Государственное бюджетное профессиональное образовательное учреждение

Новосибирской области

«Новосибирский химико-технологический колледж им. Д.И. Менделеева»

(ГБПОУ НСО «Новосибирский химико-технологический колледж им. Д.И. Менделеева»)

Специальность: Информационные системы и программирование

**РЕФЕРАТ**

**На тему:** «Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.»

Дисциплина: Информатика

Направление подготовки 09.07.19 Информационные системы и программирование

Профиль «Информационные системы и программирование»

Работу проверил(а): Голубь Е.Ф.  
Работу выполнил(а) студент 1 курса группы 09.07.32:

Мироненко Данил Андреевич

Новосибирск 2022

Оглавление

[Введение 3](#_Toc118706451)

[Понятие «Информационная война» 4](#_Toc118706452)

[Цели, методы и основные составляющие информационной войны 7](#_Toc118706453)

[Основная часть 12](#_Toc118706454)

[заключение 13](#_Toc118706455)

# Введение

Для большинства современных государств открытые военные конфликты стали бессмысленными, что отражает статистика. Согласно выкладкам канадского учёного Стивена Пинкера, от войн между племенами в древности погибало в 9 раз больше людей, чем от войн в XX веке, а в Средневековье жертвами насилия становились в 30 раз больше человек, чем в последние годы. По оценке ООН, сейчас в активной стадии находятся 11 крупных конфликтов (с более чем 1 тыс. погибших за год). Это не так много, если сравнивать с предыдущими эпохами. Другое дело, что участились так называемые информационные войны.

День сегодняшний, с его телекоммуникационными вычислительными системами, психотехнологиями кардинально изменил окружающее пространство. Отдельные информационные ручейки превратились в сплошной поток. Если ранее было возможно “запрудить” конкретные информационные каналы, то сегодня все окружающее пространство информационно коллапсировалось. Время на информационное взаимодействие между самыми отдаленными точками приблизилось к нулю. В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность - защиту от информации.

## ****Понятие «Информационная война»****

**Информационная война** – это разновидность боевых действий, в которых ключевым объектом воздействия является информация, хранящаяся или циркулирующая в управляющих, разведывательных, боевых и прочих системах противника. Концепция современной информационной войны разработана сравнительно недавно. По мнению американских специалистов, само понятие информационной войны стало возможным в результате «кибернетической революции», которая повлекла массовое внедрение во все сферы жизни различных информационных систем, основанных на применении электронных устройств.

В настоящее время в теории политологии еще не выработано единое универсальное понятие информационной войны.

Американский военный аналитик Ричард Шафрански рассматривает информационную войну в контексте вооруженного столкновения («warfare») как вооруженные действия, направленные против любой части системы знаний или предположений врага. «Противник» — это любой, чьи действия противоречат целям лидера. Вне государства это может быть «образ врага» или «не мы». Внутри врагом может быть предатель или путешественник, любой, кто противостоит или недостаточно поддерживает лидера, который управляет средствами информационной войны. Если члены группы не поддерживают цели лидера в ходе боевых действий, внутренняя информационная война (включая такие вещи, как пропаганда, ложь, террористические акты и слухи) могут быть использованы в попытке заставить их быть более лояльными к целям лидеров.

Китайский военный аналитик Ван Пуфэн , широко известный как основатель китайской информационной войны, дает ее всеобъемлющее рабочее определение. Информационная война является продуктом эпохи информации, который в сражении в большой степени использует информационную технологию и информационное оружие. Он составляет «сетевизацию» (wangluohua) поля боя и является новой моделью для окончательной борьбы времени и пространства. В центре его — борьба за контроль над информационным полем боя, с тем, чтобы оказать воздействие или принять решение о победе или поражении.

Одним из первых отечественных ученых, кто создал целостную концепцию информационных войн, является С.П. Расторгуев. Для построения умозаключений С.П. Расторгуев искусно использует точно выверенный понятийный аппарат. Базовое понятие, применяемое им, — «информационная система». Из всего многообразия систем автор теории наиболее часто обращается к функционированию информационных самообучающихся систем (ИСС) — тех, которые претерпевают изменения при информационном воздействии. Человек, народ, государство представляют классические ИСС. Анализируя существующее положение вещей, он говорит о том, что наряду с защитой информации от внешних деструктивных угроз в современный период развития высоких коммуникационных и технологий и методик психологического развития в обществе возникает проблема защиты информационной системы от избыточного объема «некачественной» информации. Это связано с тем, что при получении информации информационная система перерабатывает ее по собственному алгоритму, при этом изменяя себя. Если на вход такой системы подать информацию, приводящую к ущербу для системы, то в результате можно добиться полного или частичного ее уничтожения.

Оружием информационной войны являются устройства и методы обработки информа­ции, которые используются для широкомасштабно­го, целенаправленного, быстрого и скрытного воздей­ствия на военные и гражданские информационные системы противника с целью подрыва его экономи­ки, снижения степени боеготовности и боеспособно­сти с целью способствовать достижению окончатель­ной победы. При этом имеется в виду, что информа­ционная война может вестись как самостоятельно, то есть без применения традиционных средств и спо­собов вооруженной борьбы, так и в сочетании с дру­гими видами боевых действий.

Рассмотрев указанные концепции информационных войн можно сделать выводы, что основополагающим свойством информационных войн является их асимметрия, то есть латентность и направленность на наиболее уязвимые места в информационной обороне противника. Кроме того, в настоящее время их последствия могут быть сравнимы с применением кинетического оружия, когда расходы на проведение могут быть меньше в тысячи раз. Лидерами в разработке теории информационных войн являются исследователи из США, России и Китая.

## Цели, методы и основные составляющие информационной войны

В современном мире информация является необходимым элементом, обеспечивающим функциональность любой системы наряду с материальным оборудованием. Качество информации, которой владеют стороны противоборства, напрямую влияет на их боеспособность. Например, в ВВС анализ результатов разведки и прогноз погоды являются основой для разработки полетного задания. Точность навигации влияет на эффективность выполнения задания. Здесь мы видим, что без качественной реализации информационных функций выполнение боевой задачи будет сорвано или его эффективность существенно снижена.

Следовательно, на боеспособность противника можно повлиять, уничтожив его инфраструктуру, живую силу и технику, а можно – нарушив его процессы обмена информацией или внедрив в информационные системы противника свою информацию. С этой точки зрения, задача информационной войны – воздействие на информацию противника с целью подрыва его боеспособности и защита своей информации от вражеского воздействия. Информация может выступать как целью воздействия, так и оружием в информационной войне.

Так что же такое информационная война?

На концептуальном уровне можно сказать, что государства стремятся приобрести информации, обеспечивающую выполнение их целей, воспользоваться ей и защитить ее. Эти использование и защита могут осуществляться в экономической, политической и военной сферах. Знание об информации, которой владеет противник, является средством, позволяющим усилить нашу мощь и понизить мощь врага или противостоять ей, а также защитить наши ценности, включая нашу информацию.

Информационная война - только средство, а не конечная цель, аналогично тому как бомбардировка - средство, а не цель. Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия.

Военные всегда пытались воздействовать на информацию, требующуюся врагу для эффективного управления своими силами. Обычно это делалось с помощью маневров и отвлекающих действий. Так как эти стратегии воздействовали на информацию, получаемую

врагом, косвенно путем восприятия, они атаковали информацию врага косвенно. То есть, для того чтобы хитрость была эффективной, враг должен был сделать три вещи:

наблюдать обманные действия;

посчитать обман правдой;

действовать после обмана в соответствии с целями обманывающего.

Тем не менее, современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляции с ней. Современные технологии позволяют противнику изменить или создать информацию без предварительного получения

**К информационной войне относятся две большие группы мероприятий:**

воздействие на военнослужащих и мирное население противника с целью внедрения массовое сознание определенных установок (пропаганда, «психологическая война»);

поражение информации, информационных процессов и информационно-управляющих систем противника, независимо от применяемых средств (и высокоточная ракета, и компьютерный вирус могут выступать оружием информационной войны).

**В информационной войне существуют три основные цели:**

контроль информационного пространства и обеспечение защиты своей информации от вражеских действий;

использование контроля над информационным пространством для проведения информационных атак на врага;

повышение общей эффективности вооруженных сил путем повсеместного внедрения военных информационных функций.

Приведем наглядный пример применения информационной атаки при выполнении ВВС стратегической атаки.

Предположим, что мы хотим ограничить стратегические возможности врага по переброске войск путем уменьшения запасов топлива. Сначала мы должны выявить нефтеперегонные заводы, которые будут наиболее подходящими целями при этой атаке. Потом нужно установить, какие заводы производят больше всего топлива. Для каждого завода нам надо выявить местоположение перегонных емкостей. Мы организуем атаку и, при значительной экономии сил, выводим заводы из строя, взрывая их только перегонные емкости, и оставляя все остальное оборудование нетронутым. Это классический пример стратегической атаки.

Теперь посмотрим, как надо добиться той же цели в информационной войне. Все современные нефтеперегонные заводы имеют большие автоматизированные системы управления. Эти информационные функции являются потенциальной целью в информационной войне. На ранней стадии конфликта мы выполнили разведывательную информационную операцию по проникновению и анализу системы управления нефтеперегонным заводом. В ходе анализа мы обнаружили несколько уязвимых информационных зависимостей, дающих нам средства воздействия на работу нефтеперегонного завода в нужное нам время. Позднее, в ходе конфликта, в ходе одной из операций по блокированию вражеской группировки мы использовали одно из уязвимых мест. Мы просто остановили эти заводы. Это, тоже классический пример стратегической атаки.

**Составные части информационной войны:**

1) психологические операции - использование информации для воздействия на аргументацию солдат врага.

2) Электронная война - не позволяет врагу получить точную информацию

3) дезинформация - предоставляет врагу ложную информацию о наших силах и намерениях

4) физическое разрушение - может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем.

5) меры безопасности - стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях.

6) прямые информационные атаки - прямое искажение информации без видимого изменения сущности, в которой она находится.

Существует два вида информационных атак: косвенная и прямая. Разницу между ними лучше всего пояснить на примере. Допустим, мы хотим ввести командование противника в заблуждение относительно места дислокации нашей авиационной части. Можно построить ложный аэродром, разместить там макеты самолетов и имитировать деятельность по их техническому обслуживанию. Это – косвенная информационная атака. А можно внедрить ложную информацию о местонахождении той же авиационной части прямо в хранилище информации противника, чтобы при принятии решений вражеское командование оперировало ложными данными. Это – прямая информационная атака.

Таким образом, по своему характеру информационная война за­нимает положение между «холодной» войной, вклю­чающей, в частности, экономическую, и реальными боевыми действиями с участием вооруженных сил. В отличие от экономической, результатом информа­ционной войны является нарушение функционирования элементов инфраструктуры противника (пунктов управления, ракетных и стартовых позиций, аэродро­мов, портов, систем связи, складов и т. д.), а в отли­чие от «горячей» войны с применением обычных во­оружений и (или) оружия массового поражения ее целями являются не материальные, а «идеальные» объекты (знаковые системы) или их материальные носители. В то же время разрушение таких объектов и систем может осуществляться с сохранением их материальной основы.

# Основная часть

# заключение