

ЛЕКЦИЯ 4. PR-ТЕХНОЛОГИИ ИНФОРМАЦИОННЫХ ВОЙН В СОВРЕМЕННОМ МИРЕ

4.1. Информационная война: определение и сфера деятельности

Человечество с незапамятных времен сталкивалось с проблемой информационных войн на всех уровнях, и лук, стрелы, мечи, пушки и танки, в конце концов, только завершали физический разгром сообщества, уже потерпевшего поражение в информационной войне.

Технологическая революция привела к появлению термина «информационная эра» из-за того, что информационные системы стали частью нашей жизни и изменили ее коренным образом. Информационная эра также изменила способ ведения боевых действий, обеспечив командиров беспрецедентным количеством и качеством информации. Теперь командир может наблюдать за ходом ведения боевых действий, анализировать события и доводить информацию.

Следует различать войну информационной эры и информационную войну. Война информационной эры использует информационную технологию как средство для успешного проведения боевых операций. Напротив, информационная война рассматривает информацию как отдельный объект или потенциальное оружие и как выгодную цель. Технологии информационной эры сделали возможной теоретическую возможность – прямое манипулирование информацией противника.

Информация появляется на основе событий окружающего мира. События должны быть восприняты каким-то образом и проинтерпретированы, чтобы стать информацией. Поэтому информация результат двух вещей – воспринятых событий(данных) и команд, требуемых для интерпретации данных и связывания с ними значения.

Сам термин «информационная война» стал активно упоминаться в СМИ после проведения операции «Буря в пустыне» в 1991 г., когда новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же данный термин впервые был употреблен в директиве министра обороны США № 3600 от 21 декабря 1992 г. Под информационной войной понимается процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня путем воздействия на гражданское население, власти и (или) вооруженные силы противостоящей стороны посредством распространения специально отобранной и подготовленной информации, информационных материалов и противодействия таким воздействиям на собственную сторону.

Несмотря на относительную новизну термина, явление информационных войн не является новым. На протяжении всей истории человечества как во время войн, так и в мирные дни использовались различные модели коммуникативного воздействия с разнообразным арсеналом средств. Еще в V веке до нашей эры во время греко-персидских войн царь Ксеркс распространял слухи о бесчисленности своего воинства, чтобы запугать греков. А Сунь Цзы в своем трактате «Искусство войны» писал, что война – есть путь обмана, предполагая, что победа в войне находится не на поле боя, но вне него.

Качество информации – показатель трудности ведения войны. Чем более качественной информацией владеет командир, тем большие него преимущества по сравнению с его врагом. Так, например, в военно-воздушных силах, анализ результатов разведки и прогноза погоды является основой для разработки полетного задания. Точная навигация увеличивает эффективность выполнения задания. Все вместе они являются видами военных информационных функций, которые увеличивают эффективность боевых операций.

Поэтому дадим определение военным информационным функциям – это любые информационные функции, обеспечивающие или улучшающие решение войсками своих боевых задач.

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.

Информационное оружие воздействует на информацию, которой владеет враг и его информационные функции. При этом наши информационные функции защищаются, что позволяет уменьшить его волю или возможности вести борьбу. Поэтому дадим определение информационной войне – это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций.

Это определение является основой для следующих утверждений.

Информационная война:

- это комплексное совместное применение сил и средств информационной и вооруженной борьбы.

- это коммуникативная технология по воздействию на информацию и информационные системы противника с целью достижения информационного превосходства в интересах национальной стратегии, при одновременной защите собственной информации и своих информационных систем.

- это 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 фактов и их интерпретации. Вот краткий список характеристик современных информационных систем, приводящим к появлению подобной уязвимости: концентрированное хранение информации, скорость доступа, повсеместная передача информации, и большие возможности информационных систем выполнять свои функции автономно. Механизмы защиты могут уменьшить, но не до нуля эту уязвимость.

Составные части информационной войны

- психологические операции – использование информации для воздействия на аргументацию солдат врага.
- электронная война – не позволяет врагу получить точную информацию
- дезинформация – предоставляет врагу ложную информацию о наших силах и намерениях

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

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

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

Существует два способа повлиять на информационные функции врага – косвенно или напрямую. Проиллюстрируем разницу между ними на примере.

Пусть нашей целью является заставить врага думать, что авиаполк находится там, где он совсем не находится, и действовать на основании этой информации таким образом, чтобы это было выгодно нам.

Косвенная информационная атака: используя инженерные средства, мы можем построить макеты самолетов и ложные аэродромные сооружения, и противник будет наблюдать ложный аэродром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник по нашему мнению.

Прямая информационная атака: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут разительно отличаться.

Другим примером прямой информационной атаки может быть изменение информации во вражеской базе данных об имеющихся коммуникациях в ходе боевых действий (внесение ложной информации о том, что мосты разрушены) для изоляции отдельных вражеских частей. Этого же можно добиться бомбардировкой мостов. И в том, и в другом случае вражеские аналитики, принимая решение на основе имеющейся у них информации, примут одно и то же решение – производить переброску войск через другие коммуникации.

Оборонительной стороной информационной войны являются меры безопасности, имеющие своей целью защитить информацию – не позволить противнику провести успешную информационную атаку на наши информационные функции. Современные меры защиты, такие как операционная безопасность и коммуникационная безопасность – типичные средства по предотвращению и обнаружению косвенных действий врага, направленных на наши военные информационные функции. Напротив, такие меры защиты, как компьютерная безопасность включают в себя действия по

предотвращению, обнаружению прямых информационных действий врага и организации контрдействий.

4.2. Цели и последствия информационной войны

Существуют три цели информационной войны:

- контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация).
- использовать контроль над информацией для ведения информационных атак на врага
- повысить общую эффективность вооруженных сил с помощью повсеместного использования 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.

Следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть

составной частью обширного плана атаки. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий – будь то на реальном поле брани, либо в экономической, политической или социальной сферах.

Театр информационных боевых действий простирается от секретного кабинета до домашнего персонального компьютера и ведется на различных фронтах. Электронное поле боя представлено постоянно растущим арсеналом электронных вооружений, преимущественно засекреченных. Говоря военным языком, они предназначены для боевых действий в области командования и управления войсками, или «штабной войны». Последние конфликты уже продемонстрировали всю мощь и поражающую силу информационных боевых действий – война в Персидском заливе и вторжение на Гаити. Во время войны в Персидском заливе силы союзников на информационном фронте провели комплекс операций в диапазоне от старомодной тактики разбрасывания пропагандистских листовок до вывода из строя сети военных коммуникаций Ирака с помощью компьютерного вируса.

Атаки инфраструктуры наносят удары по жизненно важным элементам, таким как телекоммуникации или транспортные системы. Подобные действия могут быть предприняты геополитическими или экономическими противниками или террористическими группами. Примером служит вывод из строя междугородной телефонной станции компании AT&T в 1990 году. В наши дни любой банк, любая электростанция, любая транспортная сеть и любая телевизионная студия представляют собой потенциальную мишень для воздействия из киберпространства.

Промышленный шпионаж и другие виды разведки грозят великим множеством тайных операций, осуществляемых корпорациями или государствами в отношении других корпораций или государств; например, сбор информации разведывательного характера о конкурентах, хищение патентованной информации и даже акты саботажа в форме искажения или уничтожения данных. Иллюстрацией этой угрозы служит документально доказанная деятельность французских и японских агентов на протяжении восьмидесятых годов.

Сбор разведывательной информации также выходит на новые рубежи. Лаборатория Линкольна в Массачусетском технологическом институте разрабатывает аппарат для воздушной разведки размером с пачку сигарет. Другая лаборатория работает над химическими веществами, которые можно

ввести в провизию неприятельских войск, чтобы позволить датчикам отслеживать их перемещение по дыханию или выделению пота. Помимо этого уже имеются спутниковые системы слежения, имеющие разрешающую способность в несколько сантиметров.

Конфиденциальность все более уязвима по мере появления возможности доступа к постоянно растущим объемам информации в постоянно растущем числе абонентских пунктов. Важные персоны, таким образом могут стать объектом шантажа или злобной клеветы, и никто не гарантирован от подложного использования личных идентификационных номеров.

Как бы то ни было, термин «информационная война» обязан своим происхождением военным и обозначает жестокую и опасную деятельность, связанную с реальными, кровопролитными и разрушительными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и так далее.

Последствия информационной войны

Взрыв нескольких гранат нельзя назвать войной, кто бы их ни бросал. Взрыв нескольких водородных бомб – это уже и начатая и завершенная война. Информационную пропаганду 50-ых, 60-ых годов, которой занимались СССР и США, можно сравнить именно с несколькими гранатами. Поэтому никто не называет прошлое противостояние информационной войной, в лучшем случае оно заслуживает термина «холодная война».

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.

Почему надо защищать информационную систему от информации? Потому что любая поступающая на вход системы информация неизбежно изменяет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и к самоуничтожению.

Поэтому информационная война – это не что иное, как явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Исходя из приведенного определения информационной войны, применение информационного оружия означает подачу на вход информационной самообучающейся системы такой последовательности входных данных, которая активизирует в системе определенные алгоритмы, а в случае их отсутствия – алгоритмы генерации алгоритмов.

Создание универсального защитного алгоритма, позволяющего выявить системе-жертве факт начала информационной войны, является алгоритмически неразрешимой проблемой. К таким же неразрешимым проблемам относится выявление факта завершения информационной войны.

Однако, несмотря на неразрешимость проблем начала и окончания информационной войны, факт поражения в ней характеризуется рядом признаков, присущих поражению в обычной войне. К ним относятся:

- 1) включение части структуры пораженной системы в структуру системы победителя (эмиграция из побежденной страны и в первую очередь вывоз наиболее ценного человеческого материала, наукоемкого производства, полезных ископаемых);
- 2) полное разрушение той части структуры, которая отвечает за безопасность системы от внешних угроз (разрушение армии побежденной страны);
- 3) полное разрушение той части структуры, которая ответственна за восстановление элементов и структур подсистемы безопасности /разрушение производства, в первую очередь, наукоемкого производства, а также научных центров и всей системы образования; прекращение и запрещение разработок и производств наиболее перспективных видов вооружения);
- 4) разрушение и уничтожение той части структуры, которая не может быть использована победителем в собственных целях;
- 5) сокращение функциональных возможностей побежденной системы за счет сокращения ее информационной емкости (в случае страны: отделение части территории, уничтожение части населения).

Обобщив перечисленные признаки, можно ввести понятие «степень поражения информационным оружием», оценив ее через информационную емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Информационное оружие даст максимальный эффект только тогда, когда оно применяется по наиболее уязвимым от него частям ИСС. Наибольшей информационной уязвимостью обладают те подсистемы, которые наиболее чувствительны к входной информации – это системы принятия решения, управления. На основании сказанного можно ввести понятие информационной мишени. Информационная мишень – множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Исходя из определения информационной мишени, намечаются основные направления работ, как по обеспечению ее безопасности, так и по повышению ее уязвимости. Например, для того, чтобы повысить уязвимость противника, следует максимально расширить его информационную мишень, т.е. подтолкнуть его на включение в мишень как можно больше равноправных элементов, причем желательно открыть доступ в сферу управления таким элементам, которые легко поддаются перепрограммированию и внешнему управлению. Заставить противника изменить свое поведение можно с помощью явных и скрытых, внешних и внутренних информационных угроз. Причины внешних угроз в случае целенаправленного информационного воздействия (в случае информационной войны) скрыты в борьбе конкурирующих информационных систем за общие ресурсы обеспечивающие системе допустимый режим существования. Причины внутренних угроз – в появлении внутри системы множества элементов, подструктур, для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым. Скрытая угроза – это неосознаваемые системой в режиме реального времени входные данные, угрожающие ее безопасности. В информационной войне наибольший приоритет отдается скрытым угрозам, так как именно они позволяют возвращать внутренние угрозы и целенаправленно управлять системой извне.

В заключение еще раз подчеркнем, что информационная война – это война алгоритмов и технологий; это война, в которой сталкиваются именно структуры систем, как носители знаний. Это значит, что информационная война – это война базовых знаний и ведется она носителями этих самых базовых знаний. На современном этапе, когда базовые знания человечества аккумулированы в рамках различных современных цивилизациях, информационная война олицетворяет собой войну цивилизаций за место под солнцем в условиях все сокращающихся ресурсов. Открыто говорить о приемах и методах информационной войны сегодня необходимо потому, что,

во-первых, осмысление того или иного приема информационной войны позволяет перевести его из разряда скрытых угроз в явные, с которыми уже можно бороться, во-вторых, факт наличия теории информационной войны должен предостеречь потенциальную жертву от идеалистически наивного восприятия как внешнего, так и собственного внутреннего мира.

4.3. PR-технологии в информационных войнах

Специфика PR заключается в воздействии на общественное сознание с целью его изменения. И нельзя критиковать PR-технологии за то, что в их рамках происходят манипуляции и управляющие воздействия. Если их исключить – исчезнет и PR как феномен современных коммуникативных технологий. Таким образом, можно говорить о том, что специфика методов воздействия на массовое сознание определяется свойствами и спецификой самого массового сознания, а использования PR-технологий в информационно-психологической войне само по себе подразумевает задействование технологий психологических манипуляций и управленческих воздействий. В случае же, если свойства и специфика массового сознания как объекта воздействия изменятся, то неизменно претерпят изменения и сами методы воздействия. Что же касается «окрашивания» в черные и белые цвета, то подобная редукция сложности недопустима. Более того, окрашивание в определенные цвета в зависимости от поставленных задач свойственно именно манипулятивной, пропагандистской и PR-деятельности. При объективном же исследовании подобных процессов следует избегать оценочных суждений даже в цветовом смысле.

При рассмотрении методов воздействия на массовое сознание необходимо рассмотреть и другой важный аспект. Насколько эффективно можно ограничить применение нежелательных психотехнологий законодательными рамками? Кто должен определять «безопасность» и «корректность» подобных технологий, осуществлять контроль за информационно-психологическими процессами и насколько возможен мониторинг неявных, скрытых воздействий на массовое сознание? Ответы на данные вопросы сегодня неоднозначны – разрешение данных проблем возможно в каждой конкретной ситуации.

В век становления информационного общества актуальность использования средств массовой информации как канала коммуникации сложно переоценить. Благодаря постоянно растущей аудитории у СМИ резко вырос объем информации, которую государства перестали контролировать. А это значит, что информация превратилась в один из важнейших ресурсов. Впервые термин «информация» стал ассоциироваться с оружием. «Кто

владеет информацией, тот владеет миром», – крылатая фраза Н. Ротшильда, жившего в XIX веке, сейчас актуальна как никогда. Но важна стала не столько сама информация, а способы и методы ее применения. Среди них особенно эффективными в контексте воздействия на общество являются политические PR-технологии.

Повышенный интерес к PR-технологиям в сфере политики связан с несколькими процессами. Во-первых, глобальный контроль деятельности государств в различных сферах со стороны международных организаций. Теперь агрессия в любом виде не одобряется мировым сообществом. Отсюда появилась необходимость в поисках новых источников силы и влияния. Во-вторых, постоянное развитие теорий коммуникаций и влияния на массовое сознание актуализировали данную область научного знания.

Сегодня именно PR-технологии с опорой на функционирующие СМИ превратились в новую ветвь власти, от которой зависят происходящие в мире геополитические и экономические процессы глобального и локального характера. Именно поэтому проблема ведения информационных войн является столь актуальной и востребованной на современном этапе развития политики, экономики и социума.

За последние полстолетия человечество совершило серьезный скачок в области информационных технологий. Информационные носители стали более доступными и компактными, соответственно вырос и уровень информированности общества. Это отразилось в качественном развитии таких каналов коммуникаций, как радио и телевидения, а с конца 80-х гг. XX века – глобальной сети Интернет. Интернет дал невиданный ранее доступ к огромным массивам информации. Благодаря анонимности и мультимедийности он постепенно становится важнейшим источником информации. Смена поколений окончательно отодвигает телевидение на второй план.

В современном мире созданы идеальные условия для ведения информационной войны: полная свобода СМИ, отсутствие цензуры во всех ее формах, доступность получения и передачи информации в любом виде. Таким образом, особенно действенным методом ведения информационных войн становятся PR-технологии.

Под PR-технологиями следует понимать комплекс организационных мер и приемов использования СМИ, обусловленных текущим уровнем развития науки и направлен-

ных на аудиторию для воздействия на нее в нужном для организаций направлении.

Информационная война может опираться на методы планирования кампании, разработанные в рамках PR, поскольку для PR-кампании характерно не просто внимание к аудитории, но и внимание к косвенным методам воздействия.

Информационная война зачастую выглядит как масштабная PR-кампания и строится по аналогичной схеме. Например, Ф. Джефкинс предлагает модель PR-кампании, которая включает шесть этапов:

- анализ ситуации;
- определение целей;
- определение публики;
- отбор каналов массовой коммуникации и методов работы с ними;
- планирование бюджета;
- анализ результатов.

Данные этапы PR-кампании характерны и для ведения информационной войны. Основным отличием является масштабность и значимость.

Политические PR-технологии строятся не на логических доводах и фактах, а на эмоциональном впечатлении. Главной особенностью использования PR-технологий в информационных войнах становится тот факт, что мы не присутствуем при конкретных событиях, не видим их своими глазами, поэтому вынуждены руководствоваться только материалами, поданными СМИ. Из медиа мы узнаем не только о самом событии, но и получаем сразу его оценку. И, конечно, проецируем ее на себя. Оценка, качественно и своевременно поданная нам, становится нашей оценкой.

Ярким примером служит, например, вооруженный конфликт между Южной Осетией и Грузией в 2008 г. Основная особенность этого противостояния состоит в том, что если непосредственные боевые действия велись между российскими и грузинскими войсками, то в ходе информационной войны Россия столкнулась с США и Европой. На западном телевидении, в частности на CNN и BBC, представляли конфликт не иначе как вторжение агрессивной России в маленькую Грузию. Фото и видеорепортажи западных СМИ демонстрировали разрушения, которым якобы подверглась Грузия, которые сопровождались заголовками об агрессии России. А вот лишь некоторые заголовки печатных изданий Великобритании и США: «Россия не извлечет выгоды из агрессии» (The Times), «Россия – это по-прежнему голодная империя» (The Wall Street Journal).

Таким образом, западное общество стало объектом использования PR-технологий. Под влиянием СМИ им была навязана точка зрения, что Россия в этом конфликте является агрессором. Во многом эта история повторяется и в 2022-2025 гг, в ходе действий российских войск в зоне специальной военной операции.

PR-сопровождение политических процессов, войн и военных конфликтов стало настоятельным требованием нашей информационной эпохи. Результаты PR-кампаний показывают, какое влияние было оказано на мировое общественное мнение, состояние общественного сознания внутри каждой стороны – участницы конфликта.

Можно сделать вывод, что в современном мире информационная война стала вполне законным способом политического противостояния. Причем война ведется как между отдельными политическими личностями, так и между государствами. Несмотря на то, что значительная часть общества осознает процесс целенаправленного информационного воздействия на противника и допускает возможность использования манипуляционных технологий, оно все равно поддается воздействию со стороны средств массовой информации. В конечном итоге в информационной войне побеждает тот, кто более оперативно и качественно преподносит нужную ему информацию целевой аудитории, а не тот, кто просто говорит правду.