Методичка инфобойца

Нежданов Игорь

Игорь Нежданов

Методичка инфобойца

«Автор»
2023

Нежданов И. Ю.

Методичка инфобойца / И. Ю. Нежданов — «Автор», 2023

В книге детально разобраны используемые противником технологии информационных операций в интернете. Рассказано как осуществляется планирование информационных операций, определение целевой аудитории, выявление ее уязвимостей и формирование сценария влияния на аудиторию.

© Нежданов И. Ю., 2023
© Автор, 2023

Содержание

ПРЕДИСЛОВИЕ 5
ВВЕДЕНИЕ 6
ТЕОРИЯ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ 9
Конец ознакомительного фрагмента. 30

Игорь Нежданов
Методичка инфобойца

Есть много работ, содержащих в названии сокровенные "информационная война" или "информационно-психологическая война", но внутри лишь рассуждения о сферическом коне в вакууме. И никакой конкретики. И вот именно об этих технологиях и этой конкретики я вам и расскажу – о том какие шаги необходимо осуществить для достижения цели информационной операции и как именно эти шаги сделать.

ПРЕДИСЛОВИЕ

Книга, которую вы держите в руках, будет полезна для людей, в своей профессиональной деятельности прямо или косвенно касающихся проблем манипулирования общественным мнением, информационных войн, мероприятий влияния, информационно-психологических операций и т.п.. Книга позволяет понять что предпринимает противник и как этому противостоять.

Сам материал стал результатом структурирования накопленных мной опыта и знаний, и не является учебником в прямом смысле этого слова. Скорее это «методичка» – вспомогательный материал для погружения в проблематику. Тем не менее я постарался излагать таким образом, чтобы было удобно изучать, а последовательность изложения соответствует этапам проведения таких мероприятий. Это упрощает как изучение, так и использовать в качестве справочной литературы по проблематике. Далее буду называть данный материал «методичкой» для простоты изложения.

Строго говоря мысль поделиться опытом с коллегами появилась с появлением этого самого опыта. Дело в том, что давно-давно, когда только делал первые шаги в рыночной экономике, очень нуждался в неком наставлении, которое позволило бы совершить меньше ошибок. Долго искал такое наставление по информационным операциям или намек на него. Увы – ничего достойного не нашлось. Видимо плохо искал. На самом деле словосочетание то такое «информационная операция» было не известно на просторах Родины в то время. Была безопасность, был PR, был политконсалтинг. Но об информационных операциях о чем то похожем никто и не слышал.

Да и сейчас ситуация не особо улучшилась. Появилось много изданий, содержащих в названии сокровенные "информационная война" или "информационно-психологическая война", но внутри лишь рассуждения о сферическом коне в вакууме. И никакой конкретики. Проблема, смоей точки зрения, в том, что пишут такие книги вовсе не те, кто собственными руками осуществляет мероприятия влияния. А по тому авторы ничего не знают о технологиях информационных операций. И вот именно об этих технологиях я вам и расскажу.

Здесь вы не найдёте рассуждений о добре и зле, прений о терминологии и иных растеканий мыслью по древу, свойственных академическим кругам. Оставляю эту, безусловно важную и нужную, часть исследований научным деятелям. Я практик и рассказываю про инструмент, который нужно уметь правильно использовать. Зато будут детально разобраны процедуры планирования информационных операций, выявления уязвимостей аудитории, создания ударного контента, контроля эффективности мероприятий.

ВВЕДЕНИЕ

Каждое действие или бездействие имеет коммуникативный (или медийный) эффект, воспринимаемый разными аудиториями, которые формируют собственное отношение к этому действию. А вот действие инфобойца изначально направлено на создание заранее запланированной реакции аудитории.

Данная методичка служит пособием в определении того, что и как нужно делать для достижения планируемого медийного эффекта в рамках информационной операции.

Методичка состоит из нескольких основных частей.

Часть 1 «ОБЩЕЕ» это краткое описание интернета как особой среды, где и происходят интересующие нас процессы, и немного описание роли и места этих процессов в жизни общества.

Часть 2 «ТЕОРИЯ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ» знакомит с основами информационных операций от понимания «что это такое» до цикла информационных операций.

Часть 3 «ПРОВЕДЕНИЕ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ» посвящена вопросам собственно организации информационных операций, их планированию и планированию отдельных этапов.

Часть 4 «ПРАКТИКУМ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ» здесь даны дополнительные материалы, которые будут полезны в такой работе.

Особенности интернета как нового ТВД

У интернета есть ряд особенностей, которые делают его уникальным инструментом в информационных войнах.

1 Информация в интернете распространяется мгновенно. Считается, что если вы не предприняли специальных усилий, то после нажатия «Enter» ваша информация становится доступна всем пользователям интернета. Конечно, это с рядом оговорок, но на бытовом уровне именно так. Поэтому интернет стал конкурентом ТВ и Радио в скорости распространения ударного контента.

2 В интернете нет границ и расстояний – вы с одинаковой скоростью и комфортом можете взаимодействовать как с соседом по лестничной клетке, так и с человеком на другом континенте. Для вас нет разницы как далеко от находится ваш визави.

3 В интернете есть возможность анонимизации, опять-же, с некоторыми оговорками, что позволяет злоумышленнику не просто остаться в тени, но и создать неограниченную «армию» фейковых аккаунтов, которые смогут имитировать массовость поддержки некой идеи.

Рост проникновения интернета

Интернет стремительно входит во все новые сферы нашей жизни. По данным исследователей активных пользователей интернета в 2023 году стало 5,01 миллиарда человек и рост их числа продолжается. Уже не менее 65,6%, населения Земли имеют доступ к Интернету и этот показатель растет ежедневно. А это те люди, которые не просто «подключены» к интернету, а и подвержены воздействию через интернет. Для них интернет стал прямым каналом доставки ударного контента.

Экспоненциальный рост объёмов информации

Объем контента, создаваемого в интернете, только растёт, что делает в принципе невозможным его ручную обработку. На август 2021 года, в интернете насчитывается 1,88 млрд сайтов. А объем информации с 2010 по 2020 увеличился еще в 50 раз и процесс прироста только ускоряется. В результате говорить о ручной обработки таких объемов данных не приходится – нужна автоматизация всего, что возможно. Люди не способны справиться с тем потоком новостей, который на них обрушивается ежедневно. И этим пользуются манипуляторы.

Постоянное изменение структуры интернета

В интернете постоянно происходит изменение как его структуры, так и формата данных. Это выражается в появлении:

–Новых сервисов;

–Новых типов сервисов;

–Новых сайтов и страниц на сайтах;

–Новых каналов и технологий доставки ударного контента.

Такая ситуация требует своевременного выявления подобных изменений и постоянной адаптации любых создаваемых систем под такие изменения.

Роль инфо-пси в современных конфликтах

Современная западная военная мысль отводит информационным операциям важнейшую роль в конфликтах разной интенсивности. Это связано в первую очередь с тем, что информационная операция позволяет совершать агрессию вплоть до победы без «горячей фазы конфликта». Это существенно снижает риск перерастания конфликта в ядерный или глобальный.

Фундаментальное изменение ТВД

Защита от вторжения в настоящее время требует своевременно выявлять информационные операции противника, осуществлять и распространять свои инфо-операции. Поэтому меняется структура методов ведения войны в сторону ненасильственных, в том числе информационного противоборства и кибер-агрессии.

До 19 века включительно любые военные действия носили исключительно насильственный характер (уничтожение живой силы, разрушение укреплений и инфраструктуры и т.п..). И лишь в редких случаях использовалась агитация, его дезинформирование.

В 20 веке ненасильственным метода отводилось уже больше места в войнах. Активно использовались агитация и пропаганда, обман противника и дестабилизация его тылов за счет паники. По оценкам военных аналитиков доля ненасильственных методов стала составлять до 20%.

В начале 21 века войны приобрели гибридный характер и роль информационных методов воздействия на противника стала еще существеннее. Тут уже помимо названных технологий в полной мере проявились методы воздействия на системы принятия решений. А военные аналитики стали отводить от 50 до 60% на ненасильственные методы воздействия.

Еще интереснее выглядит прогноз этих аналитиков. Они предполагают, что в ближайшее время доля ненасильственных методов воздействия на противника будет составлять около 80%. Это будет и ино-пси операции, и кибер-операции. Причем целью воздействия станет менталитет военных и граждан противника.

Видимо именно поэтому противник считает наиболее перспективным развитие сил и средств для войны в киберпространстве, особенно для конфликтов малой интенсивности. И

это направление выделено у стратегов Пентагона в отдельный домен (сферу) наряду с морем, сушей, воздухом и космосом.

Усилия противника

В соответствии со своей военной стратегией противник сосредоточил огромные средства в разработке, закупке и эксплуатации сил и средств для ведения войны в киберпространстве.

Так в бюджете Пентагона на 2023 год на затраты, связанные с киберпространством, выделяется около 178 млрд долларов, это 23% от всего бюджета Пентагона. Мало того, в рамках этой доли бюджета только на исследования в данной области выделяется около 27 млрд долларов.

Помимо этого, противник создал масштабную, вертикально-интегрированную структуру для психологических операций и управления ими как в рамках одного государства (США), так и в рамках объединений (НАТО, «5 глаз» и т.п.).

В стратегии противника, основанной на докладе RAND от декабря 2022 года (Роль информации в концепции стратегического соперничества), прямо указывается, что наличие у соперничающих стран ядерного оружия обеспечивает им высокую степень иммунитета к прямому военному принуждению и существенно ограничивает возможность военного ответа. В такой ситуации информационно-психологическое воздействие становится наиболее подходящим, а иногда и единственно- возможным.

Наиболее перспективными направлениями использования информационно-психологического воздействия стратеги Пентагона называют:

–Подрыв воли противника к борьбе (сопротивлению);

–Вмешательство в процесс принятия решений;

–Создание условий, благоприятных для дружественных сил.

А в качестве конкретных действий в рамках этой парадигмы предлагаются следующие:

–Отнесение действий противника к негативно-воспринимаемой категории (обвинение в геноциде, в терроризме или его поддержке и т.п..);

–Вынесение обвинительных заключений в отношении ключевых лиц противника (расследования, санкционные списки, Гаагский трибунал);

–Эмбарго, запреты и прочие ограничения под любыми, в том числе ложными, предлогами;

–Любые соглашения, договоренности с противником, но без их исполнения;

–Легитимизация любых своих действий как ответных на соответствующую активность противника;

–Использование международных институтов для принуждения, дискредитации или наказания противника (МОК, ОБСЕ, ОЗХО…).

ТЕОРИЯ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ

Использование информационных операций является неотъемлемой частью широкого спектра современных военных, дипломатических, экономических, гражданских и информационных усилий государств, направленных на предотвращение конфликтов,реагирование на кризисы или достижения своих геополитических амбиций.

Что такое информационная операция

В разных странах приняты разные определения информационной операции. Если их свести воедино, то:

информационная операция в интернете – это совокупность взаимосвязанных действий, направленных на манипулирование выбранной аудиторией с целью подтолкнуть эту аудиторию к целевому действию.

При этом информационные операции прямо влияют на волю как дружественных, так и нейтральных, и враждебных сил в целевой аудитории и в «сопредельных» аудиториях. Такой эффект достигается за счет оказания воздействия на устремления аудиторий через управление их отношением, настроением, желаниями. И в конечном счете склоняет эти аудитории, например, к поддержке национальной политики и национальных целей. А для военного руководства информационные операции служат одним из средств достижения военных целей.

В настоящее время способы оказания воздействия на поведение человека разнообразны и позволяют адаптировать влияние под особенности любой аудитории. Такое положение стало возможным благодаря разработке современных научных подходов к исследованию мотивов поведения человека и разнообразию высокотехнологичных каналов связи. При этом цель информационных операций в интересах военного ведомства остается прежней – способствовать достижению целей военных операций как в мирное, так и в военное время путем изменения мнений, отношений, чувств, а в конечном итоге поведения людей, являющихся объектом воздействия в информационной операции.

Миссия подразделений информационных операций

Информационные операции проводятся на стратегическом, оперативном и тактическом уровнях. Силы информационных операций обеспечивают возможность передачи специально подготовленной информации выбранным ЦА, чтобы влиять на их эмоции, мотивы, мышление, принятие решений и поведение. Бойцы ИО выполняют следующие основные функции для достижения цели информационной операции:

Консультирование вышестоящего руководства по информационным операциям, которые будут выполняться и их ограничениям. Это позволяет добиться максимально эффективного взаимодействия и сводят к минимуму неблагоприятные воздействия на защищаемую ЦА.

Воздействие на атакуемую ЦА, чтобы повлиять на, поведение и добиться желаемых действий. Эти действия облегчают военные операции, сводят к минимуму ненужные человеческие жертвы и побочный ущерб.

Противодействие вражеской пропаганде, дезинформации и иным действиям, чтобы правильно и позитивно изображать дружественные намерения и действия, тем самым лишая противника возможности поляризовать общественное мнение внутри страны.

Цели и задачи ИО

Цель информационной операции всегда одна – заставить аудиторию совершить целевое действие в сейчас или в будущем. В работах западных аналитиков указывается, что цель информационных операций, в глобальном плане, это разум человека как индивидуальный, так и коллективный. А информационная война в общем виде называется нетрадиционной формой ведения войны, в которой используются технологии (кибер-инструменты) для изменения мыслительных процессов людей-мишеней (аудитории противника).

Это война против того, что думает, любит или во что верит вражеское общество, путем изменения его восприятия. Это война за то как враг думает и принимает решения, как он видит мир и как его оценивает.

Целевое действие аудитории, которое хочет достичь противник, в разных операциях может быть самым разным:

–Выйти на не согласованные протестные акции;

–Не выходить на протестные акции;

–Проголосовать за нужного кандидата на выборах;

–Поставить лайк к нужной публикации в соцсети;

–Отказаться от сотрудничества с кем-то;

–Написать открытое письмо в поддержку;

–Совершить иное действие, нужное манипулятору.

Но это обязательно некое действие. Иногда за цель информационной операции принимают пусть и глобальную, но промежуточную задачу. Например «смена ценностных ориентиров аудитории» вовсе не конечная цель информационной операции. Конечная цель будет то действие, которое эта ЦА должна совершить после смены ценностных ориентиров. Как вариант – принять активное участие в очередной цветной революции. Именно это действие и является целью всей информационной операции, а не смена ориентиров.

Если под таким углом взглянуть на некоторые геополитические процессы, то ситуация становиться более понятной. Так информационная война, ведущаяся против России «коллективным Западом», нацелена на достижение вполне конкретной цели: сохранения глобального господства этого «коллективного запада». Это стратегическая цель. А вот каким образом это господство сохранить является целями более низкого уровня. К ним относятся:

Недопущение создания центров влияния, способных конкурировать с гегемоном;

Уничтожение сформировавшихся центров влияния, способных конкурировать с гегемоном.

Следующий уровень указанных целей – это объяснение как реализовать пункты 1 и 2. Например для пункта «Уничтожение сформировавшихся центров влияния, способных конкурировать с гегемоном»:

1. Выявление таких центров влияния и их изучение:

1.1. Собственно выявление таких центров влияния

1.2. Определение опасности таких центров влияния

2. Нейтрализация таких центров влияния:

2.1. Выявление уязвимостей таких центров влияния

2.2. Определение способа воздействия (уничтожение, раскол на несколько элементов, отвлечение ресурсов…)

2.3. Реализация воздействия.

А уже от выбранного «гегемоном» способа нейтрализации угрозы зависит то, каким образом будет осуществляться воздействие, в том числе какие сценарии информационной

войны может реализовать противник и какие промежуточные цели будут заложены в информационные операции.

В традиционной войне информационные операции способны повышать боевую эффективность войск при неизменной их численности и качественного состава. Информационные операции, если их осуществление было начато заблаговременно, и они проводились с высокой эффективностью, могут позволить достичь цели без применения военной силы.

Задачи информационной операции зависят от поставленной цели и технологически могут заключаться в:

1. Подрыве доверия населения к руководству своей страны:

1.1. Недовольство населением действий руководства страны;

1.2. формировании (увеличении) уровня поддержки среди войск и населения противника антивоенных настроений;

2. Подрыве доверия личного состава войск противника к своем руководству, снижении боеготовности, снижении интенсивности боевых действий:

2.1. Снижении уровня доверия личного состава войск противника к своему руководству и командованию;

2.2. Формировании готовности (провоцировании) личного состава противника к неповиновению командованию, совершение самосуда, дезертирства, членовредительства, повреждения вооружения и военной техники, сдачи в плен и других способов уклонений от участия в боевых действиях;

3. Подрыве доверия населения страны к правоохранительной системе;

3.1 Подрыве у руководства страны противника, военного командования и личного состава войск противника психологической стойкости и готовности к выполнению задач назначения;

3.2 Формировании и обострение существующих противоречий среди населения общественно-политического, экономического, культурного, этнического, религиозного характеров;

3.3 Формировании ощущения безысходности, брошенности, бесполезности;

4. Проведение мероприятий по введению противника в заблуждение.

Отдельными работами в рамках одной информационной операции могут являться следующие действия:

–Вброс или первичная публикация ударного контента;

–Разгон уже вброшенного ударного контента разными методами;

–Вспомогательные действия (сокрытие следов, адаптация аккаунтов и т.п..).

Эти работы в разных сочетаниях образуют то, что обычно называют информационной операцией.

Первичная публикация ударного контента или вброс – действие, когда манипулятор впервые публикует ударный контент с целью дальнейшего его распространения.

Ударный контент – это контент, используемый для манипулирования целевой аудиторией. Ударный контент может быть не достоверной информацией, может быть полностью достоверной, или достоверной с незначительными вкраплением лжи, достоверной информацией с нарушением логики, или с добавлением эмоций. Структура ударного контента зависит от метода, выбранного злоумышленником, для манипулирования аудиторией.

Осуществляя воздействие на аудиторию, манипулятор использует ряд особенностей интернета как среды обмена информацией и особенностей восприятия человеком информации. Этих особенностей достаточно много поэтому здесь представлены наиболее используемые.

Технологические эффекты

Для реализации информационных операций используется технологические особенности интернета.

1 Скорость распространения информации в интернете максимально возможная, поспорить может только радио и телевиденье. Но они стремительно теряют аудиторию и влияние. Считается, что после нажатия Enter ваша информация становится доступна всему интернету если только не предприняты специальные меры по ее сокрытию.

2 Отсутствие границ и расстояний – в интернете нет традиционного восприятия расстояния. Вы можете одинаково общаться как с соседом по площадке, так и с человеком на другом континенте. И на это никак не влияют границы государств, если только вы не в Китае)

3 Относительная «вечность» хранения информации – есть мнение, что информация, однажды попавшая в интернет, будет «болтаться» в нем пока существует интернет. Опять-же если не были предприняты специальные действия.

4 Анонимность – если говорить об обычном пользователе с минимальными административными и финансовыми ресурсами, то для такого пользователя можно создать неограниченное число суррогатов и сформировать любую иллюзию.

Психологические эффекты

Для осуществления запланированного воздействия на аудиторию в рамках информационных операций используются соответствующие особенности психики человека. Точнее особенности восприятия, обработки информации и принятия решений.

По утверждениям ученых, в ходе эволюции у человека был создан особый механизм быстрого принятия решений в условиях неопределенности. Тот самый механизм, который в течении первой секунды выдает нам мнение о новом знакомом или подсказывает что лучше купить в случае сомнений. Создан был этот механизм в результате постоянного разрешения дилеммы, один из вариантов решения которой приводит к смерти.

Представьте себе первобытного человека, идущего в высокой траве. Вдруг он слышит недалеко от себя шуршание явно не от ветра. У него есть два вариант: либо это животное, которое он может убить и обеспечить себя едой, либо это хищник, который съест его. В зависимости от этого человеку нужно или атаковать или быстро ретироваться. Цена ошибки очень велика, ведь если он подумает, что там хищник, убежит то останется без обеда, но живым. А вот если он посчитает, что там возможная добыча и ошибется, то скорее всего погибнет.

Именно для решения подобных задач в нашем мозгу и был создан механизм быстрого принятия решений в условиях неопределенности. Именно воздействие на этот механизм считается наиболее эффективным с точки зрения манипулирования поведением человека. Если захотите детальнее разобраться в этой проблеме, то рекомендую вам почитать Канемана Даниеля, Дэвида Лейбсона, Черниговскую Татьяну Владимировну.

1 Эффект негатива – в ходе эволюции люди стали больше доверия негативной информации. Хочешь мира – готовься к войне или лучше подготовится к плохому варианту, а он не произойдёт чем наоборот. Поэтому мы охотнее верим негативной информации, а негативный контент воздействует на нас сильнее. Именно поэтому ударный контент чаще всего облекают в негативную форму. Убедить в плохом проще.

2 Хронический страх – страх – одна из самых сильных эмоций. Люди в постоянном состоянии страха быстро теряют способность адекватно воспринимать информацию и логически мыслить. Исходя из этого аудиторию пичкают негативной информацией. В результате аудитория перестает адекватно воспринимать происходящее и легче поддается манипулированию. Для этого и делают посев негативной информации перед вбросом ударного контента.

3 Эффект стадности – какую точку зрения больше всего люди поддерживают, то и правда. А почему? А по тому, что вдруг они что-то знают… Еще, «посев» позволяет, за счёт большого числа публикаций от визуально разных аккаунтов, создать иллюзию, что идею поддерживает большинство в данной социальной группе. В результате реальное большинство, не поддерживающее идею, думает, что оно находится в меньшинстве. И начинает скрывать свое мнение. Толи из страха, толи из стыда…. И идея меньшинства становится преобладающей. Именно поэтому все меньшинства, продвигая свою точку зрения, делают это так агрессивно.

4 «Социальность» информации – у нас больше доверия сообщениям людей, а не информагентств. Просто по тому, что «люди врать не будут». Неподготовленный пользователь, видя такое «общение» предполагает, что реальные люди обсуждают и думает, что они ведь не знают о его существовании. А значит и не планируют им манипулировать. Следовательно им можно верить.

5 Эффект «первого впечатления» – мы больше верим тому, что узнаем первым. А впоследствии это первое впечатление очень трудно вытеснить. Для получения этого эффекта манипулятор старается первым донести информацию до аудитории, чтобы именно его интерпретация первой поселилась в головах аудитории. И тогда эта версия приобретает дополнительную устойчивость в голове объекта манипулирования.

6 На воре и шапка горит – кто оправдывается тот и не прав. Поэтому при отражении информационной атаки оправдания можно использовать только в особых случаях. А манипулятор всеми силами провоцирует вас на оправдание.

7 Клиповость восприятия – современные люди не в состоянии справиться с тем потоком информации, что на них обрушивается. Вспомните как вы читаете новости – вы читаете заголовки и если уж заголовок заинтересовал, тогда только идете по ссылке почитать саму новость. Именно по этой причине появилась технология создания вовлекающих заголовков. Их цель спровоцировать читателя прочесть весь материал, а не ограничится только заголовком.

8 Визуальный контент – у человека больше доверия визуальным образам за счет их двойного воздействия на нас, они наглядны и не требуют слов, которые обрабатываются нашим мозгом медленнее. Кроме того, визуальному каналу восприятия мы доверяем больше по тому, что «видели своими глазами».

Виды информационных операций

Существует несколько основных видов информационных операций:

–Оборонительные;

–Наступательные;

–Информационные операции поддержки;

–Информационные операции стратегического обеспечения.

Кроме того, по масштабам, информационные операции могут быть:

–Локальными (тактическими);
–Оперативными (региональными);
–Стратегическими.

А по задействованным сценариям такие операции делят на:
–Линейные;
–Нелинейные;
–Многомерные.

Оборонительные информационные операции

Оборонительная информационная операция – это действия, направленные на сдерживание противника. Обычно агрессия противника, которую нужно сдерживать, может выражаться в:

–Проведении противником своих информационных операций;
–Наступательных операциях вооруженных сил противника;
–Подрывной и диверсионной активностях;
–Иных агрессивных действиях противника.

Цель информационной операции в обороне заключается в оказании воздействия на целевую аудиторию таким образом, чтобы снизить эффективность агрессии противника, либо сделать ее невозможной, либо подтолкнуть противника к отказу от таких действий:

1. Снижение эффективности наступательных действий противника:
1.1. Формирование у населения противника недоверия к своему руководству;
1.2. Формирование у своего населения неприятия противника;

2. Дезорганизация управления противника:
2.1. Формирование сомнения правильности решений у личного состава вооруженных сил противника и систем госуправления;
2.2. Формирование недоверия у личного состава вооруженных сил противника и систем госуправления;
2.3. Дезинформирование руководства противника;

3. Снижение эффективности информационных операций противника.

В интересах оборонительных информационных операций может осуществляться воздействие на следующие целевые аудитории:

1. Аудитории противника:
1.1. Личный состав войск противника;
1.2. Личный состав штабов противника;
1.3. Гражданское население противника;
1.4. Гражданское население тылов противника если он действует не на своей территории;
1.5. Научное и экспертное сообщество противника;

2. Свои аудитории (обычно с целью противодействия ИО противника);
3. Аудитории заинтересованных стран и/или регионов.

Основным принципом борьбы с информационными операциями противника является усиление медиа грамотности и осведомленности своих целевых аудиторий. В рамках оборонительных информационных операций обычно используют следующие методы:

1. Снижение вероятного влияния будущей информационной операции противника:
1.1. Технические мероприятия:
1.1.1. Пресечение возможности вброса ударного контента;
1.1.2. Пресечение возможности распространения ударного контента;
1.2. Психологические мероприятия:
1.2.1. Формирование невосприимчивости личного состава и населения к ИО противника;
1.2.2. Разъяснительная и воспитательная работа среди населения и личного состава;
1.2.3. Информационные прививки;

2. Нейтрализация уже начатой информационной операции противника:
2.1. Технические мероприятия:
2.1.1. Блокирование распространения ударного контента противника;
2.2. Психологические мероприятия:
2.2.1. Дискредитация ударного контента;
2.2.2. Дискредитация источника и канала доставки ударного контента;
2.2.3. Разоблачение устремлений противника;
2.2.4. Стимулирование невосприимчивости личного состава и населения к ударному контенту;
2.2.5. Разъяснительная работа с личным составом и населением.

Свои силы и средства информационных операций в процессе своей деятельности, помимо прочего, проводят анализ информационной деятельности противника, выявление направлений его интереса и вероятной аудитории возможных информационных операций противника. Используемых им источников для распространения ударного контента и оценки потенциальной эффективности информационных операций противника.

Темы и направленность, содержащиеся в ударном контенте противника, определяются с целью понимания вектора его устремлений и для дальнейшего обоснованного формирования сценария противодействия.

Наступательные информационные операции

Наступательные информационные операции являются элементом в общей наступательной стратегии и могут проводиться во время подготовки наступательных действий, в ходе наступательных действий, или в качестве подготовки к будущим действиям в новых локациях.

Цель наступательно информационной операции заключается в оказании воздействия на целевую аудиторию противника таким образом, чтобы снизить эффективность его оборонительных действий, либо сделать такие действия невозможными, либо подтолкнуть противника к отступлению или сдаче в плен, что может выражаться в:

1. Снижение эффективности оборонительных действий личного состава:
1.1. Формирование у противника нежелания сопротивляться;
1.2. Сомнения в правильности решений руководства (непрофессионализм);

2. Дезорганизация управления противника:
2.1. Формирование у личного состава недоверия к руководству;
2.2. Дезинформирование руководства противника.

В интересах наступательных информационных операций может осуществляться воздействие на следующие целевые аудитории противника:

–Личный состав войск противника;
–Командование противника и личный состав его органов управления;

–Гражданское население противника;

–Научное и экспертное сообщество противника.

Информационные операции поддержки

Информационные операции поддержки предназначены для общей информационной поддержки действий вооруженных сил, поддержки определенных действий вооруженных сил (например операций) и формирования общей позитивной репутации ВС. Осуществляются информационные операции поддержки в координации с теми структурами, чьи действия поддерживаются.

Основной целью информационных операций поддержки являются:

–Формирование доверия к военной политике государства, реформам и эффективности курса в международной политике;

–Формирование общественного мнения по вопросам, касающимся обороны государства, подготовки и применения вооруженных сил;

–Поддержание позитивного имиджа вооруженных сил;

–Облегчение координации между субъектами коммуникаций на всех уровнях управления, синхронизация совместных усилий в интересах целей и задач государства.

В качестве примера – как ЦИПСО проводило информационную операцию поддержки на примере ЗАЭС. Строго по методичкам PSYOP Пентагона. И это не стратегическая операция обеспечения.

Работают по всем основным аудиториям конфликта:

–Нас запугивают ядерной катастрофой, потерей всех территорий вокруг и длительными последствиями.

–У европейцев формируют образ злобных русских, готовых "весь мир в труху".

–У украинцев стимулируют ненависть к России и продолжают развивать проект "анти-Россия".

Используют все возможные каналы доставки ударного контента:

–Традиционно СМИ, соцсети, ТВ и радио в виде новостей, ток-шоу, образовательных программ и т.п.;

–Обзвоном населения с предупреждениями о возможной эко катастрофе;

–Распространением по подразделениям Минздрава инструкций как работать с последствиями заражения территорий;

–Обучением детей в школах азам противодействия радиоактивным угрозам;

–Имитацией учений по обеззараживанию территорий;

–Имитацией подготовки убежищ от радиации;

–Выпрашивание у Европы помощи под это дело;

–Истерики и завывания с разных высоких трибун....

Тезисы данной инфо-операции ЦИПСО:

–«Огромная площадь заражения» – в сети распространяется некая карта зоны радиоактивного поражения, которое якобы случится в случае теракта на ЗАЭС.

–«По Энергодару ездят российские мобильные радиационные лаборатории».

–«ВС РФ разместили взрывчатку на крышах энергоблоков» (эту информацию опровергло даже МАГАТЭ).

–Минздрав Украины распространяет инструкции как защититься от радиации.

–В новостях и ток-шоу рассуждают о последствиях и мерах защиты.

Организация и осуществление информационных операций поддержки, в соответствии с их целью, содержанием и путями реализации, происходит с использованием следующих каналов:

–Публичная дипломатия;
–Связи с общественностью;
–Внутренняя коммуникация;
–Информационная операция;
–Гражданско-военное сотрудничество.

Публичная дипломатия (ПД) является эффективным элементом системы информационных операций поддержки для стимулирования диалога со своей внутренней аудиторией и с международным сообществом.

Использование ПД в системе информационных операций поддержки направлено на формирование и укрепление в информационном пространстве позитивного имиджа страны, повышение доверия к решениям руководства страны со стороны общества и своевременное реагирование на репутационные угрозы руководству страны.

Позитивный имидж является условием результативности ПД, способствует формированию доверия международной общественности и необходимой информационной повестки дня в мировых СМИ.

Публичная дипломатия имеет три направления деятельности:

–Ежедневное общение, направленное на донесение информации о деятельности государства до целевых аудиторий;

–Стратегическое общение, направленное на формирование международной коммуникативной среды и противодействие попыткам подрыва репутации страны и ее руководства;

–Развитие прямых контактов с целевыми аудиториями.

Основными инструментами ПД являются СМИ, международные и национальные неправительственные организации, международные неформальные контакты и обмены, призванные донести необходимую информацию о стране и ее руководстве целевым аудиториям (внутренним и внешним).

–Варианты мероприятий ПД:
–Визиты (дружественные),
–Семинары,
–Конференции,
–Пресс-конференции,
–Общественные дебаты,
–Исследования,
–Публикации,
–Радио-, теле-, кинопродукция и т.д.
–Различные некоммерческие проекты.

Информационные операции стратегического обеспечения

Цель информационной операции стратегического обеспечения заключается в превентивном сборе информации о вероятном противнике, его аудитории, его технологиях, уязвимостях, возможных угрозах и прочих факторах, влияющих на информационное пространство.

Такой подход позволяет повысить эффективность планирования возможных наступательных или оборонительных информационных операций в будущем.

Задачи информационной операции стратегического обеспечения могут быть следующие:

1. Наблюдение за:

1.1. Интересующими локациями (территориями);
1.2. Интересующими ЦА;
1.3. Активностью противника и его ресурсами;

2. Проведение подготовительных мероприятий для будущих информационных операций:
2.1. Изучение аудиторий возможного воздействия;
2.2. Изучение медиа-ландшафта на интересующих территориях;
2.3. Изучение каналов распространения информации в регионах интереса;

3. Осуществление превентивных мер по предупреждению ИО противника:
3.1. Превентивное формирование общественного мнения.

Информационное пространство каждой страны имеет структуру, которая достаточно индивидуальна и зависит от истории развития региона, традиционных и нетрадиционных СМИ, культуры и особенностей общения. С развитием технологий и доступностью к данным информационная среда становится более сложной для анализа и понимания. Все происходящее в физическом измерении информационного пространства всегда имеет эффекты в информационном и когнитивном измерениях.

Типы стратегий информационных операций

По характеру действий стратегии информационных операций могут быть следующие:
–Пассивная оборона;
–Активная оборона;
–Превентивные действия;
–Наступательные действия.

Пассивная оборона подразумевает выявление информационных операций противника и противодействие ее последствиям. По своей сути это реагирование на действия противника и игра по его правилам. Это самый простой способ защиты своего информационного пространства.

Обычно так происходит, когда обороняющаяся сторона не понимает масштабов угрозы информационных операций или не в состоянии организовать более эффективно противодействие деструктивному влиянию.

Активная оборона – выявление информационных операций противника и противодействие им на стадии реализации, что позволяет существенно ослабить запланированное противником негативное влияние на аудиторию по сравнению с пассивной обороной.

Это уже чуть сложнее и требует как понимания основ ифо-пси, так и несколько больших ресурсов для реализации. Но и эффективность такой деятельности выше, чем пассивная оборона.

Превентивные действия – выявление подготовки информационных операций противника и принятие превентивных мер в виде соответствующей работы с аудиторией или с противником.

Это еще более высокий уровень управления информационными процессами, требующий соответствующих компетенций и ресурсов.

Наступательные информационные операции – активное воздействие на информационную обстановку, формирование новостной повестки и манипулирование аудиторией. Может вестись в двух направлениях:

–Выявление уязвимостей своей аудитории и их прикрытие.

–Выявление уязвимостей аудитории противника и их эксплуатация.

Наиболее сложный и требовательный по ресурсам способ работы, но и наиболее эффективный. Его эффективность связана с тем, что вы всегда опережаете противника, заставляя его догонять, реагировать и действовать по вашим правилам.

Структура информационной операции

Любая информационная операция состоит из нескольких элементов, каждый из которых является обязательным для реализации данной информационной операции.

–Составные части информационной операции:

–Целевая аудитория информационной операции;

–Ударный контент;

–Технологии доставки ударного контента и воздействия;

–Используемые для информационной операции площадки.

Целевые аудитории

Целевая аудитория информационной операции – это та часть интересующего нас социума, которая должна совершить целевое действие, планируемое в рамках этой информационной операции.

Целевыми аудиториями информационных операций могут являться:

–Личный состав и командование вооруженных сил противника, его союзников и государств (организаций), которые способствуют ему в осуществлении военных (гибридных) действий против страны;

–Личный состав и командование незаконных вооруженных формирований,

–Лица, привлеченные к содействию функционирования вооруженных сил противника, незаконных вооруженных формирований;

–Политическое руководство противника, представители его органов государственной власти и местного самоуправления, его союзников, государств или организаций, которые способствуют ему в осуществлении его планов;

–Население противника, его союзников, государств и организаций, которые способствуют ему в осуществлении военных его планов;

–Население стран, их руководство, отдельные их представители (как объекты информирования);

–Свое население (как объекты информирования),

–Еще кто-то….

Состав целевой аудитории зависит от специфики информационной операции от целевого действия, до сценария влияния.

Ударный контент

Основным элементом информационной операции является смысл, доносимый до целевой аудитории, как основополагающая идея, призванная обеспечить эмоциональное обоснование определенных действий и, во многих случаях, моральные основания для их реализации.

Смысл (идея) должен охватывать все х членов целевой аудитории, несмотря на географические, языковые или культурные различия. Смысл является основой конструкции «план убеждения» аудитории (сценарий воздействия на аудиторию).

«План убеждения» должен содержать следующее:

–текущее состояние – описание проблемы, требующей решения, или желаемое условие, которое нужно сохранить;

–будущее состояние – описание целей, поддержка текущего состояния или трансформация и т.п.;

–путь – разъяснение, каким образом добиться желаемого результата;

–обоснование – почему предложено изменение состояния или почему поддержка текущего состояния является оптимальной или лучше альтернативных.

План убеждения должен наполнять смыслом ударный контент, создаваемый для данной информационной операции. Ссылаться на имеющийся стратегический нарратив нужно на любом уровне и в любом документе по управлению информационной операцией.

Ударный контент – это контент, используемый для манипулирования целевой аудиторией в рамках конкретной информационной операции.

Ударный контент может быть изготовлен в форме информационного, графического и видеоматериалов или их сочетании, а именно:

–Статьи, публикации и заметки;

–Инфографика, карикатуры, коллажи и т.п.;

–Электронные открытки;

–Радио- и телевизионные сообщения и программы, видео- и аудио- ролики;

–Интервью, репортажи, обращения;

–Записи допроса военнопленных;

–Имитационные и другие аудиозаписи к звуковещательным средствам;

–Сообщения в мессенджерах, СМС-сообщения;

–Электронные письма и т.п.

–Традиционные открытки, буклеты, постеры, газеты, журналы…;

–Сувенирная и рекламная продукция, традиционные письма и т.п.

Технологии доставки ударного контента

Технологии доставки ударного контента до целевой аудитории – это механизмы ознакомления пользователей с ударным контентом с заданными параметрами. Для этого используют самые разнообразные механизмы от слухов до космических каналов связи. В ряде западных источников «технологии доставки ударного контента» называют «каналами доставки ударного контента».

Все доступные каналы доставки ударного контента в информационной операции:

1. Сервисы интернета:

1.1. поисковые системы

1.2. новостные агрегаторы

1.3. сайты СМИ;

1.4. социальные сервисы (соцсети, форумы, блоги…);

1.5. пиринговые сети;

1.6. иные сервисы интернета (доски объявлений, сервисы найма, сервисы хостинга…)

2. Сети мобильной связи и другие информационно-телекоммуникационные системы;

3. Радио, телевидение в т.ч. спутниковое и кабельное;

4. Печатные СМИ и другие «бумажные» информационные ресурсы;

5. Носители внешней рекламы;

6. Агентурная сеть и партизанский движение.

7. Системы воздействия в прифронтовой зоне:
7.1. звуковещательные системы
7.2. агитационные боеприпасы
7.3. ЛА, БПЛА, аэростаты.

Технологии доставки ударного контента в интернете – это технологии, с помощью которых манипулятор имеет возможность продемонстрировать ударный контент целевой аудитории:

–Публикация на площадках, посещаемых целевой аудиторией
–Рекламные механизмы
–Рекомендательные механизмы
–Поисковая выдача
–Посев
–Вирусность контента
–SMM
–Хакерские методы

Площадки интернета

Площадки интернета – это сайты (подсайты, аккаунты…) – используемые в информационной операции для размещения ударного контента. Такими площадками могут быть традиционно используемые для общения (соцсети, форумы, блоги, СМИ…) так и специализированные (сервисы рисования карикатур или мемов, биржи SMM и т.п.).

Методы и технологии информационных операций

Здесь речь пойдет о технологиях, используемых в информационных операциях на разных стадиях для повышения их эффективности воздействия на аудиторию.

Техники манипулирования человеком

Таких манипулирования много, поэтому для погружения в проблематику рекомендую почитать специализированную литературу. А здесь приведены наиболее используемые в информационных операциях приемы манипулирования. Первые семь – самые используемые в информационных операциях.

Дискредитация – это обвинение объекта атаки (мишени) в чем-то. Дискредитация является наиболее часто используемым методом манипулирования аудиторией. При этом само обвинение может быть достоверным, может быть полностью придуманным (фейком), может содержать часть достоверной и часть ложной информации, а может быть в виде намёка. За счет обвинения манипулятор формирует негативное отношение аудитории к Объекту атаки.

Данный приём активно используется в большой политике, когда необходимо обезвредить оппонента, но нет реальной фактуры для атаки на него. В этом случае находят к чему

придраться или имитируют что-то, что не одобряет общество. И выдают предположение, что это «нечто» соответствует действительности, а для усиления эффекта инициируется расследование. Итог расследования всегда один – снятие обвинений. Но общественности достаточно самого факта обвинения, чтобы на всякий случай прекратить любые отношения с объектом атаки.

Так было с Саркози, которого в 2013 обвинили в налоговых преступлениях, а спустя пять лет надзорный суд Милана Берлускони по делу Mediaset полностью реабилитировал, и бывший премьер-министр смог избраться в Европарламент. Так было со Стросс-Каном, когда ему предъявили обвинения в домогательствах к горничной в отеле. Это стоило ему президентского поста. Когда прекратили уголовное дело, было уже поздно на что-то претендовать. Гельмут Коль был вынужден уйти в отставку с поста почетного председателя ХДС в связи с расследованием о незаконном финансировании партии, которые не подтвердились. Франсуа Фийон тоже был выбит скандалом – в 2017 году он стал кандидатом в президенты Франции от правоцентристов, но вся кампания пошла насмарку – на фоне обвинений в фиктивном найме парламентского помощника, собственной жены.

Внушение – это имитация убеждения аудитории в чем-то. Механизм убеждения работает за счет эффекта «привыкания» к ударному контенту. Злоумышленник инициирует массовое «обсуждение» нужной ему идеи (в соцсетях, в СМИ), чаще всего искусственно, но не обязательно. Вначале без нажима и принуждения. Имитируя нейтральное общение по проблеме большого числа аккаунтов.

Такое частое «мелькание» перед глазами аудитории, а заодно выступления «аналитиков», высказывания «авторитетных мнений», споры в ток-шоу и т. д. внушает аудитории нужную злоумышленнику точку зрения. Похоже на многократное повторение как в рекламе, но чуть тоньше.

Эмоциональность – данный метод основан на том, что в состоянии аффекта или эйфории человек делает совсем не то, что в обычных обстоятельствах. И это позволяет подтолкнуть аудиторию к нужному действию.

Злоумышленник провоцирует у аудитории сильные эмоции после чего дает аудитории модулирующую информацию. Чаще для этого используются негативные эмоции так-как их проще инициировать у человека, и они традиционно сильнее влияют на нас, но и позитивные тоже используются хоть и реже.

Ложные авторитеты – люди подвержены влиянию авторитетных личностей. Злоумышленник создает вымышленного авторитета и от его имени распространяет ударный контент. А созданные таким образом «авторитеты» и «эксперты» незаслуженно возвеличиваются, активно продвигается их образ как экспертов, признанных авторитетов в некой предметной области.

Либо используются действительно уважаемые в нужной области знаний люди, имя которых используется для придания значимости распространяемому контенту. Нередко такое использование происходит без ведома самого уважаемого человека.

Замалчивание нежелательной информации – целевая аудитория не видит скрываемую манипулятором информацию, или не обращает на нее внимание (чуть более тонкий механизм). Фрагментация данных (форма замалчивания) – информации подается порционно, частями, не равномерно, что мешает человеку увидеть картину в целом.

Чаще всего данный метод манипулирования мы видим в формате блокирования источников противника в формате лишения лицензии СМИ, выдворения журналистов, а в интернете в форме блокирования нежелательного сайта на территории государства.

Намеренное искажение – предоставление аудитории недостоверной, заведомо ложной, противоречивой информации. Может осуществляться как прямой обман, так и обман в завуалированной форме. Сюда-же нужно отнести использование слухов, домыслов, предвзятых толкований в качестве достоверных фактов и мнений, лже-событий, заказных инфоповодов.

Ложные выводы – нарушение логики рассуждения или подмена логики и фактов идеологическими выводами, лозунгами, призывами, идеями, ведущими аудиторию в нужную манипулятору сторону.

Ярлыки – навешивание ярлыков давно и эффективно используется, чтобы вызвать у целевой аудитории определенное отношение или страх. С помощью этого метода провоцируются выводы, основанные на эмоциях, а не на беспристрастном анализе фактов.

Перенос отношения – качества одного объекта переносятся на иной объект за счет их сравнения, сопоставления или помещения в соответствующее окружение. Именно так происходит негативизация изначально нейтральной новости при помещении ее в окружение из негативных новостей.

Народность или «я свой» – имитация связи с народом – убеждение аудитории в том, что говорящий для них свой – это человек, которому данная публика может доверять. Для этого манипулятор использует в своей речи стиль свойственный данной целевой аудитории.

Частное-общее – формирование обобщающих выводов на основе одного факта. Единичный случай проявление чего-либо называется системой. Обратная техника – искусственное деление единой цепочки событий на отдельные факты и их «оправдание» по отдельности.

Создание ощущения беспомощности – манипулятор искусственно выпячивает негативные новости и события (катастрофы, бедствия, коррупция, войны, эпидемии, преступность), выделяет негативной повестке больше инфо-поля, чем позитиву (часов эфира, первых полос в газетах). У аудитории искусственно формируется ощущение, что она живет в окружении сплошного зла, вокруг только плохое (болезни, войны, страдания, преступность). Это лишает аудиторию воли, желания что-то делать (всё бесполезно, всё зря), делает аудиторию послушной.

Практическое применение техник воздействия

Приведенные выше техники манипулирования используются в соответствующих методах воздействия на аудиторию. Причем нередко в одном ударном контенте задействуется несколько техник одновременно.

Отвлечение внимания – это перевод внимания аудитории на что-то другое. Так уж устроено человеческое внимание, что более привлекательное явление (контент) в данный момент затмит собой всё остальное. В результате скрываемый эпизод (объект) становится менее интересным, на него не обращают внимание и он постепенно вытесняется из области интереса аудитории.

Таким объектом или событием, на которое можно переключить внимание аудитории, может быть:

–нечто более интересное, зрелищное.

–нечто более важное, полезное.

–нечто более смешное, увлекательное.

Отдельно обращаю внимание на технологию использования «второго плана» для оказания воздействия. Ее смысл сводится к том, что лицо второго плана на фото (изображении) мы «замечаем» только когда на него обращают наше внимание. Но вот наше подсознание «видит» второй план сразу и если он например негативен для вас, то происходит неявный «перенос» негативного отношения и на объект первого плана.

Привлечение внимания – обратная задача – привлечение внимания аудитории. Но не просто привлечение, а и провоцирование аудитории на определенные действия через формирование отношения к проблеме.

В одном Российском регионе решили привлечь внимание к выборам молодежной аудитории и использовали провоцирующий контент, играющий на гордыне и сексе с соответствующим визуальным рядом:

–А тебе точно уже можно?

–Это только для взрослых…

–Ты у родителей спросил?

А вот использование ЛОМов (лидеров общественного мнения) – это разновидность данной технологии, которая имеет дополнительны фактор эффективности. Конечно, при условии, если ЛОМа таки удалось спровоцировать на желаемые действия. Так в один прекрасный момент около офиса компании SpaceX американского бизнесмена Илона Маска появились баннеры, приглашающие его принять участие в форуме для малого бизнеса в Краснодаре. Не знаю узнал-ли Илон об этом и если узнал, то как среагировал, но Краснодарские СМИ обсуждали эту новость долго.

Отвлечение ресурсов – создание события (проблемы) или цепочки событий, на которые оппонент вынужден будет отвлечь свои ресурсы и тем самым ослабит свою активность на защищаемом нами направлении.

Дело в том, что ресурсы всегда ограничены, даже у самых богатых, а потому есть возможность уменьшить «силу» информационного воздействия на объект путем стимулирования «генератора негатива» на иную деятельность. Например, на отражение информационной атаки на него или на защиту его подопечного объекта… В зависимости от особенностей такой контратаки, ее результат может быть как локальный, так и стратегический.

Доведение до абсурда – это усиление имеющегося негатива до фантастических и явно не возможных размеров, добавив еще и придуманного вами. И все это подается пользователям со словами на подобии «а еще мы поклоняемся инопланетному дьяволу и едим младенцев…». Присутствие явного бреда провоцирует аудиторию на восприятие и остального негатива как бреда.

Еще один способ доведения до абсурда – это собрать весь негатив об объекте и распространять его меняя имя (название) объекта на другие имена (названия) – любой нормальный чел увидев такое посчитает авторов текстов не совсем нормальными, а материалы – враньем. В том числе и реальные материалы.

RT после обвинений ее сенатом США во всех смертных грехах разместила рекламные баннеры на улицах и в метро Вашингтона и Нью-Йорка с таким содержанием (при переводе на русский язык):

–«Застрял в пробке? Проиграл выборы? Обвини в этом нас!»

–«ЦРУ называет нас «пропагандистской машиной». Узнай, как мы называем ЦРУ»

–«Сыграл на понижение на фондовом рынке и потерял всё. Виноват RT!»
–«Смотри RT, чтобы узнать, кто станет следующей жертвой нашей хакерской атаки».

Модификация – это изменение вектора воздействия контента за счет подмены смысла или его искажения или добавления модифицирующей надписи.

Например, для снижения негативного влияния на внутреннюю аудиторию ярлыка «ватник» его увязали с ватниками, ставшими основой зимней одежды пехоты армии-победительницы в ВОВ, а затем запустили линию модной одежды, стилизованной под ватники. В результате негативное отношение к термину размылось и перестало быть столь сильным как ранее.

Разновидностью модифицирования является визуальное изменение первичного посыла (изображения), лучше в нескольких вариантах, и распространение этих вариантов параллельно с первичным вариантом.

Помните, как по сети начали распространять старое фото нового министра культуры с не корректной надписью на футболке? А чуть позже параллельно пошли те-же изображения, но с другими надписями. Это позволило вначале смягчить негативное восприятие, затем его заменить на юмор и в результате канализировать негодование возбужденной общественности.

Прививка – заблаговременное формирование нужной реакции аудитории на определенный раздражитель. Информационная прививка достаточно действенный способ, основанный на «выработке иммунитета» у аудитории к негативу об объекте, это как приучить аудиторию к тому, что негатив есть, но он ложен.

Достигается такой эффект разными способами. Самый простой – заранее распространить информацию о возможных вариантах негатива с пояснением, что «не разобравшись в проблеме, некоторые люди начинают рассказывают разные небылицы типа этой и вот этой…»

Например, сознание можно привить от воздействия из-вне следующими штампами:
–это мне неинтересно;
–это вранье;
–я все равно в этом ничего не понимаю;
–я все уже про это знаю – и т.п.

Еще несколько распространенных подводок к прививке:
–«По нашим данным противник готовит провокацию…»
–«В августе начнутся вбросы о проблемах в банке Югра…»
–«Власть будет подтасовывать результаты выборов»

Прививать аудиторию можно «в лоб», говоря, что вскорости противник заявит что-то. А можно чуть тоньше – не говоря о возможных действиях противника, а раскрывая информацию, которая опровергнет его будущее возможное заявление.

Троллингом обычно называют некорректное общение, чаще связанное с провоцированием оппонента на необдуманные действия или инициирование ругани, нередко с использованием ненормативной лексики.

Как вариант, это наполнение комментариев всем, чем угодно, но не тематическими сообщениями. Или сообщениями, которые отталкивают нормальных пользователей от чтения. Главное, чтобы эти самые обычные пользователи или не заметили, то, что инициаторы троллинга решили скрыть, или не захотели читать, испытав отвращение к написанному троллями.

Но как можно использовать троллинг в информационных операциях? В данном направлении интересны два варианта действий: продвижение нужного контента (идеи, смысла и т.п..)

с помощью троллинга и недопущение продвижения нежелательного контента. Тогда основные техники троллинга следующие:

–Срач;
–Размытие;
–Провоцирование на ответ;
–Отвлечение внимания.

Срач или инициация ругани используется для создания у пользователя неприятного впечатления от посещения некоего обсуждений. Так поступают с целью скрыть от посторонних наблюдателей опасную информацию. Предположим, некий юзер получил в выдаче поисковой системы по своему запросу ссылку в том числе и на обсуждение некоего поста в соцсети. Значит, предполагает этот юзер, там есть то, что он ищет и перейдя по этой ссылке попадает в комментарии, которые начинает читать, в поисках той самой инфы. Если-же эти комментарии представляют из себя непрерывную ругань с использованием нецензурной лексики, то у нормального человека после прочтения нескольких таких реплик пропадает желание читать дальше. Цель достигнута – пользователь не дошел до скрываемых данных.

Размытие подразумевает наполнение обсуждения всевозможной вспомогательной, комментирующей, параллельной информацией, которая вроде как по теме, но не раскрывает того, что нужно скрыть. Если наполнить комментарии такими материалами на пять страниц, то врядли у кого-то хватит терпения дочитать до скрываемой информации. Как говорят в определенных кругах: на четвертую страницу выдачи ходят только аналитики и боты.

Отвлечение ресурсов оппонента или провоцирование на ответ работает следующим образом. Предположим, что в комментариях к публикации некий персонаж начал распространять нежелательную информацию. Забанить вы его не можете, например, в силу отсутствия модераторских прав. Что делать? Начинаете общаться с персонажем с целью понять его болевые точки (темы на которые он болезненно реагирует). И как только такая тема обнаруживается, начинаете максимально провокационно ее излагать. Противник реагирует, чаще всего бурно, вы поддерживаете этот фонтан красноречия регулярными стимулами. В результате оппонент переключается на оппонирование вам и уже не распространяет нежелательную для вас информацию. Цель достигнута и без бана.

Более мягкий вариант сокрытия целевой информации – это заинтересовать участников общения «родственными» темами или деталями, спровоцировав их обсуждение и отвлекая аудиторию от защищаемой информации. В данном случае неплохо работают всевозможные сенсации, привлекающие внимание, но безвредные для вашей цели.

Например, отвлечь внимание целевой аудитории от рекламы оппонента, лучше если на себя. Ведь если вы вовремя обнаружили в начавшейся рекламе конкурента изъян или иную возможность поучаствовать в общении с аудиторией, то вполне можно начать общение с ЦА используя рекламный инфоповод конкурента.

Многократный повтор – так уж устроен обычный человек, что через 30 минут он помнит только 60% содержания. В конце дня в памяти остается уже только 40%. А в конце недели – 10%. В результате проблема исчезает сама собой в течение 10 дней, если, конечно, она не будет "подогреваться". Вот и «напоминают» человеку с определенной регулярностью то, что по замыслу манипулятора он должен помнить и чем должен руководствоваться в принятии решений.

При таком постоянном мелькании определенного тезиса или бренда перед глазами человека, подсознание последнего в ситуации выбора начинает «предлагать» именно этот бренд, как наиболее «известный» подсознанию и не связанный с опасностью.

Размытие – создание большого количества информации по теме (по ключевым словам). Нейтральной или позитивной. Например, многократное дублирование новостей об объекте. Или новостей об объекте-синониме. Это как размытие в троллинге, но более масштабно – в рамках всего инета, а не одной конкретной публикации в соцсети.

В ситуации размытия удобнее задействовать не свои ресурсы, а спровоцировать пользователей на распространение нужного контента. Именно поэтому размытие часто осуществляется с помощью мемов, демотиваторов, юмора, вирусов и т.п. Ведь стоит только размывающему контенту понравиться публике, и она уже сама его распространит без усилий со стороны манипулятора.

Способы маскировки манипулирования

Для снижения у аудитории недоверия к ударному контенту, обычно скрывают сам процесс манипулирования, маскируя его под некие естественные процессы. Для чего используют соответствующие приемы.

Без маскировки

Ситуация, когда атакующий не предпринимает усилий по сокрытию своих действий. Тут все просто – никакой маскировки, никаких попыток имитировать что-то, материал чаще всего публикуется на только-что созданной площадке (сайте, под-домене…). Это наиболее дешёвый способ, а по тому вполне используемый. Злоумышленник обвиняет Объект атаки во всех смертных грехах, не утруждая себя доказательствами или только намекая на них.

Имитация общения

Это создание видимости общения двух или более людей. Переписка под статусом в соцсети или на форуме, в комментариях блога или в комментариях к статье в СМИ… У прочитавшего создается впечатление «подслушивания». Ведь это общаются люди, которые о существовании его (прочитавшего) даже не подозревают. Ну как они могут им манипулировать? А значит это всё правда.

Срабатывает инстинкт, сформированный эволюцией человека – человек больше доверяет своим родственникам, соплеменникам (вместе было легче выжить), а в расширенном виде – тем, кто ему симпатичен, а в крайнем случае другим людям – это архетип благорасположенности.

Один из пока слабо освоенных вариантов такого «общения» это «общение» в Навигаторе в вашем смартфоне. Вы стоите в пробке и пробуете понять, что там такого произошло и как долго вам еще стоять. Для этого читаете что пишут другие водители по вашему маршруту. И получаете бесценный контент, тревожность, по отношению к которому у вас снижена. А значит такой контент с большей вероятностью будет пропущен вашими фильтрами.

Например «кофе в Бур%@# говно!». «Что за бред» подумаете вы, но ваше подсознание запомнит и в момент выбора в какую кофейню зайти подсунет вам ранее прочитанное.

Символы

Символами в данном случае называются образы, имеющие значение для аудитории в силу воспитания, убеждений, в силу психологических особенностей личности, в силу авторитетности…. Техника такого воздействия основан на созданной ранее ассоциации между самим образом и отношением аудитории к нему. Например, спортсмены ассоциируются у нас с успешностью, с достатком …

Утечка информации

Создание видимости случайной или целенаправленной утечки информации (документа, письма, архива переписки и т.п..) тоже активно используется для маскировки ударного контента. Якобы хакеры что-то украли и выложили. Или неизвестный доброжелатель, видя несовершенство этого мира разочаровался в жизни и решил таким образом восстановить справедливость.

И вот где-то в интернете появляется такая утечка. Пользователи видят это и первое, что подсознание неявно подсовывает пользователю мысль, что раз уж утекло, то видимо не особо беспокоятся о конфиденциальности своей информации, а тем более будут наплевательски относиться и к чужой. Так начинается первичное формирование негативного отношения. Затем пользователь начинает читать утекший материал и вникая в суть написанного усугубляет своё негативное восприятие. А иначе зачем-бы эту утечку организовали?

Отзыв, мнение

Отзывы в самых разных областях пользуются спросом у аудитории в связи с желанием людей воспользоваться чужим опытом и самому избежать возможных ошибок. Злоумышленник, понимая востребованность отзывов, использует их для распространения нужного уму мнения.

Отдельного внимания заслуживают отзывы на Яндекс-картах и Google-картах. Смысл такого подхода заключается в том, что очень часто пользователю нужно найти местоположение интересующей его организации. Удобнее всего это сделать с помощью специализированных сервисов. А найдя искомое, пользователь видит, что он не первый, что уже есть опыт взаимодействия с компанией у других пользователей и конечно-же у него возникает желание обезопасить себя от ошибок, совершенных другими. Это по своей сути стимулирование мнения «я учусь на ошибках других, я умнее других».

Отзывы в закрытых экосистемах (на маркетплейсах) имеют свои особенности, связанные в основном с ограничениями по входу в эти сервисы и ограничения по поводу чего вы можете оставлять отзывы. Но это вполне преодолимо.

Исследования, расследования, опросы

Это набор технологий, мимикрирующей под разные процессы, но использующие один механизм воздействия на аудиторию. Речь об имитации некой общественно-значимой деятельности и под ее видом распространения ударного контента (нарративов) с целью манипулирования аудиторией.

Социологические исследования, как и любые другие исследования, требующие сбора мнений (ответов на вопросы), имеют в себе две возможности для манипулирования общественным мнением:

–Соответствующим образом сформулированные сами вопросы к аудитории – формирующие вопросы;

–«Правильно» оформленные и поданные результаты опроса.

Формирующий (индуцирующий) опрос – форма агитации, замаскированная под социологический опрос общественного мнения. Основное отличие опросов от других форм воздействия – более высокая интенсивность воздействия за счет того, что человеку не «просто попадается на глаза агитационный материал», а человека просят совершить некое действие – подумать над вопросом и дать ответ. Пришла она из западных политических технологий, где известна под названием «push poll».

Интересно, что даже незначительные изменения формулировки вопросов, вызывают разные ответы респондентов и это было не случайным явлением, а системным. Таким образом,

манипулируя вопросом, можно манипулировать и ответами на него и более – формировать мнение участников процесса.

Второй особенностью этой технологии заключается является то, что человек, озвучивший свой ответ, впоследствии крайне неохотно меняет свои взгляды. И, таким образом, его становится гораздо проще склонить к следующим нужным реакциям.

Как повлияла на ваш бюджет новая социальная политика государства?

Планируете ли вы сократить свои расходы в ближайшее время?

Считаете ли Вы, что кандидат Иванов будет хорошим мэром, несмотря на его пристрастие к спиртному?

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, купив полную легальную версию на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.