**Программно-математическое информационное оружие**

**СОДЕРЖАНИЕ**

1. ОБЩАЯ ХАРАКТЕРИСИКА РАБОТЫ

2. ОСНОВНОЕ СОДЕРЖАНИЕ

2.1 Введение

2.2 Определение, понятие и классификация

2.3 Объекты воздействия и поражающие факторы

2.4 Меры противодействия ПМИО

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. **ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ**

АКТУАЛЬНОСТЬ ТЕМЫ

Информация всегда играла важную роль в мире. А в наше время она стала неотъемлемой частью нашей жизни.

Современные технические средства ускорили процесс добывания, обработки и доставки информации, процесс ее обновления. Она стала оперативной, глобальной и разноплановой. Информация стала средством воздействия на мысли, поступки, поведение, принимаемые решения, на образ жизни и мировоззрение отдельного человека, коллективов, наций и народов. Выразительность показа, богатая цветовая гамма, высокое качество звучания, искусство монтажа и освещения событий резко повысили эффективность воздействия на человека, позволили формировать вектор такого воздействия в требуемом направлении. Таким образом, вмешиваясь в регулирование информационных потоков, в процесс их обработки и управления, можно влиять на те или иные события. При этом необходимо подчеркнуть глобальность информационных воздействий в различных сферах деятельности. Это касается не только известных технических приемов воздействий на компьютерные сети, каналы получения и обработки информации, на центры управления и наведения, глобальные военно-космические информационные системы, но и разрабатываемых методов информационных воздействий на человека и общество, в целом на информационную сферу государства.

Темпы развития информационной техники и технологии, масштабы ее внедрения являются беспрецедентными для мировой истории. Таким образом, информатизация (компьютеризация, электронизация) становится одним из важнейших факторов общественного развития, едва ли не решающим участником исторического соперничества на мировой арене.[1]

ЦЕЛЬ РАБОТЫ

Целью данной работы является рассмотрение роли ПМИО в современном мире.

**ЗАДАЧИ РАБОТЫ**

Для достижения поставленной цели необходимо рассмотреть следующие задачи:

1. Понятие ПМИО
2. Объекты воздействия данного вида оружия и его поражающие факторы
3. Меры противодействия
4. **ОСНОВНОЕ СОДЕРЖАНИЕ**
   1. **ВВЕДЕНИЕ**

Информационным оружием называют способы и средства уничтожения, искажения или похищения информационных массивов, преодоления систем защиты информации, ограничения или запрета доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всей инфраструктуры высокотехнологического обеспечения жизни общества и функционирования системы управления государством.

Определение «информационное оружие» включает технические и программные средства, обеспечивающие несанкционированный доступ к базам данных, нарушение штатного режима функционирования технических средств и программного обеспечения, а также вывод из строя ключевых элементов информационной инфраструктуры отдельного государства или группы государств.

Правомерность использования термина «информационное оружие» обусловлена тем, что в контексте использования информации как основы вида оружия она может характеризоваться следующими показателями: целенаправленность, избирательность, рассредоточенность, масштабность воздействия, досягаемость, скорость доставки, комплексность влияния на технические способы, системы и на личный состав, возможность регулирования «мощности» воздействия.

Информационному оружию присущи атакующий характер, универсальность, скрытность, многовариантность форм реализации (в т.ч. программно-аппаратной и технической), радикальность влияния, широкие возможности в выборе времени и места применения, наконец, экономичность, что делает его чрезвычайно привлекательным для атакующей стороны и чрезвычайно опасным для подвергшегося информационному воздействию.

Самая большая опасность этого вида оружия - обезличенный характер его применения, что позволяет вести наступательные действия анонимно, даже без объявления войны. К тому же, запретить разработку и использование информационного оружия (как это сделано, например, в отношении химического или бактериологического) едва ли возможно, как и ограничить усилия многих стран по формированию единого глобального информационного пространства. Все это и объясняет повышенное внимание к информационному оружию и перспективам его дальнейшего развития.[2]

Представляется логичным провести классификацию информационного оружия (ИО) в соответствие с видами информационной борьбы (войны) и подразделить его на два основных вида: *информационно-техническое и информационно-психологическое*. В этом случае главными объектами нападения информационного оружия первого вида является *техника*, второго *люди*.

Необходимо заметить, что термин «информационное оружие » получил широкое распространение после завершения военной операции Международных сил (МНС) против Ирака в 1991 г. Военные специалисты тогда посчитали, что решающий вклад в победу Международных сил над вооруженными силами Ирака внесло комплексное применение средств разведки, управления, связи, навигации и РЭБ. Совокупность этих средств и было определено как информационное оружие, названное потом информационным оружием театра военных действий (ИО ТВД).

Возросшее значение информации в жизни современного общества позволило в начале 80-х годов выделить в совокупном потенциале государства ресурсы особого рода — *информационные (ИР)*, в которые включается прежде всего информация на материальных носителях или существующая в любой другой форме. Особое значение ИР обусловлено не только их качественными показателями, сколько тем ключевым положением, которое они в силу особой роли информации как системообразующего фактора занимают по отношению к любым другим ресурсам государства — экономическому, научно-техническому и военному. Широкое вовлечение ИР в сферу экономического и военного противоборства различных государств способствует ускоренному развитию экономической, научно-технической и собственно военной составляющих военных потенциалов государств. Материальными носителями информации в современном мире являются центры обработки и анализа информации, каналы информационного обмена, линии связи, системы и средства защиты информации, составляющие в совокупности *информационную инфраструктуру государства*. Именно на нее направлено острие информационно-технических средств воздействия, являющихся собственно *программно-математическим (интеллектуально- техническим) оружием*. [4]

**2.2 ОПРЕДЕЛЕНИЕ, ПОНЯТИЕ КЛАССФИКАЦИЯ**

ИНФОРМАЦИОННОЕ ПРОГРАММНО-МАТЕМАТИЧЕСКОЕ ОРУЖИЕ (ИПМО) — это совокупность способов и средств, позволяющая целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование носителей информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, применяемая в ходе информационной борьбы (войны) для достижения поставленных целей.

Это оружие включает:

* средства разрушения (подавления) информационного обмена в телекоммуникационных сетях, его фальсификации, передачи по каналам государственного и военного управления нужной (для воздействующей стороны) информации;
* средства воздействия на каналы обмена информацией путем создания помех, искажения содержания информации, введения ложных сведений, дезинформации;
* программные закладки («троянская программа», «логическая бомба», «логический люк», «программная ловушка», «программный червь»), заранее внедряемые в информационно-управляющие центры, компьютерные сети, программно-технические средства, которые самостоятельно (в установленное время) или по специальному сигналу приводятся в действие, уничтожая (искажая) информацию или дезорганизуя их работу. Специальные программы (например, «троянский конь») позволяет осуществить скрытый доступ к информационному массиву противника с целью получения разведывательной информации;
* компьютерные вирусы, способные разрушать, искажать программное обеспечение и информацию в компьютерных сетях, электронных телефонных станциях, системах управления и связи;
* нейтрализаторы тестовых программ, обеспечивающие невозможность выявления недостатков программных средств или наличие в них вирусов с помощью специальных тестовых программ;
* способы и средства, позволяющие внедрять «логические бомбы» и вирусы в информационные сети противника.[4]

## Программно-математическое оружие делиться на два типа:

## Средства воздействия на программный продукт;

* Средства воздействия на канал передачи информации.

Особенностями данного типа оружия являются следующие факторы:

* Универсальность;
* Скрытность;
* Экономическая эффективность;
* Масштабность применения;
* Сложность международного контроля;
* Эффект «Цепной реакции»;
* Психологическое воздействие.

Способы и средства воздействия:

* Средства разрушения;
* Программные закладки;
* Средства воздействия на каналы распространения информации;
* Компьютерные вирусы;
* Нейтрализаторы тестовых программ;
* Средства внедрения постороннего кода.[5]
  1. **ОБЪЕКТЫ ВОЗДЕЙСТВИЯ И ПОРАЖАЮЩИЕ ФАКТОРЫ**

В современных войнах объектами информационного влияния станут сознание и психика человека, системы управления и другие информационно-технические системы, средства боевого поражения.

В развитии систем вооружений сейчас прослеживается устойчивая тенденция увеличения в них удельного веса информационного оружия. Подобная «информационная эволюция» происходит в несколько этапов.

1-й этап связан с применением информоружия для противодействия средствам поражения. Здесь следует выделить средства радиоэлектронного противодействия (РЭП), которые не являются оружием, разрушающим объекты, но их применение предшествует в современной войне началу боевых операций, «расчищает» дорогу для беспрепятственного применения боевых систем высокоточного оружия.

РЭП призвано блокировать или усложнять функционирование электронных средств неприятеля способом излучения, отражения электромагнитных, акустических и инфракрасных сигналов. РЭП осуществляется автоматическими наземными, корабельными и авиационными системами постановки помех. За несколько суток до начала операции «Буря в пустыне» США впервые в широких масштабах провели радиоэлектронное подавление активных средств ПВО, органов управления и иных важных объектов на территории Ирака. Как отмечали западные эксперты, это был «шторм в эфире» - американцы нанесли такой мощный радиоэлектронный удар по Ираку, что заглушили даже некоторые радионаправления на территории южных военных округов Советского Союза.

Особенность 2-го этапа эволюции в том, что основным объектом информвлияния становятся системы управления и связи, информационные и компьютерные сети. Для вывода из строя таких систем и объектов разработано специальное информационное оружие, к которому относятся средства программно-математического влияния, такие, как компьютерные вирусы, логические бомбы, «троянские кони», нейтрализаторы тестовых программ, и электромагнитное оружие.

**Компьютерный вирус (Software Virus, КВ)** - специальная программа, которая внедряется в «чужую» электронную среду. КВ может передаваться по линиям связи и сетям обмена информацией, проникать в электронные телефонные станции и системы управления. В заданное время (или по сигналу) КВ уничтожает информацию, хранящуюся в памяти ЭВМ, может деформировать ее произвольным образом или целенаправленно.

**Логическая бомба (Logic Bomb, ЛБ)** - так называемая «программная закладка», которая заранее вносится в информсистемы и сети, обеспечивающие управление объектами военной и гражданской инфраструктуры. ЛБ по сигналу (или в установленное время) приводится в действие, стирая или искажая информацию в компьютере.

**«Троянский конь» (The Trojan Horse, разновидность ЛБ)** - программа, позволяющая осуществлять скрытый, несанкционированный доступ к информресурсам неприятеля с целью добывания разведывательных данных.

**Нейтрализаторы тестовых программ (Testing Software Neutralizer)** делают невозможным выявление случайных и специально созданных недостатков программного обеспечения. Кроме того, существуют разнообразные отклонения и дефекты, которые сознательно вносятся в программное обеспечение изготовителями программных продуктов.

К средствам программно-математического влияния относятся также **средства подавления информобмена в телекоммуникационных сетях**, фальсификация информации в каналах государственного и военного управления, а также различного рода ошибки, сознательно внесенные программистами или лазутчиками в программное обеспечение **(Software Holes)**.

Разработка **электромагнитного оружия** началась в 80-х годах в рамках реализации программы «Звездные войны», завершившейся созданием пушки, позволяющей осуществлять направленный выброс высокоэнергетического пучка в радиочастотном диапазоне. Одно из его основных преимуществ - относительная дешевизна.

Применение вышеупомянутых средств программно-математического влияния способно парализовать функционирование государственной власти в стране и подавить всю систему управления вооруженными силами. Поэтому современная война начинается именно с массированного применения информоружия в таких формах, как радиоэлектронная борьба, радиоразведка, дезорганизация систем управления войсками и оружием, специальное программно-математическое влияние, направленное против существующих информсистем. Комплекс таких действий призван парализовать противника, что позволит свести к минимуму потери при проведении наземных операций.

Но самому большому информвоздействию как сегодня, так и в будущих войнах подвергается человек - как ключевой компонент любых вооруженных сил. Концентрация усилий вокруг наращивания информвлияния на человека и является характерным признаком 3-го этапа развития систем информоружия. К таким системам следует отнести прежде всего психотропное оружие, средства зомбирования человека и средства психологической войны. Эти системы влияют на сознание и психику людей, что дает возможность руководить их поведением.

Цель психологической войны - разрушить или изменить в массовом сознании другой нации ее собственное видение своих роли и места в мировых процессах, а также разрушить или изменить представления об этом у остального мира.

Объектом воздействия становятся как широкие слои населения, так и политико-экономическая элита государства. Здесь могут использоваться дипломатические методы, пропагандистские и психологические кампании, деятельность местных СМИ, проникновение в компьютерные сети и базы данных и пр. Здесь сходятся в одной точке экономическая, политическая и социальная формы ведения войны.

Среди основных средств влияния на человека следует отметить, в частности, психотропное оружия (пси-оружие). Его действие основано на использовании дистанционного влияния пси-одаренного оператора (экстрасенса) на другого человека с целью корректировки поведения или влияния на физиологические функции. Существует также возможность создания соответствующих технических устройств, например различного рода боевых психотропных устройств (генераторов).

В узком значении под психотропным оружием следует понимать использование в военных целях потенциала пси-феноменов - экстрасенсорной перцепции (телепатии, ясновидения, предвидения) и психокинеза в природном или техническом «исполнении».

Практика показывает, что процесс экстрасенсорного влияния значительно облегчается при использовании какой-либо «опорной» системы коммуникации: телефонной связи, радиотрансляционной сети или системы телевещания. Теле- да и любые массовые сеансы экстрасенсорного влияния иллюстрируют реальную возможность влиять на личность, в том числе опираясь на существующие технические способы связи или передачи информации.

информационный оружие программный

Акустическое оружие - это излучение энергии определенной частоты, позволяющее наносить поражение живой силе и радиоэлектронным средствам противника.

Боевые генераторы могут устанавливаться на морских, воздушных и космических носителях. Излучение энергии непосредственно на объект поражения или создание соответствующего фона способно превратить дивизию противника в стадо испуганных идиотов. Люди будут ощущать беспричинный страх, сильную головную боль, их действия станут непредсказуемыми, возможно полное необратимое разрушение психики.

Акустическое оружие активно разрабатывается и уже существует в лабораторных вариантах. Оно может быть принято на вооружение в некоторых странах в течение 10-15 лет.

Уже достаточно известен и так называемый «вирус №666», пагубно влияющий на «психофизиологическое состояние» оператора ЭВМ. Этот «вирус-убийца» выдает на экран особую цветовую комбинацию, приводящую человека в состояние гипнотического транса, и вызывает подсознательное его восприятие, резко меняющее функционирование сердечно-сосудистой системы вплоть до блокирования сосудов головного мозга.[2]

**2.4** **МЕРЫ ПРОТИВОДЕЙСТВИЯ**

## Для защиты информации от ПМИО используют такие средства защиты как: программные, аппаратные и технические. Рассмотрим каждое из данных средств подробнее.

## Программные средства защиты информации

* Встроенные средства защиты информации
* Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых решений следует отметить следующие две системы, позволяющие ограничить и контролировать информационные потоки.
* Межсетевые экраны (также называемые брандмауэрами или файрволами — от нем. *Brandmauer*, англ. *firewall* — «противопожарная стена»). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.
* Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript).
* VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

## Аппаратные средства защиты информации

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

* специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
* устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
* схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
* устройства для шифрования информации (криптографические методы).

## Технические средства защиты информации

Для защиты периметра информационной системы создаются:

• системы охранной и пожарной сигнализации;

• системы цифрового видео наблюдения;

• системы контроля и управления доступом (СКУД).

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями:

• использованием экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;

• установкой на линиях связи высокочастотных фильтров;

• построение экранированных помещений («капсул»);

• использование экранированного оборудования;

• установка активных систем зашумления;

• создание контролируемых зон.

**ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ**

В данном реферате была рассмотрена тема «Программно-математического информационного оружия». Так же были выявлены основные направления, по которым применяется данный вид оружия, указаны типы, особенности, средства и способы воздействия ПМИО.

**СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1. Н.А. Костин «Общая математическая модель защиты информации»

2. Перепелица Г. «ИНФОРМАЦИОННЫЕ ВОЙНЫ»

3. http://flot.com/publications/books/shelf/safety/18.htm

4. http://ru.wikibooks.org/wiki/Контроль\_Разума

5. http://08.at.ua/publ/4-1-0-28