояния человек верит, что рассказанное ему было на самом деле и с уверенностью сообщает это другим.

**Программирование на нужное поведение**.

Данный трюк обычно удается только при глубокой стадии гипноза. После погружения в транс, объект, с применением определенных слов и представлений, трансформируют в желаемую личность, как бы имитирующую известный из литературы, кинофильма, либо реальной жизни персонаж. Такую акцию осуществляют с помощью специально установленных кодовых фраз, причем новых личностей здесь может быть несколько (многоуровневое программирование применяемое при зомбировании) Сходным образом возможно закодировать объект на конкретное деяние, каковое он обязан будет совершить, если услышит кодовое слово или же возникнет некоторая ситуация. Следует учитывать, что "лобовое" поствнушение, явно противоречащее нравственному принципу объекта чаще всего не реализуется, а поэтому приходится использовать причудливые обходные (скажем, имитацию игры, или обман) маневры. Автоматика срабатывания по конкретному сигналу сохраняет силу в продолжении примерно одного года.

## 2.3 Наркодопрос

В технике профессионального допроса наркотики используют для создания в сознании индивида определенной "сумеречной зоны". Наркотик обеспечивает растормаживание конкретных сдерживающих центров мозга, и человек не может ясно рассуждать и что-либо придумывать, хотя память о прошлом у него обычно сохраняется. Если воздействие наркотика было не очень сильным и у объекта не исчезло сознание, чтобы понять то чем у него спрашивают, то он в состоянии скрыть правду. Сложность, поэтому, лежит в подборе оптимальной рабочей дозы препарата, которая должна исключить способность к сознательному сопротивлению (возможного при скудной дозе), и не допустить, чтобы объект "нес околесицу" (при слишком большой дозе). Ввод наркотического вещества обычно прекращают тогда, когда веки у человека начинают дрожать, а речь становится нечеткой. Сопротивляемость наркотику довольно субъективна и, в частности, зависит от физического состояния, психического типа, имеющегося опыта и других сугубо индивидуальных факторов. Иной раз человек выкладывает информацию лишь после получения третьей - четвертой порции любой из "сывороток правды". Конкретные вопросы обычно формулируют предельно кратко (чтобы допрашиваемый не забыл их начало при изложении конца и еще в них должна отсутствовать внушаемость). Последнее особенно относится к невротикам, которые чрезвычайно склонны к фантазиям. Освободившись от влияния наркотика допрошенный, как правило, не помнит о содержании выданной им информации и не имеет представления о продолжительности сеанса.

Химические препараты, подавляющие волю, можно обнаружить в крови не далее, чем через несколько часов после укола, а след иглы обычно виден пару дней, хотя имеются иглы (к примеру, инсулиновые), не оставляющие никаких следов. Всегда надо учитывать, что многие наркотики сильнее действуют весной и летом, а также на рассвете, утром, или в бурю.

Если воздействию наркотика принудительно подвергли Вас, желательно определить его ведущий тип, фиксируя внимание на доминирующее ощущение (блаженство, безразличие и разные нюансы восприятия), значительных изменениях в величине и четкости предметов, а также в насыщенности освещения.

**Для преодоления прессинга от "сывороток правды" можно попробовать**:

* сосредоточить внимание на определенной реальности (тиканье часов, пятно от влаги на стене) и осознав по этому фиксированному эталону, что реалистичность мышления ухудшается, предельно сконцентрироваться на необходимости преодолеть накатывающее состояние и очень четко мыслить;
* зациклиться на воспоминаниях о неких эмоциональных, но не существенных с позиций безопасности вещах (таких, как секс, переживания вины, зависти, злобы), отстраняясь подобным образом от нежелательной опасной исповеди;
* сосредоточиться на воспоминаниях чего-либо (или кого-либо) особо дорогого;
* пробовать запутать мысленный процесс, высказывая всяческие несуразности.

**Вызов болтливости у собеседника**

В реализации подобной цели используется свойство наркотических веществ заметно растормаживать психику, что часто вызывает эйфорию с повышенной общительностью и дружелюбием при исчезновении настороженности и сдержанности. Для этого можно:

* предложить человеку сигарету, в которой к табаку подмешано немного (около горошины) сушеных листьев и верхушек конопли;
* добавить в алкоголь 0,05 г барбамила (поскольку барбамил блокирует переработку алкоголя, избыток его дозы способен оказаться жизненно опасным для организма).

**Кодирование объекта на желаемый поступок**

Химические препараты и техника введения в транс здесь те же, что и в случае наркодопроса, а схема выполнения внушения - как при гипнозе. Внушение делается резким и энергичным императивным тоном в период засыпания (когда используемая доза препарата мала) или во время пробуждения (если доза велика).

Известный недостаток наркопрограммирования заключается в том, что оно менее стойко, чем гипнотическое, а удобство - что его можно применять против желания объекта.

В работе с наркоманом, конкретное внушение осуществляется перед уходом его в обычный наркотический сон (опий) или на фоне спонтанно возникающих, а затем направляемых галлюцинаций (гашиш).

## 2.4 Зомбирование

Под термином "зомбирование" подразумевается форсированная обработка подсознания человека, благодаря которой он теряет направляющий контакт со своим прошлым и программируется на безоговорочное, притом неосознаваемое подчинение приказам своего хозяина. Известны "жесткое" и "мягкое" психопрограммирование. Причем "жесткого" зомби нередко удается определить по "экстерьеру" и манере поведения (отрешенность на лице, не соответствующая выражаемым в словах эмоциям, необычность цвета белков глаз, вялые интонации голоса, неправильная речь, отсутствие способности сосредоточиться, замедленность реакций и провалы в памяти, нелепая стереотипность поведения). Тогда как "мягкий" зомби по существу ничем не отличается от всех других людей. Профессиональное зомбирование по "мягкой" категории чрезвычайно сложно и требует досконального изучения психофизиологии объекта, использования специальной медицинской и компьютерной аппаратуры, привлечения кодировщиков-гипнотизеров, виртуозно владеющих техникой многоступенчатого гипноза. Для ориентирующего ознакомления приведем типичный прием зомбирования:

* персону изымают из ее прежней среды, контакты с которой полностью прерываются;
* режим дня должен целиком противоречить ее прежним привычкам;
* активно провоцируется недоверие ко всем, кто жертву окружает (ее нагло обманывают, на нее подло доносят, ей злобно угрожают...);
* осуществляются непрерываемые акции дискредитации (подтасовка, высмеивание) всего, чем человек дорожит;
* диета преимущественно углеводная и безбелковая, с подмешиванием отупляющих сознание препаратов (аминазин) и обязательным недосыпанием;
* по достижении состояния тупого безразличия, проводится необходимое кодирование приемами активного внушения или гипноза. [3]

Данная методика широко применяется в тоталитарных сектах для подавления воли своих последователей (Аум Синрикё, Белое Братство и др.).

## 2.5 Нейро - лингвистическое программирование

Нейро - лингвистическое программирование (НЛП) - созданная в 1975 году в США группой психологов (Дж. Гриндер, Р. Бэндлер, Р. Дилтс и др) - методологическая концепция скрытого влияния на человеческое мышление. Первоначально НЛП базировалась на шаблонах эффективной психотерапии (в основном, гипноза), в связи с этим до сего дня среди специалистов по НЛП преобладают психотерапевты. Современное НЛП ориентированно на поиск достаточно общих последовательностей мыслительных процессов у разных людей в ходе принятия решений (такие последовательности именуются в НЛП "стратегиями"). Упомянутые последовательности сравнительно легко могут быть навязаны индивидуальному и массовому сознанию, побуждая отдельных индивидов и большие группы людей к запрограммированным реакциям. При этом навязывание определенных реакций является неочевидным, скрытым. Его можно сравнить с такими неосознаваемыми большинством людей понятиями - поведенческими стимулами, как предрассудок, "сложившееся мнение", импульсивные действия и решения, эмоциональный ответ на определенные слова.

Впервые широкомасштабно НЛП было опробовано в президентской предвыборной кампании Р. Рейгана, затем - в первой президентской предвыборной кампании Б. Ельцина. В настоящее время НЛП является основным способом оформления сюжетов политической и торговой рекламы, поэтому для противодействия такой рекламе также требуются навыки НЛП. Так, лозунг "Ельцин - Президент всех россиян" хрестоматийно соответствует тому, что в НЛП называется "гипнотическим трюизмом"; а лозунги избирательной кампании "Голосуй - или проиграешь" и "Голосуй - и победишь" в терминах НЛП соответствуют использованию мета-стратегий "избегание неприятного - поиск приятного". При внешней простоте они затрагивают весьма глубокие структуры человеческого мышления. [7]

Важным достоинством нейро - лингвистического программирования является его скрытность. Человек считает, что авторство идей и решений принадлежит ему самому.

Для того чтобы в процессе беседы незаметно влиять на человека, необходимо сначала подстроиться под него. Вы должны говорить с такой же интонацией, с той же громкостью, с тем же темпом, что и ваш партнер. Желательно, также и повторение его мимики, жестов и позы. Люди крайне редко обращают внимание на такую "подстройку". Наоборот, сразу же бросается в глаза и вызывает у нас неудовольствие, если чье-то поведение отличается от нашего.

Для проведения нужной мысли или идеи необходимо захватить внимание партнера, живописуя с помощью его модальных слов все то, что он действительно переживает в сей момент. Затем, через переходные слова (“если”, “таким образом”, “следовательно”), подсовывают (используя исходную модальность) навязываемые представления, которые в таких условиях покажутся ему “своими” и вполне убедительными, хотя могут быть совсем не однотипными с идущими вначале утверждениями.

Классическая схема исподвольного внедрения в сознание и подсознание человека выглядит при этом так: подстроечные предложения - переходное слово - фраза ведущая в намеченном направлении.

Высказывания строятся с использованием внутренней стратегии партнера (определяемой по выявленным предварительно движениям его глаз) с употреблением тех же слов и в той же фразовой последовательности, как это делает он.

В ходе осуществления воздействия внимательно следят за каждой возникающей реакцией объекта на все произносимые слова, и корректируют свой образ действий до тех пор, пока в сознании визави не сформируется вполне устраивающий вас отклик.

# 3. Возможные объекты нападения

## 3.1 Гражданский сектор

Гражданский сектор чаще всего подвергается нападению. Можно даже сказать, что на него постоянно оказывают влияние средства массовой информации, телевизионные и радиопрограммы и т.п. «агрессоры», которые пытаются склонить к тому или иному мнению, изменить его настроение и пр. Такой вид нападения носит массовый характер и в основном не наносит особого физического или морального вреда человеку.

#

### 3.1.1 Информационная война

Другой вид «глобального» воздействия – информационная война. Информационное оружие принципиально отличается от всех других средств ведения войны тем, что с его помощью могут вестись (и давно ведутся) необъявленные и чаще всего невидимые миру войны и что объектами воздействия этого оружия являются, прежде всего, гражданские институты общества и государства - экономические, политические, социальные и т. д. Кроме того, впервые военная стратегия использования информационного оружия оказалась тесно связанной с гражданским сектором и стала во многом от него зависеть. Разнообразие информационного оружия, форм и способов его воздействия, особенности появления и применения породили сложнейшие задачи защиты от него гражданского общества.

Информационное оружие призвано обеспечить разрешение военных конфликтов на ранней стадии и исключить применение сил общего назначения. Стратегия применения информационного оружия носит исключительно наступательный характер. Однако есть понимание собственной уязвимости, особенно гражданского сектора, поэтому проблемы защиты от информационного оружия и информационного терроризма сегодня выходят на первый план. В условиях бурного развития международных открытых сетей типа Internet и присоединения к ним большинства стран кардинально меняется идеология ведения разведки, в которой основной акцент теперь делается на использовании новейших информационных технологий для добывания конфиденциальной информации.

#

### 3.1.2 Защита от информации

Учитывая вышеперечисленные факты, обозначилась проблема защиты личности от информации. Рассмотрим информационные способы воздействия на объект, непосредственно касающиеся понятия защиты от информации. К ним относятся:

* манипулирование информацией (искажение, уничтожение дезинформация и т.д.);
* использование средств массовой информации с позиций, противоречащих положению и интересам граждан.

Проблемы разработки, использования и защиты от информационного оружия уже сегодня стали высшими приоритетами в политике национальной безопасности западных стран, ориентированной на XXI век. Защита гражданского сектора должна осуществляться государством – это его прямая обязанность, даже если это не в его интересах.

Но человек в гражданском обществе должен полагаться в первую очередь не на государство, а сам должен «фильтровать» информацию. Общественная информационная безопасность порождается состоявшейся личностной информационной безопасностью множества людей. Человек должен уметь различать в каких случаях он отстранёно или предостерегающе созерцает негативный прогноз, а в каких случаях деятельно, возможно бездумно программирует бедственное дальнейшее течение событий.

### 3.2.1Способы самоуправления

В основе общественной в целом информационной безопасности лежит способность множества индивидов обеспечить свою собственную личностную информационную безопасность.

Исторически, реально существует концепция общественного устройства жизни, в которой люди с «демоническими» наклонностями норовят поставить себе на службу возможности окружающих их людей всеми доступными им средствами воздействия (в том числе и морально - психологическими). При этом они действуют предумышленно, или на основе бездумно воспринятых «автоматизмов поведения».

Стремление эксплуатировать других людей исторически массовое явление.

Многие процессы информационного обмена хорошо известные из кибернетики; теории и практики построения технических систем находят свои аналоги как при общении людей друг с другом, так и в процессе воздействия на каждого из них науки, техники, СМИ и других достижений культуры, понимаемой в качестве информации и не передаваемые генетически от поколения к поколению.

Психика любого человека является самоуправляющейся системой в объемлющих её подсистемах. В связи с этим мы имеем возможность организовать в ней выработку управленческих решений и алгоритмов поведения в среде несколькими способами.

*Первый способ*: Информация, поступающая из внешней среды, обладает наивысшим приоритетом и непосредственно подаётся на вход алгоритма выработки управленческого решения и поведения.

*Второй способ*: Информация, поступающая из внешней среды, загружается непосредственно в долговременную память, а алгоритм выработки управленческого решения черпает информацию из этой памяти, сравнивая с ней информационный поток, поступающий из внешней среды.

*Третий способ*: Информация, поступающая из внешней среды, загружается в «буферную» память временного хранения. Некий алгоритм, выполняя в данном варианте роль сторожа, анализирует информацию в буферной памяти, присваивая ей значения «*ложь*» - «*истина*» – «*требует дополнительной проверки*». Только после этого определения алгоритм – сторож перегружает информацию в долговременную память, информационная база которой обладает более высоким приоритетом для алгоритма выработки управленческого решения, по сравнению с информацией, поступившей в него непосредственно из внешней среды.

При прочих равных условиях, время реакции системы на поступление информации из внешней среды растёт от первого к третьему, т.е. быстродействие, оцениваемое по времени реакции системы на воздействие, падает. Однако, если в информационном потоке, поступающем в систему из внешней среды, присутствует помеха типа «бессмысленный шум», или типа «наваждение», то устойчивость процесса самоуправления растёт от первого к третьему. Это объясняется тем, что растёт помехозащищённость выработки управляющего воздействия, которое строится на основе стабильной или медленно изменяющейся информационной базы долговременной памяти в целом.

Названные помехи выражают целенаправленную попытку из вне изменить самоуправление нашей системы в соответствии с чуждой нам концепцией.

В первом способе выработки управленческого решения «шумонаваждение» является непосредственной базой выработки этого решения.

Во втором способе «шумонаваждение» включается в информационную базу выработки управленческого решения, по мере того, как им замусоривается долговременная память. Затем оно вовлекается в алгоритм выработки управленческого решения в качестве достоверной информации.

В третьем способе «шумонаваждение» прежде чем войти в информационную базу, на основе которой строится управленческое решение и поведение системы, должны обмануть алгоритм – сторож. Алгоритм – сторож перегружает информацию из буферной памяти временного хранения в долговременную память. Это происходит после определения принадлежности информации к взаимно не пересекаемым категориям: «ложно», «истинно», «требует дополнительной проверки».

С точки зрения обеспечения информационной безопасности в смысле устойчивости самоуправления по определённой концепции в которой определены цели управления и средства их достижения нормальным является третий способ.

Первый способ управления допустим в чрезвычайных ситуациях, в которых предпочтительней хоть какое-то управление, чем отказ от управленческого воздействия на течение событий. Второй способ – это ущербный третий.

Человеческая психика, если это психика нормального человека, генетически настроена на осуществление третьего способа самоуправления, однако, по причине извращения нормальной генетической обусловленности исторически реальной культурой, в организации психики большинства людей в обыденной повседневности осуществляется первый способ управления.

Комбинация второго и третьего способов управления характеризуется вне чрезвычайных обстоятельств, но не в обыденной повседневности, а когда от человека требуется некоторое творчество.

Суета и истерика - нецелесообразные и не имеющие смысла - в человеческом поведении в чрезвычайных обстоятельствах являются выражением преобладания первого способа управления. Оцепенение и шок в чрезвычайных обстоятельствах – есть торможение управления по первой схеме при возможности осуществить вторую или третью схемы.

В психике человека есть собственный алгоритм – сторож, есть внешние по отношению к ней сторожа, начиная от тех, кто защищает своей любовью и кончая Высшим Разумом, если идти по порядку расширения сфер заботы.

Одна из задач «демонизма», решение которой необходимо ему для эксплуатации возможностей других индивидов – это выведение психики личности из-под защиты всей совокупности «сторожей». Такое выведение тем более эффективно, чем в большей степени *поражены ложью методологические стереотипы личности*, лежащие в основе её собственных алгоритмов – сторожей и определяющих взаимодействие с внешними сторожами.

Именно поэтому личностная безопасность обеспечивается тем в большей степени, чем устойчивее психика человека в третьем способе выработки управленческих решений и чем более истинны воззрения человека, относящиеся к методологическому приоритету обобщённых средств управления.

# 4. Организационные, технические и правовые методы обеспечения морально – психологической информационной безопасности

Организационные методы и средства морально – психологической информационной безопасности можно разбить на две условные категории:

* Осуществляющие контроль над используемой на объекте информацией, сведениями, сообщениями.
* Осуществляющие контроль внешнего информационного поля и предупреждение нежелательных последствий со стороны каких-либо внешних информационных структур общества.

Необходимо заметить, что системы первого типа должны контролировать также и входящую и выходящую корреспонденцию.

Средства первого типа необходимы в первую очередь информационно-аналитическим системам (ИАС), осуществляющим управление за счет сбора и анализа информации (как внешней, так и внутренней). В данном случае необходимо уже в процессе разработки ИАС предусматривать защиту от применения целенаправленных воздействий на информацию и принимаемых на ее основе решений. Специфика функционирования ИАС такова, что к таким угрозам прежде всего должны быть отнесены возможность воздействия на интерпретацию информации и ее фальсификацию в системе управления. В целях нейтрализации угроз информационной безопасности поставлена задача создания информационно-телекоммуникационной системы специального назначения, которая также обеспечивает предупреждение информационного воздействия органов управления.

Для эффективного решения системы поставленных задач предлагается следующее:

а) создание системы независимых и несвязанных между собой источников информации с заданной для каждого источника функцией достоверности, отражающей вероятность истинности информации в различных разделах. Причем для успешного анализа необходимо также иметь источники с наихудшей функцией достоверности, а также заведомо дезинформирующие источники;

б) создание контролирующих источники структур, собирающих информацию о самих источниках, а также отслеживающих действия противников (конкурентов) в отношении источников и в общем плане;

в) создание сети изолированных друг от друга аналитических центров, осуществляющих анализ и обработку получаемой от источников (п.1, п.2) информации, с целью последующего составления отчетов. На основе сопоставления извлекается наиболее достоверная информация, на основе которой могут приниматься какие-либо решения;

г) желательно (а в некоторых случаях обязательно), чтобы все перечисленное в пунктах а), б), в) осуществлялось раздельно и не было совмещенных структур, а передача информации осуществлялась лицами, не связанными ни с одной из структур пунктах а), б), в). Такое повсеместное разделение предотвратит возможные угрозы от внутренних источников.

Приведенные выше положения должны с высокой степенью достоверности обеспечить правдоподобность информации и защищенность ИАС от искажения и ложной информации.

Рассмотрим аспекты защиты, связанные с понятием «*вредная информация*» как фактора поражающего действия информационных систем (в том числе и систем защиты от информации). К данной категории можно отнести различного рода компьютерные вирусы, программы-закладки, а также любые программы, нарушающие нормальное функционирования информационной (в конкретном случае) системы. Для предупреждения такого вида угроз следует воспользоваться методами защиты от *не санкционированного доступа* и вредоносного программного обеспечения, а также создавать собственный (или воспользоваться государственным) сертификационный центр, занимающийся тестированием аппаратно-программных средств на предмет обнаружения закладок.

Не менее действенными методами информационной защиты являются правовые аспекты информационной безопасности.

Непосредственное отношение к проблеме имеют законодательные акты, связанные с созданием и распространением вредоносного програмного обеспечения манипулированием информацией, хищением и нарушением информации и технологии обработки, прав на частную собственность и свободу слова.

В совокупности, перечисленные выше методы первого типа (организационные, технические и правовые) должны обеспечить приемлемый уровень контроля защиты ИАС.

Совокупность средств, используемых для контроля за внешним информационным полем пока практически не определена, но, тем не менее, можно выделить в основную группу правовые методы.

Появление средств воздействия на общественное сознание через глобальные информационные системы государственного и военного управления путем дистанционного и скрытного нарушения функционирования телекоммуникационных и информационных сетей выдвигает на первый план проблемы развития международных нормативно-правовых основ формирования глобального информационного пространства, предотвращающего применение информационного оружия.

Нельзя забывать о том, что даже наличие международных договоров и соглашений о запрещении деструктивного воздействия на информационные системы, соответствующих нормативно-правовых актов федерального и регионального уровней не снижает остроты проблем разработки средств и методов информационной инфраструктуры и обеспечения информационной безопасности. В настоящее время имеет силу федеральный закон «О средствах массовой информации» (приложение А). Закон ограничивает распространение эротических программ, регулирует осуществление благотворительной и особенности рекламной деятельности в СМИ.

Законопроект вменяет в обязанность СМИ не разглашать данные предварительного следствия, не распространять информацию, нарушающую презумпцию невиновности, не разглашать информацию о частной жизни лица, его персональных данных без его согласия.

Необходимо также наличие юридической и уголовной ответственности за объявление и распространение ложной информации.[5]

# Заключение

Обеспечение безопасности – как личности, так и общества в целом при достаточно глубокой проработке, выявляет необходимость комплексного подхода к решению проблемы. Понятие комплексного подхода подразумевает глубокую проработку всех смежных аспектов проблемы. В данной курсовой работе была поверхностно рассмотрена только одна сторона проблемы «Гражданского общества и информационного оружия»: влияние морально – психологических средств и методов, как видов информационного оружия, на личность и гражданское общество в целом.

Воздействовать на ум и поведение человека можно различными путями, одни из которых требуют лишь специфичной подготовленности специалиста, а другие - еще и специальной аппаратуры. Методы прицельного влияния могут быть щадящими и изощренными, трудноуловимыми и дополняющими.

Нападение может быть совершено на любого человека, или даже на общество в целом. Результат же (удалась, или нет попытка нападения) будет зависеть конкретно от личностных качеств подвергшегося нападению и от его осознания самой попытки нападения, но, как правило, человек зачастую не подозревает о происходящих в его сознании изменениях. Но немаловажным является и тот факт, помогает ли кто-нибудь человеку в борьбе с атакой на его психику, защищают ли его от подобных нападений.

И поэтому овладеть навыками психологической защиты может только человек, знакомый с техникой атаки. Первоочередная задача в этом направлении – подготовка людей в области морально – психологической защиты.

# Список использованных источников

1. Терминология в области защиты информации. Справочник. – М.: ВНИИстандарт, 1993.

2. Данченко В. Принципы современной психической самозащиты. Электронный вариант.

3. Пимкин Д.Е. Морально-психологические средства и методы обеспечения информационной безопасности. Журнал "БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ" 1998г. 1/3

4. Левин А.А. Секрет фирмы. – М.: Сириус, 1992.

5. Ивонин М. В. Средства и методы защиты от информации. Журнал "БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ" 1998г. 1/3

6. Кулагин Ю. В. Доклад на 2-й Северо-Западной международной конференции "Бизнес и безопасность", 22 октября, Санкт-Петербург.

7. Алдер Х. НЛП: современные психотехнологии. – СПб.: Издательство "Питер", 2000.-160 с.

# Приложение А

(справочное)

Выдержка из закона РФ от 27 декабря 1991 г. № 2124-1"О средствах массовой информации" (с изменениями от 13 января, 6 июня, 19 июля, 27 декабря 1995 г., 2 марта 1998 г.)

Федеральным законом от 19 июля 1995 г. N 114-ФЗ в статью 4 настоящего Закона были внесены изменения:

Статья 4. Недопустимость злоупотребления свободой массовой информации

Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для призыва к захвату власти, насильственному изменению конституционного строя и целостности государства, разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, для пропаганды войны, а также для распространения передач, пропагандирующих порнографию, культ насилия и жестокости.

Запрещается использование в теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок, воздействующих на подсознание людей и (или) оказывающих вредное влияние на их здоровье.