Методичка инфобойца

Нежданов Игорь

Игорь Юрьевич Нежданов

Методичка инфобойца

http://www.litres.ru/pages/biblio_book/?art=69846271
SelfPub; 2023

Аннотация

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.

Содержание

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 информа-

ционных 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 появ-

лении:

–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. По-

этому 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 воен-

ного 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 принуж-

дения, 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 тех-

нологии (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 геополи-

тические 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 нейтрализа-

ции 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) лично-

го 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 при-

нятия 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 Та-

тьяну 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 на-

ходится 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 на-

селения 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 руко-

водству;

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, ка-

сающимся 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 "антиРоссия".

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 ин-

струкций 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 формирова-

ние 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 мо-

гут 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 удар-

ным 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 негатив-

ное 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 автори-

тетных 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 узнали 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 стимулирова-

ния «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 об-

щественности.

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 извне 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 вряд-ли 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 чело-

век, 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 че-

ловека – 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 ме-

стоположение 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?

«Многоходовые комбинации» это, когда мысль (идея, установка, message) не прямо навязывается в уже законченной форме, а методично, последовательно внедряется в сознание и подсознание посредством «частей/кусочков/элементов» из которых, в дальнейшем сложится нужная, законченная мысль (и восприниматься она будет не как навязанная извне (мысль/идея), а как своя собственная, т.к. сознание человека, в данном случае, само проделает работу по её формированию, хоть и из «подкинутых извне» «частей/кусочков/элементов»).

Еще один механизм влияния опросов на аудиторию – это обнародование результатов этих опросов, но специально подготовленных. В ряде случаев для манипулирования аудиторией даже не обязательно проводить опросы, а достаточно обнародовать придуманные результаты. Тут уже срабатывает механизм стадности. Если большинство поддерживает одного кандидата, а я нет, то я задумаюсь – ведь не может ошибаться такое число людей, а может они знают что-то такое чего не знаю я…..

«Мозговые центры» (Think Tanks) представляют собой как-бы независимые структуры, созданные для сбора, накопления и структурирования знаний, проведения исследова-

ний и объединения профессионалов для решения общих задач. Такие структуры как-бы заполняют вакуум в «серой» зоне – пространстве между академическим миром, с одной стороны, и властью, с другой.

Но в ходе свое деятельности ничто не мешает таким структурам создавать «идеологические правильные» отчеты, прогнозы и с их помощью формировать общественное мнение или ожидания общества. Мало того, материалы из таких источников воздействуют на экспертное и научное сообщество, которое уже непосредственно влияет на выработку решений, в том числе и стратегических.

В целом «мозговые центры» действуют по следующим направлениям:

–Генерируют новые идеи, подходы, варианты решений, а также более глобальные концепции.

–Представляют развившихся в их рядах экспертов для работы во властных структурах.

–Организуют обсуждение наиболее важных вопросов.

–Формируют общественное мнение, используя опросы, отчеты, публикации в СМИ и публичные выступления.

Журналистские расследования также прекрасный способ замаскировать манипулирование аудиторией и придать дополнительную авторитетность ударному контенту. Аудитория по большей части склонна верить в «независимую журналистику», а уж если такой журналист проводит расследо-

вание…. И вот тут у манипулятора открываются дополнительные возможности по воздействию на аудиторию:

–Замалчивание неудобных фактов и выпячивание удобных;

–Особая эмоциональная нагрузка;

–Подача материала в формате предположений, допущений, гипотез;

–Сокрытие источников информации и возможность сослаться на не проверенный источник…

В результате аудитория получает не достоверные данные как того ждёт, а набор предположений и допущений, целью которых сформировать нужное манипулятору мнение.

Обучение это уже процесс формирования в том числе и мнения обучаемых, а уж обучение специально подобранной аудитории, да специфическим темам… Собственно так и поступают всевозможные как-бы меценаты от политики, создавая всевозможные около-образовательные программы и финансируя разработку и издание «правильных» учебников.

А обучать с целью манипулирования аудиторией можно по самым разнообразным направлениям от истории до журналистских расследований с использованием OSINT. А в ходе такого обучения закладывать в головы страждущих идеологически-выверенные нарративы.

Волонтерство, также позволяет воздействовать на мировосприятие участников этого процесса. Например, в ходе помощи бездомным, в головы волонтеров, пока они под воздействием от увиденного, легко можно заложить негативное отношение к власти, которая довела общество до такого….

Технологии доставки ударного контента

Для того, чтобы добиться максимального распространения ударного контента в аудитории, используют соответствующие технологии его продвижения.

Посев

Посев или повторы – многократная демонстрация ударного контента целевой аудитории. Такой прием создает эффект массовости поддержки нужной идеи, в результате конкурирующая идея представляется аудитории неправильной, непрогрессивной, ее представители неявно дискредитируются в сознании аудитории. Осуществляется с помощью многократного дублирования ударного контента. Для этого используются следующие технологии:

–Реклама;

–Репосты ботами, троллями, сторонниками;

–Рекомендательные алгоритмы социальных сервисов;

–Платные публикации в группах, на «стене» авторитетных аккаунтов;

–Распространение по свое «сетке» источников.

Реклама – конечно-же для распространения ударного контента используются механики распространения рекламы. Эти механики изначально предназначены для распространения манипулирующих материалов, только укладывающихся в понятие «реклама» и адаптированы под решение задачи донесения до ЦА.

Контекстная реклама в поиске

Контекстная реклама – тип интернет-рекламы, при котором рекламное объявление показывается в соответствии с содержанием, выбранной аудиторией, местом, временем или иным контекстом интернет-страниц. Т.е. пользователь ввел поисковый запрос в поисковую строку Яндекса (или Google, или еще какого поисковика) или перешел на сайт содержащий определенный контент, и ему показали рекламу, соответствующую контенту этой страницы. Другими словами, эта реклама зависит от «контекста», демонстрируемого пользователю.

Используются и механизмы контекстной рекламы в поисковых сервисах от глобальных до локальных. Ведь пометка «реклама» в поисковой выдаче плохо видна, а рядовой пользователь часто эту пометку не замечает и с большей вероятностью кликает на то, что вверху страницы поисковой выдачи.

Баннерная реклама

И баннерная реклама тоже используется для распространения ударного контента. Правда у современного человека выработалась баннерная слепота и об эффективности данного способа продвижения можно поспорить.

Баннерная реклама – это вид объявлений на сайте в виде баннера. Подразумевает продвижение товаров или услуг при помощи изображений, но в редких случаях используется «голый» текст. Баннер (англ. banner «транспарант») – графическое изображение рекламного характера, аналогичное рекламному модулю в прессе.

Тизерная реклама считается родственной баннерной. Она используется для увеличения посещений сайта с пиратским контентом, чтобы продать исцеляющие от всех заболеваний средства и многое другое. Для нее важны яркие заголовки и броский дизайн, который нельзя не заметить. Если соблюсти это правило, то реакция пользователей будет сопоставима реакции на желтую прессу.

Реклама в виде всплывающих окон тоже считается родственной баннерной. Недобросовестные вебмастеры используют ее, чтобы помешать закрыть страницу. Но при ненавязчивом использовании она действительно снижает показатель отказов и повышает вовлеченность.

Таргетированная реклама

Таргетированная реклама – это онлайн-реклама, в кото-

рой используются настройки поиска целевой аудитории в соответствии с заданными параметрами (характеристиками и интересами) людей, которые могут интересоваться рекламируемым товаром или услугой. «Таргетированная» – это реклама по определенному «таргету», т.е. определенному набору характеристик пользователя, которому ее нужно продемонстрировать. Допустим женщины старше 24 и младше 50, проживающие в определенном регионе и интересующиеся кошками.

Таргетированная реклама в социальных сервисах не менее ценна для распространения ударного контента, где в вашу френдленту подмешиваются проплаченные рекламодателем материалы.

Репосты

Имитация массового распространения ударного контента ботами, троллями, чаще нанятых на биржах или с использованием своих бото-ферм. Смысл такого действа сводится к имитации интереса аудитории к распространяемому контенту.

Рекомендательные алгоритмы

Это то, какой контент социальный сервис предлагает вам исходя из предположения, что это вас может заинтересовать. Основывает свои предположения такой алгоритм на данных о ваших предпочтениях и на ваших действия в социальном

сервисе.

Арбитраж трафика

Арбитраж трафика или партнерский маркетинг – это система, основанная на привлечении внимания пользователя с помощью партнера (специализированного сайта), его трафика и перенаправление пользователей на целевую (посадочную) страницу.

Всех интернет-пользователей, которые посещают определенный сайт, называют трафиком, который можно измерить за определенный отрезок времени: час, день, неделю или месяц. Источником такого трафика может быть любой платный или бесплатный ресурс, с которого пользователь приходит, обычно по ссылке. Например, другой сайт, блог, социальная сеть, прямая ссылка, контекстная реклама и т. д.

Тогда арбитраж трафика – это процесс привлечения трафика на сайт путем его закупки в одном месте и перенаправления в другое. Простыми словами, это перепродажа трафика – перепродажа тех интернет пользователей, которые зашли на сайт арбитражника. Специалист, который занимается этим, называется арбитражником.

Партнерская сеть – это сервис, размещающий у себя рекламные предложения (офферы) и обеспечивающий взаимодействие между рекламодателями и партнерами.

Есть 6 видов арбитража трафика:

–прямой – пользователь вручную набирает адрес ресурса;

–органический – посетители приходят со страницы выдачи поисковой машины;

–реферальный – переходы из приложений и мессенджеров;

–платный – пользователи приходят на сайт после клика по контекстной или таргетированной рекламе (таргете);

–трафик из соцсетей – это VK, FB, Twitter;

–неопределенный – темный трафик, природу которого сложно определить.

SMM

«Социальный» разгон контента – привлечение внимания аудитории к распространяемому контенту за счет инструментов соцсетей и провоцирование реакции аудитории. Но вначале давайте разберемся как распространяется информация в социальной сети.

Если вы делаете публикацию у себя на странице, то ее увидят ваши френды в своей френдленте. Но если кто-то из ваших френдов прокомментировал, репостнул или лайкнул вашу публикацию, то она отображается во френдленте его друзей, как и в случае если он сделал репост. Частота показов зависит от частоты и объема этих лайков и комментариев. Поэтому каждое действие очередного френда с вашей публикацией значительно расширяет охват публикации – видимость другим людям. Это очень упрощенная схема, но она позволяет понять, как это происходит.

Вопрос в том, как получить больше лайков, репостов, комментариев от своих френдов? Для этого нужно сделать контент интересным для френдов. Привлекательным, полезным, смешным…. Это называется органическая накрутка.

Органическая «накрутка» лайков, репостов, комментариев может быть осуществлена с помощью простых действий. Далее расскажу о некоторых из них подробнее. Вот наиболее используемые:

–Использование чужого инфоповода;

–Использование тегов;

–Использование соревновательности;

–Провоцирование.

Использование чужого инфоповода

Смысл данного приема сводится к тому, что наиболее обсуждаемая в данный момент новость привлекает внимание максимального числа людей. Поэтому если показать аудитории что-то об этой новости, то внимание аудитории обеспечено. Далее, эксплуатируя это внимание нужно дать аудитории уже продвигаемый вами контент.

Для начала ищем наиболее обсуждаемые сейчас новости-публикации. Чтобы найти такие популярные в данный момент новости можно воспользоваться бесплатными сервисами от Медиаметрикс или от БрендАналитикс.

Далее «привязываем» по смыслу к ним свой ударный контент. В идеале это должно быть логично и осмысленно, но

если не получается привязать по смыслу, то не комплексуем, а берем часть обсуждаемой новости и приклеиваем к ней нужный нам текст без какого-либо перехода. И такую сборку публикуем.

Использование тегов

Использование тегов неплохо работает в соцсети Илона Маска и соцсети Цукерберга для обмена фотографиями и видео. В других соцсетях теги менее эффективны. Смысл данного механизма в том, что при поиске по тегу ваш материал будет демонстрироваться ищущим и в случае проявления интереса к определенному тегу, в ленту интересующегося подмешиваются публикации с этим тегом. В результате число просмотров публикации возрастает. А если используется популярный или набирающий популярность в данный момент тег, то число просмотров, а значит и охват, возрастает значительно.

Если решили использовать эту технику, то смотрим какие теги сейчас популярны и добавляем их в свою публикацию. Но тут проблема с целевой аудиторией. Ведь нужно подобрать тег, который интересен вашей ЦА. Можно ограничить популярные теги только определенной территорией, других вариантов таргетинга нет. Это несколько усложняет использование тегов для продвижения.

Провоцирование

Дословно с латинского слово “провокация” переводится как “вызов”. Провокацию еще можно назвать хорошо продуманным и целенаправленным раздражителем, пробуждающим в людях определенные эмоции и чувства и толкающим их на необдуманные поступки. В нашем случае провоцирование – побуждение аудитории к действиям или выводам, нужным манипулятору.

Провокация воздействует на то, что нам важно. На наши глубинные убеждения и ценности, привитые с детства. Именно поэтому провокация работает так хорошо. Поскольку ценности и убеждения очень важны для нас, то провокатор очень легко достигает своей цели – мы, как правило, реагируем очень эмоционально. А, эмоции, в свою очередь, не дают возможности мыслить и действовать рационально. Таким образом, делая интервенцию, провокатор вызывает сильный эмоциональный отклик, сужающий наше сознание до уровня автоматического поведения по защите ценности или убеждения, на которые идет атака.

Разновидность провоцирования – это провоцирование соревновательности у аудитории или «засорялочка». Соревновательность как качество личности – склонность проявлять ревностное стремление превзойти, отличиться в каком-либо деле, на каком-либо поприще. По своей сути это эксплуатация гордыни у человека.

Подталкивание читателей на соревнование между собой за приз, который может быть банальными деньгами, неким

предметом, похвалой или победе в соревновании. Наверняка вы сталкивались с такими публикациями:

–«Чей коммент последний – тому достанется приз!»

–«Чей коммент продержится 10 минут без лайка – тот получит подарок»

–«Какая кличка у вас была в детстве?»

–«Что вам должны написать, чтобы вы забанили?»

–«Кто согласен – жми лайк, кто нет – репост!»

Посев в соцсети

Как и в остальном интернете, посев в соцсетях это многократное обнародование однотипной информации. Но в соцсетях есть несколько способов осуществить такое распространение.

Публикация на странице аккаунта (на стене) – прямая публикация чтобы видели френды.

Публикация в группе – публикация материала в группе или в паблике с интересующей аудиторией. В данном случае публикацию увидят участники группы.

Публикация в комментариях – если публикация в группе запрещена или по другим этическим соображениям делать прямую публикацию нельзя, то можно взять уже имеющуюся публикацию в группе и в ее комментариях сделать свой вброс. Желательно чтобы «материнская» публикация подходила хоть немного по тематике.

Рассылка в личных сообщениях френдам или участникам

интересующей группы распространяемого материала. Порой такой посев является более действенным, хотя и более трудоёмким.

Активность вокруг сообщения

Активность вокруг продвигаемой публикации основывается на специфике работы рекомендательных механизмов – чем больше пользователей как-то отреагировали на публикацию, тем шире круг лиц, которые увидят ее в своей френдленте.

Речь идет о лайках, репостах, комментариях. Поэтому подталкиваем пользователей к взаимодействию с продвигаемой публикацией всеми уместными способами, в том числе не забывая о визуальности контента. И используем своих ботов для накрутки лайков, комментариев и репостов.

Паблики

Создание под продвигаемый контент специализированных страниц в соцсетях открывает еще ряд возможностей по продвижению материала, в том числе и продвижению средствами рекламы этой соцсети. Такими страницами в соцсети могут быть:

–Персональные страницы;

–Паблики;

–Группы;

–События – особый тип страницы в соцсетях.

У каждого из перечисленных вариантов есть свои плюсы и минусы, которые нужно учитывать при планировании продвижения. В группах проще организовать общение и с его помощью продвигать свою точку зрения. Контент пабликов удобнее рекламировать встроенными в соцсеть инструментами. События имеют уникальный формат, ориентированный именно на распространение информации о событиях. Персональные страницы с большей эффективностью позволяют создать иллюзию общения с известным персонажем и использовать его авторитет.

Реклама в соцсетях

Продвижение материала в соцсетях можно и нужно осуществлять и с помощью рекламных механик как самой соцсети, так и внешних сервисов. Внутренние инструменты соцсети это рекламный кабинет.

Реклама через специализированные биржи – это покупка размещения нужного вам контента на стенах, в пабликах или в группах выбранных вами исполнителей.

В некоторых случаях можно использовать косвенное рекламирование. Например, вы проводите некое мероприятие по популяризации вашего продукта. Это мероприятие открытое, в парке, с раздачей призов, но вас никто не знает и на ваше имя не придет много зрителей. Рекламу про вас давать бессмысленно. Что делать? Некоторые особо продвину-

тые идут на обман пользователей. Они дают рекламу неких придуманных интересных мероприятий в том-же месте и в то-же время, что и основное, на которое нужно заманить народ. Выступление известных музыкальных коллективов, общение с интересными людьми, детские развлекательные мероприятия, раздача книг или еще чего-то….. Главное привлечь внимание, заманить как можно больше людей и дать им продвигаемый контент. Чаще всего это используют для проектов с коротким жизненным циклом в сочетании анонимностью таких умельцев. Им не важны долгосрочные последствия – они их не должны коснуться, по их мнению.

Обращение к ЛОМу

Помимо перечисленных техник, позволяющих усилить распространение контента, есть один специфический прием, связанный как с особенностями алгоритмов соцсетей так и с особенностями психики человека.

Обращение к бренду или персоне – упоминание его аккаунта в соцсети в своем сообщении с использованием, например знака @. Если это бренд, то для него это дополнительный повод напомнить о себе, а для вас – втянуть в общение сторонних людей. Если это персона, особенно персона скандальная, то это провоцирование на перепалку, которая также втянет в охват и аудиторию этой персоны. В результате такого поста или комментария с обращением вы получаете значительный охват с минимальными затратами.

Вирусный контент

Вирусным обычно называют контент, который пользователи хотят распространять и распространяют «по велению души». Срабатывает фактор новаторства или хвастовства. Человеку хочется выделится, хочется одобрения и он старается его получить разными способами, в том числе распространяя чужой контент. На эксплуатации этой особенности человека и построена вся технология создания и распространения вирусного контента.

Чаще всего пользователи хотят поделиться контентом если:

–Этот контент привлекает внимание (неординарностью, красотой…);

–Контент может чему-то научить или помочь;

–Может развлечь;

–Вызвать сильные эмоции.

Необычные объявления

Самый простой «шаблон» – это необычные объявления данные на Авито или на НН или на других специализированных сервисах. Они всегда привлекают внимание вначале по тому, что выбиваются из общего ряда однотипных объявлений. А затем, по тому, что развлекает читающего и провоцирует распространение объявления. Например, поиск необычного сотрудника (астролога для предсказаний

итогов переговоров).

Необычное название

По-разному можно назвать магазин (продукт, услугу, товар, свой офис…). Иногда названия придумывают необычные, иногда их заведомо делают провокационными, но в любом случае это привлекает внимание как минимум. Помните «ЁбиДоёби»?

Чужой инфоповод

Чужой яркий инфоповод один из самых простых способов добавить вашему контенту ускорения и спровоцировать его самораспространение за счет реакции аудитории. Это достигается по средством того, что вы присоединяетесь к теме, заведомо интересной аудитории.

Провоцирование

Один из самых распространенных приемов создания вируса это провоцирование аудитории на нужную реакцию и нужные манипулятору действия. Например, абсурдные судебные иски провоцируют вначале журналистов написать об этом как о чем-то странном, необычном, а затем уже пользователей соцсетей посмеяться над убогим. Но именно это и нужно провокатору – чтобы материал с его упоминанием обсуждали, дублировали, распространяли, а вместе с этим поднимали узнаваемость. Скандал пройдёт и забудется, а участ-

ников запомнят.

Иногда провокация бывает пожестче. Одна авиакомпания устроила акцию, в рамках которой у россиян будет возможность купить 200 тысяч билетов по ценам от 499 до 1999 рублей. Распродажа стартовала 12 августа и из-за наплыва посетителей сайт авиакомпании слетел. Спустя пару часов его подняли и на главной странице появилась очень неоднозначная реклама билетов в город Нальчик, обыгрывающая название города Нальчик: «А Нальчик?».

«Мученик»

Если нужно продвинуть никому не интересную тему, то манипулятор может прибегнуть к такому способу привлечения внимания и распространения контента как «борец за права» или против чего-нибудь, особенно против власти или конкретного чиновника. Любят наши люди разного рода мучеников и жертв. Собственно это и использует манипулятор в разных форматах. Можно взять публикацию в местной газете, тему которой нужно разогнать, и развернуть вокруг неё скандал на предмет требований со стороны ответственных товарищей удалить эту публикацию. Уже на этом этапе к публикации проявят интерес. А уж если дойдет до судов, публичных заявлений и оскорблений, то это гарантированно выведет данную статью в самые читаемые. Ну и апофеоз привлечения внимания – разные протестные мероприятия от голодовок до митингов.

Хак-достава

Данное понятие объединяет разные способы продемонстрировать целевой аудитории нужный манипулятору контент, но с использованием технологий или инфраструктуры киберпреступников.

Взлом – Для придания «веса» новости и снижения порога тревожности у аудитории иногда используют взломанный аккаунт человека или организации, являющихся реальными авторитетами в нужной предметной области. В этом случае злоумышленник получает большую аудиторию, так-как у таких аккаунтов как правило много френдов, аудитория профильная. Плюс пользователи думают, что получают контент от известного им персонажа, мнению которого доверяют и с большей охотой поглощают фейк.

Взламывают информационные системы или системы, имеющие возможность информировать клиента о чем-то, и доставка ударного контента до целевой аудитории с их помощью.

Зловреды – Последнее время довольно все чаще используют специально созданные вредоносные программ – зловреды для распространения ударной информации. Таких технологий продвижения несколько:

–подмена выдачи браузера жертвы, например, при отоб-

ражении результатов поисковой выдачи в Яндексе, Google и т.п.;

–подмена контента в новостных агрегаторах, установленных на устройстве жертвы;

–скрытая установка на ПК жертвы нужного для распространения манипулятивных материалов софта и распространение этих материалов от имени жертвы или использование прокси-сервера на девайсе жертвы для сокрытия следов злоумышленника;

–червь для распространения материалов в мессенджерах, который «ходит» по контактам пользователей мессенджера и оставляя у каждого заранее подготовленное сообщение.

Так для распространения ударного контента с устройства жертвы использовались: Shopper (Android-троян), Faketoken (Android-троян).

Дефейс – Взлом сайта оппонента и подмена содержимого первой страницы на специально подготовленную, пропагандистскую. Такая подмена может носить скрытый или явный характер. Скрытую подмену используют в основном для дезинформрования или разового вброса манипулятивной информации. А явную для прямой дискредитации Объекта атаки.

Так, летом 2020 официальный сайт Президента Армении взломали. На головной странице армянского появилось ви-

део с выступлением Алиева, фотографии азербайджанских солдат и фраза "Карабах – это Азербайджан".

Киберсквоттинг – это создание доменных имен созвучных или полностью повторяющих подделываемый. Например известную торговую марку, бренд, название, имя и т.д.. И распространение с их помощью манипулирующей информации.

Именно по причине визуальной схожести написания домна они вызывают больше доверия у аудитории и порог ее тревожности снижается.

Созвучные домены – Злоумышленники покупают доменные имена, созвучные с названием жертвы или с доменом жертвы. Часто от оригинала они отличаются одним, реже двумя символами (Adidas – Abibas или disneyland и disneiland). Используют их для введения в заблуждение пользователей и выманивания денег имитируя какую-то активность.

Визуальная имитация – Схожее направление – это создание сайтов визуально имитирующих сайт известной организации с целью получения логинов и паролей. Домен в данном случае не обязательно должен быть очень похож на оригинал. Достаточно общей похожести, ведь на такой ресурс заманивают жертву по ссылке.

Использование чужой инфраструктуры

Это использование для продвижения ударного контента уже готовой, кем-то созданной инфраструктуры, изначально не предназначенной для решения таких задач.

Самый простой способ использования чужой инфраструктуры – покупка на соответствующих биржах в DarkNet взломанных аккаунтов или групп в соцсетях с набранной аудиторией и от их имени распространение ударного контента.

Посложнее – использование сервисов рассылки рекламы для распространения ударного контента в специфических группах мессенджеров (мамочки, соседи…). Распространение ударного контента через сервисы отзывов тоже способ эксплуатации чужой инфраструктуры в интересах информационной операции. Подключение к открытым web-конференциям по любым темам и распространение ударного контента.

Википедия

Википедия давно уже стала площадкой продвижения идеологии, и способов продвижения своих нарративов там несколько.

Создание новых статей по темам вашей информационной операции с соответствующим перекосом в изложении. Иногда статьи публикуются с запретом на корректировку, иногда

создаются заранее под будущее событие.

Корректировка уже существующих статей, так или иначе связанных с темой вашей информационной операции с соответствующим перекосом в изложении.

Правки и провоцирование «обсуждения» чьей-то статьи и предложение аудитории ударного контента в процессе этого обсуждения – «война правок».

Игры

Игры также активно используют в целях информационных операций. Причем возможностей для манипулирования в игре несколько:

1. Реклама в игре:
1.1. Традиционная реклама;
1.2. Нативная реклама;

2. Общение в игре:
2.1. В самой игре;
2.2. На форумах игры;

3. Игровая атмосфера:
3.1. Игровые персонажи, объекты, техника…;
3.2. Сюжет игры;
3.3. Введение, вступление, игровая энциклопедия.

Петиции

Сервисы подачи петиций так-же неплохой способ разгона ударного контента, так-как при правильной подготовке и поддержке позволяет привлечь внимание значительной аудитории и сформировать впечатление массовости сторонников или противников темы.

ПЛАНИРОВАНИЕ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ

Информационные операции имеют несколько этапов (набор обязательных действий), отсутствие или изменение которых может привести к снижению эффективности всего мероприятия. Поэтому с разной степенью детализации каждый этап присутствует в любой серьезной информационной операции. Далее разберем каждый из этих шагов.

Общая организация работ

Для начала несколько слов о важности скорости в информационных операциях. Средний «жизненный цикл» ударного контента в интернете колеблется от 6 часов до пяти суток. Это то время, которое проходит от момента его публикации до падения интереса аудитории к контенту. Из этого времени наиболее эффективный период для нейтрализации воздействия контента на аудиторию составляет первые 1-3 часа. Это время уходит у злоумышленника на первичное распространение ударного контента, которое обычно осуществля-

ется за счет суррогатов. Поэтому воздействие на аудиторию минимальное.

Именно этот период (1-3 первых часа) и нужно использовать для эффективного противодействия информационной операции противника. И исходя из этого строится и тактика реагирования на информационную операцию:

Вам необходимо как можно быстрее обнаружить потенциально-опасную публикацию;

Вам нужно в течении максимум трёх часов определится с потенциальной опасностью контента, выработать сценарий противодействия, согласовать его с руководством и начать реализацию этого сценария.

Для быстрого обнаружения ударного контента противника нужно:

–Мониторинг сообщений об Объекте должен идти 24/7;

–Возможность быстрой адаптации мониторинговой системы под изменение интернета (новые источники, новые технологии доставки ударного контента…).

Для оценки, принятия решения и начала противодействия в течении этого-же периода (1-3 часа) необходимо:

–Доступность лица, согласовывающего активные мероприятия 24/7;

–Заранее проработанные наиболее вероятные сценарии противодействия под разные, наиболее вероятные, тактики противника;

–Заранее подготовленный контент под наиболее вероятные варианты информационных операций;

–Заранее подготовленная инфраструктура распространения вашего контента.

Все это требует определенных ресурсов, соответствующей выстроенной инфраструктуры и отлаженной систем управления и взаимодействия. С другой стороны, при планировании своих информационных операций, необходимо учитывать способность противника быстро и эффективно противодействовать нашим информационным операциям – то, как у него выстроена система выявления, противодействия и какова скорость реакции. По сути это оценка того времени, которое будет у вас для реализации своих задумок до момента, когда противник начнет вам активно мешать.

Функции и структура подразделения ИО

Для понимания какие сотрудники нужны и в каком количестве, нужно оценить объем и сложность работ. Так вот подразделение информационных операций в рамках своих компетенций должно решать следующие задачи:

1. Проведение оборонительных информационных операций:

1.1. Выявление информационных операций противника;

1.2. Оценка опасности информационных операций противника;

1.3. Выработка сценария противодействия информационным операциям противника;

1.4. Реализация сценария противодействия;

2. Проведение наступательных информационных операций:

2.1. Определение цели, задач и возможных ограничений планируемой информационной операции;

2.2. Определение целевой аудитории и ее уязвимостей;

2.3. Выработка сценария воздействия;

2.4. Создание инфраструктуры под операцию;

2.5. Реализация сценария воздействия

3. Проведение информационных операций поддержки:

3.1. Определение стратегии поддержки и ее особенностей;

3.2. Определение целевой аудитории и ее особенностей;

3.3. Разработка сценария воздействия;

3.4. Реализация сценария воздействия;

4. Проведение информационных операций стратегического обеспечения:

4.1. Отслеживание потенциальных угроз;

4.2. Подготовка для возможных информационных операций;

4.3. Превентивные мероприятия по предупреждению возможных информационных операций противника.

Для решения этих задач подразделение информационные операции должно иметь следующие функциональные службы:

1. Служба мониторинга – сбор информации по всем направлениям
1.1. Аналитики сбора (лингвисты)
1.2. Операторы сбора

2. Аналитическая служба
2.1. Аналитики
2.2. Сценаристы
2.3. Переводчики

3. Служба контента
3.1. Отдел текстового контента
3.2. Отдел визуального контента
3.3. Отдел видео-контента

4. Служба распространения
4.1. Операторы распространения
5. Служба поддержки
5.1. Аналитики интернет-технологий
5.2. Лингвисты

Проведение информационных операций рано или позд-

но привлечет внимание противника, и он попробует проникнуть внутрь такой структуры технически или через агентуру. Поэтому помимо традиционных управленческих систем также нужна и система обеспечения безопасности, в том числе и контрразведывательная.

Подготовка информационной операции

Планирование информационных операций заключается определении цели информационной операции, описании действий по достижению этой цели и необходимых для этого ресурсов.

В ходе планирования необходимо решить следующие задачи:

–Целеуказание – формулируем цель информационной операции и задачи в рамках достижения этой цели;

–Определение ЦА, с чьей помощью будет достигнута цель операции, на которую будет воздействие;

–Выявление уязвимостей аудитории – изучить эту ЦА, определить ее восприимчивость, ее уязвимости;

–Определение общей стратегии и сценария воздействия на аудиторию;

–Формирование плана распространения ударного контента;

–Определение показателей эффективности воздействия

на аудиторию.

Далее каждый пункт описан детально в разделе «Планирование информационных операций».

Что нужно учитывать

В ходе планирования информационной операции и необходимых ресурсов учитываются множество факторов, каждый из которых мы разберем. А для понимания масштабности работ вот перечень наиболее значимых из них:

1. Сопротивление противника в инфо-пси сфере:

1.1. Активность силовиков в интернете (цензура, свои ИО, расследования…);

1.2. Усилия «активистов» в интернете (выискивают, жалуются, атакуют…);

1.3. Наличие у противника специализированных сил выявления операций противника и скорость их работы;

2. Особенности целевой аудитории:

2.1. Степень приятия продвигаемой идеи в ЦА (согласие, нейтрально, неприятие);

2.2. Степень тревожности ЦА;

2.3. Особенности восприятия ЦА (язык, ЛОМы, склонности…);

2.4. Доступность ЦА в интернете;

3. Кто планирует информационную операцию (исполнитель или заказчик):

3.1. Адекватное целеуказание;

3.2. Подбор ЦА;

3.3. Сценарий воздействия на ЦА;

3.4. Темник ударного контента;

3.5. План информационной операции;

4. Степень маскировки информационной операции:

4.1. Легендирование (свои аккаунты, чужие, свежеугнанные…);

4.2. Маскировка управления процессом (прямое, прокси, транс-граничное…);

4.3. Метод маскировки воздействия на ЦА;

5. Технологии доставки ударного контента до ЦА;

6. Сам ударный контент:

6.1. Кто создает (заказчик или исполнитель);

6.2. Объемы ударного контента;

6.3. Опасность ударного контента для государства ЦА.

7. Интенсивность ИО:

7.1. Планируемый охват ЦА;

7.2. Сколько раз продемонстрировать ударный контент;

7.3. Как долго показывать ударный контент;

8. Вариативность ИО:

8.1. Число внутренних сценариев воздействия в рамках одной ИО;

Сопротивление противника в инфо-пси сфере

Это набор факторов, связанный с действиями, которые предпринимает противник в области инф-пси для недопущения воздействия на свою аудиторию. Ведь совершенно разные усилия и ресурсы нужны для воздействия на аудиторию если никто не контролирует контент в инфополе, действия пользователей, их общения, никто не говорит им об опасностях, не пугает страшными новостями…. И иные усилия потребуются для воздействия на аудиторию, которую жестко контролируют в плане того, какой контент аудитория получает, что и кому говорит, какие темы обсуждают, и об этом контроле аудитория знает и подвергается регулярному «воспитательному» воздействию в плане разъяснений что можно, а что нельзя. Тут уже придется предпринимать значительные усилия для преодоления систем противодействия противника, тревожности аудитории и отторжения ею определенных нарративов.

Обычно в данной области следует учитывать:

–Наличие цензуры в интересующем сегменте интернета и ее механизмы;

–Законодательство в данной области и активность его

применения;

–Воспитательно-образовательные усилия государства по интересующей аудитории;

–Проводимые противником информационные операции по интересующей аудитории;

–Наличие и активность неформальных и негосударственных структур и объединений, ратующих за чистоту контента в интернете;

–Наличие активистов и волонтеров, предпринимающих усилия по очистке интернета от опасного контента;

Особенности целевой аудитории

Не менее важным фактором являются и особенности аудитории, выбранной в качестве мишени для воздействия. Такими особенностями являются:

1. Присутствие аудитории в интернете и на планируемой для воздействия площадке;

2. Степень приятия аудиторией используемого для воздействия нарратива (идеи) (согласие, нейтрально, неприятие);

3. Уровень общей тревожности аудитории;

4. Особенности потребления информации аудитории:

4.1. язык аудитории, сленг, предпочтения по подаче информации (аналитика, публицистика, юмор, инфографика…);

4.2. предпочтения по типу информации (текст, звук, кар-

тинка, видео…);

4.3. визуальные предпочтения (приятные-неприятные образы, цвета, сюжеты);

4.4. предпочтения по источникам и авторам, на чье мнение ориентируются…

На основе данной информации формируется рекомендация по созданию ударного контента для данной аудитории.

Необходимость и степень маскировки информационной операции также оказывают серьезно воздействие на необходимые ресурсы. Согласитесь, одна ситуация, когда не нужно тратить силы и средства не сокрытие процесса воздействия на аудиторию и совсем другая ситуация, когда необходимо скрывать всё:

–Необходимость маскировки всей информационной операции или ее отдельных элементов;

–Необходимость легендирования своих аккаунтов, найма и использования чужих;

–Маскировка процесса управления операцией, что подразумевает использование прокси серверов, шифрования, «ретрансляторов» команд и т.п.;

–Маскировки собственно воздействия на аудиторию, придания этому процессу вида общения, утечек, мнения авторитетных людей и т.п.;

Также нужно учитывать особенности самой информационной операции:

–Прямое воздействие (без маскировки);

–Воздействие от чужого имени;

–Неявное воздействие.

Технологии доставки ударного контента до ЦА

То, каким способом планируется доставлять ударный контент до целевой аудитории, также сильно влияет на необходимые для реализации ресурсы. Есть существенная разница между разовой публикацией в одном паблике соцсети и посевом от сотен разных аккаунтов в нескольких соцсетях. И эта разница может оказывать значительное влияние на эффективность всей информационной операции.

Сам ударный контент

То, какой ударный контент используется в рамках информационной операции также влияет на необходимые ресурсы в случае, если ударный контент создается вами. Для придумывания текста в одно предложение нужен один объем ресурсов, тогда как для создания сложного часового видео-ролика нужен совсем другой объем ресурсов.

Мало того, токсичность ударного контента прямо влияет на два показателя:

–То, как ЦА будет его воспринимать и сколько понадобится ресурсов для убеждения;

–То, как государство будет реагировать на распространение такого контента.

Интенсивность информационной операции

Не менее важна для расчета ресурсов и интенсивность информационной операции, то есть ее продолжительность, сколько раз ударный контент должен быть продемонстрирован аудитории и размер этой аудитории.

В зависимости от токсичности среды проведения планируемой информационной операции и ее сценария можно обойтись одним аккаунтом, а может понадобиться несколько тысяч. Во втором случае добавляются проблемы управления и координации действий задействованных аккаунтов.

Вариативность самой информационной операции

Вариативность информационной операции – это то, какое число разных сценариев воздействия на аудиторию используется в рамках данной информационной операции. От этого зависит и число необходимых аккаунтов, и число единиц уникального ударного контента.

Но начинается всё с разведки, которая в рамках информационных операций осуществляется с помощью мониторинга открытых источников интернета.

Кто и на каком этапе информационной операции участвует

При планировании и расчёте ресурсов важно еще понимать кто осуществляет каждый этап информационной операции от целеуказания до реализации (исполнитель, заказчик, внешний подрядчик). Точнее кто тратить свои ресурсы на осуществление каждого действия:

1. Общее планирование

1.1. Адекватное целеуказание – точная и понятная постановка задачи;

1.2. Подбор целевой аудитории, ее изучение и выявление уязвимостей;

1.3. Формирование сценария воздействия на аудиторию;

2. Подготовка инфраструктуры воздействия;

2.1. Темник для ударного контента;

2.2. Создание самого ударного контента;

2.3. Подготовка инфраструктуры распространения;

3. Реализация воздействия

3.1. Распространение

3.2. Контроль эффективности

И какие инструменты, какие ресурсы и в каком количестве нужны исполнителям для осуществления каждого действия.

Мониторинг

При проведении информационных операций важнейшим направлением становится наблюдение за меди-активностью как противника, так и своей. По сути, мониторинг становится разведкой в интересах того, кто осуществляет информационную операцию. Поэтому на том, как осуществлять эффективный мониторинг инфополя остановимся отдельно.

Мониторинг необходим для решения целого спектра задач:

–Выявление угроз как текущих, так и потенциальных;

–Определение целевой аудитории для воздействия;

–Выявления особенностей и уязвимостей целевой аудитории;

–Отслеживание реакции аудитории на распространяемый ударный контент;

–Отслеживание противодействия противника вашей операции.

Подробнее о организации мониторинга написано в разделе «ПРАКТИКУМ» – «Мониторинг». В данном разделе приведен необходимый минимум по вопросу.

Проблемы мониторинговых систем

К сожалению, у сбора информации (мониторинга) есть ряд особенностей, которые прямо влияют на эффективность сбора информации, и на применимость мониторинга для решения тех или иных задач.

Ловушка размерности – Все существующие на рынке мониторинговые системы традиционно попадают в ловушку размерности. Это связано с несколькими факторами. Дело в том, что уже сейчас объемы нового контента огромны и с каждым днем этот объем только увеличивается. А мониторинговая система должна всё это собирать. Мало того, собирать быстро – чтобы заказчик, в идеале, видел нужный ему контент в момент его публикации. Для решения этой задачи нужно очень большая и разветвленная инфраструктура, которая стоит очень дорого и требует много денег и сил для поддержания ее в рабочем состоянии.

И вот тут начинается борьба между трусостью и жадностью, в том смысле, что собрать всё мониторинговая система не может себе позволить. И ей приходится выбирать что собирать, а что нет. Выбор по понятным причинам падает на ресурсы, которые обычно называют более авторитетными или более влиятельными. В самом простом понимании это ресурсы с наибольшим охватом. И это без учета, что до некоторых данных мониторинговая система дотянуться не может. Не по тому, что пароль для доступа или в TOR-е, а по тому, что, например, контент только появился на недавно зарегистрированном ресурсе и на него не ведет ни одна ссылка.

В результате мониторинговая система «видит» не всё, что появляется в плане контента в открытом доступе, а только часть и не всегда в «увиденном» находится то, что нужно для

решения вашей задачи.

Не менее интересным является и то, как мониторинговая система препарирует собранные данные. В смысле что считает и как показывает пользователю. Обычно это статистический анализ: чего, когда, в каком количестве, где и в каком виде публиковалось. Этого не то чтобы мало для определения есть атака или нет, а вообще никак не помогает для ответа на данный вопрос. Ведь что такое атака на репутацию в интернете? Это искусственное распространение нежелательного контента. Именно искусственное. По тому, что естественное распространение – это обычно недовольство клиентов. В общем все эти красивые графики не позволяют сказать есть атака или нет. И тем более не позволяют разобраться в особенностях атаки. Понять задействованные силы, оценить масштабы и примерные затраты на организацию атаки, определить используемые приёмы и как развивалась атака.

Активное противодействие – На эффективность организации мониторинга влияет активное противодействие противника в формате маскировки, дезинформирования и «борьбы с русскими троллями», в рамках которой им (противником) проводится работа:

–По выявлению возможных мероприятий влияния со стороны России;

–По выявлению инфраструктуры влияния;

–По блокированию источников (в т.ч. аккаунтов), задействованных в распространении «Российской пропаганды».

Это подразумевает необходимость предпринять усилия по сокрытию следов работы системы и вытекает в дополнительные условия по ее анонимности.

Масштабы планируемой ИО

Неопределенность в масштабах будущих информационных операций выражается в следующем:

–Заранее неизвестно в каких локациях понадобится работать в будущем;

–Заранее неизвестно с какими языками придётся работать;

–Заранее не известно с какими социальными сервисами (в т.ч. соцсетями) придётся работать;

–Заранее неизвестно с какими объемами ударного контента понадобится работать в будущем.

Это подразумевает соответствующие требования к инфраструктуре, к аппаратным мощностям создаваемой системы и к возможностям её адаптации.

Технологические ограничения

Есть ряд специфических ограничений, связанных с особенностями осуществляемых действий и среды функционирования – технологические ограничения:

–Число поддерживаемых системой аккаунтов для разных

сервисов (суррогатов);

–Число площадок (сервисов), доступных системе для активной работы;

–Число одновременно ведущихся операций по поиску и по сбору информации и их интенсивность;

–Число пользователей, одновременно работающих с системой;

–Число стран (территорий), где планируется ведение информационных операций и соответственно поддерживаемых языков.

Мало того, создание и поддержка пула аккаунтов для поиска и сбора информации требует предварительной проработки следующих вопросов:

–В каких сервисах планируются работы;

–Сколько активностей в сутки планируется;

–На сколько «токсичный» контент;

–Какие схемы анонимизации и имитации человекоподобия планируются;

–Какие технологии продвижения (разгона) использовать;

–Кто и как будет поставлять аккаунты для активных мероприятий.

От этого зависит сколько аккаунтов, в каких соцсетях и какого качества нужно иметь в оперативной доступности, сколько в резерве и сколько новых нужно будет периодиче-

ски добавлять в систему для поддержания требуемого уровня работоспособности.

В каких соцсетях планируется работать – каждая соцсеть (сервис социального взаимодействия) имеет ряд своих особенностей, которые могут значительно отличаться и это тоже необходимо учитывать:

–Набор доступных пользователю функций в каждой конкретной соцсети;

–Связанность соцсети с госструктурами и подконтрольность им;

–Уровень русофобии администрации ресурса и страны;

–Терпимость основной массы пользователей к контенту не соответствующему их взглядам.

От этого зависит какие затраты необходимы направить на решение задач:

–Анонимизации и поддержки человекоподобия аккаунтов;

–Маскировка воздействия и адаптация контента под особенности аудитории и среды распространения;

–Доступ к разным механизмам распространения ударного контента в каждом конкретном социальном сервисе.

Сколько активностей в сутки планируется – имеется ввиду сколько обращений к сервисам по поиску и по скачиванию в сутки нужно инициировать. Например, несколько обраще-

ний от одного аккаунта уже достаточный повод для блокировки такого аккаунта администрацией сервиса.

На сколько «токсичный» контент планируется к поиску и сбору – на сколько контент опасен с точки зрения «власти» той страны, где планируется поиск и сбор. Если контент опасен, то аккаунты, которые его ищут и скачивают быстро попадут в поле зрение госорганов и будут удаляться администрацией соответствующих сервисов, или будет организована оперативная игра, например по дезинформированию. А значит необходимо контролировать «незасвеченность» используемых аккаунтов и нужна будет регулярная замена этих аккаунтов на новые, а это дополнительные затраты на их закупку и адаптацию.

На сколько хорошо должен быть легендирован сам аккаунт и совершаемые им действия. Данный параметр зависит от закрытости сервиса, где планируется поиск и сбор. Так для попадания в закрытую часть форумов обычно необходимо активное и полезное общение на форуме или рекомендация от уже проверенного участника форума.

Отдельно вопрос в том, кто и как будет получать аккаунты для поиска и скачивания с соцсервисов. С учетом того, что и нужно много и периодически аккаунты будут банить по подозрению и без оного. Поэтому нужно постоянно пополнить их парк.

Варианты получения аккаунтов:

–Самостоятельное создание и развитие аккаунтов;

–Покупка аккаунтов на торговых площадках в ДаркНет;

–Аренда чужих аккаунтов напрямую или через биржи.

–Самостоятельная регистрация, наполнение и развитие требует много ручной низкоквалифицированной работы, а значит и затрат времени, затрат на сим-карты и их поддержку и девайсы для подтверждения аккаунтов и фонд оплаты труда.

Покупка аккаунтов на торговых площадках в ДаркНет предполагает решение вопросов с ОРД так-как речь идёт о взломанных аккаунтах.

Аренда аккаунтов на биржах сопряжена с риском утечки информации так-как администрация таких бирж особого внимания безопасности данных клиентов не уделяет. Кроме того, большинство таких бирж в рунете имеет украинские корни. Другое дело если создать свою подконтрольную биржу и развить ее, тогда кроме доверенного сервиса по найму аккаунтов еще появляется источник информации о планируемых манипулятивных проектах.

Нет устойчивого контентного признака информационных операций – вброс (первичная публикация ударного контента) это не обязательно ложная информация – фейк. Для вбросов используют и достоверную информацию как ударный контент, и реальную информацию с вкраплением дополнительных данных, и полностью искусственно сгенери-

рованную информацию. Поэтому наличие лжи или иного манипулирования нельзя использовать как достаточный признак вброса. Как и наличие в контенте признаков манипулирования аудиторией вовсе не является достаточным признаком для утверждения, что контент используется противником для соответствующего воздействия на аудиторию.

Невозможность контролировать работу рекомендательных алгоритмов – для принудительного распространения ударного контента в масштабных информационных операциях используются рекомендательные алгоритмы крупных социальных сервисов. Такое решение принимается на уровне менеджмента данных площадок. А отслеживать такую активность без доступа к серверам соцсети очень затратно. Даже если вы создадите аккаунты в целевой соцсети со всеми возможными характеристиками защищаемых ЦА (метод ловушек), всё равно есть вероятность пропустить какой-то ударный контент например по причине особых требований к ЦА у противника или появление интереса противника к новой (неожиданной) ЦА в силу выработки новой стратегии воздействия.

Необходимо быстро выявлять новые аккаунты – для вброса ударного контента нередко используется только-что созданный аккаунт, который мониторинговые системы на начальном этапе «не видит». Поэтому если идти по пути мони-

торинговых систем начало вброса будет пропущено (не вовремя выявлено). Скорее всего будет выявлено искусственное продвижение ударного контента. И то при условии, что задействованные в продвижении аккаунты отслеживаются мониторинговой системой. Исходя из этого важным становиться быстрое выявление новых аккаунтов в отслеживаемой соцсети.

Этому мешают:

–Закрытость экосистемы соцсетей;

–Борьба с «русскими троллями» в ряде популярных соцсетей;

–Огромные масштабы «пространства» интернета, которое нужно держать под наблюдением;

–Неопределенность будущих угроз.

Закрытость экосистемы соцсетей – специально предпринимаемые самой соцсетью усилия по ограничению индексирования поисковиками, отсутствие эффективного внутреннего поиска, сложность получения и использования API, а в ряде случаев жесткие ограничения в использовании API за исключением пары Российских соцсетей.

Борьба с «русскими троллями» выражается в дополнительных ограничениях, накладываемых на пользователей из России или продвигающих про-Российский контент, отказе в регистрации и использовании API и блокировании таких аккаунтов по малейшим подозрениям или незначительным

«жалобам».

Зачем нужен мониторинг

Для эффективного мониторинга нужно очень четко представлять для чего он вам нужен. И вот тут нередко возникает определенное недопонимание. Наиболее частый ответ «чтобы отслеживать упоминания объекта». Это далеко не всё, что нужно для эффективного нейтрализации инфо-операций противника, и тем более для эффективной реализации своих. Мониторинг инфополя вам нужен для того, чтобы вовремя, а лучше заранее, обнаружить потенциальные угрозы защищаемому Объекту и вовремя обнаружить возможности для защищаемого Объекта.

Цель мониторинга: собирать информацию, необходимую для своевременного выявления возникающих угроз, открывающихся возможностей и для их исследования. В нашем случае в разрезе информационных операций противника.

Задачи мониторинга:

1. По угрозам

1.1. Собрать информацию, позволяющую своевременно выявлять:

1.1.1. Угрозы Объекту защиты

1.1.2. Изменения у целевой аудитории

1.1.3. Изменения у противника

1.1.4. Чужие информационные операции

1.2. Собрать информацию, позволяющую выявлять информационные операции по Объекту

1.2.1. Подготовку к инфо-операциям

1.2.2. Начало инфо-операций

1.3. Собрать информацию для изучения ИО

1.3.1. Отслеживания информационных операций противника

1.3.2. Выявления ресурсов противника

1.3.3. Понимания тактики и стратегии противника

1.3.4. Определения новых технологий, приёмов, механизмов воздействия

1.4. Собрать информацию для понимания тенденций в инфопси

1.4.1. Исследования

1.4.2. Новые технологии и приемы

1.4.3. Новые коалиции и группы влияния

1.5. Собрать информацию для выработки стратегии, тактики своих информационных операций

1.5.1. Защищаемые ЦА, их свойства и уязвимости

1.5.2. ЦА противника, их свойства и уязвимости

1.5.3. Свои ресурс, технологии и возможности

1.5.4. Ресурсы противника, его технологии и возможности

2. По возможностям

2.1. Собрать информацию, позволяющую своевременно выявлять

2.1.1. Гео-политические возможности
2.1.2. Научно-технологические возможности
2.1.3. Рыночные возможности
2.1.4. Военные возможности

Выявление угроз

Под угрозами Объекту защиты обычно понимают следующие:

1. Угрозы нормальному функционированию Объекта
1.1. Угроза управлению
1.2. Угроза репутации
1.3. Угроза ресурсам

2. Угрозы существованию Объекта
2.1. Угроза целостности Объекта
2.2. Угрозы автономности Объекта
2.3. Угроза независимости Объекта (суверенитету)

В зависимости от особенностей Объекта эти угрозы могут меняться по своему составу. Так «Угроза управлению» для государства это практически вся его система управления от системы выборов до системы принятия решений и передачи управляющих сигналов по бюрократической лестнице. А вот для частного лица этот блок сужается до структуры воспринимаемой ею информации и особенностей влияния на данное лицо другими.

Выявление возможностей

Под возможностями необходимо понимать всё то, что позволяет вам эффективнее или быстрее достигать своих целей. В некоторых случаях это в принципе новые возможности в том числе и в новых направлениях. Это могут быть изменения в структуре управления противника или появление новой уязвимости у защищаемой им аудитории или новая технология доставки ударного контента, еще не известная вашему противнику.

Возможностью для Объекта может являться то, что является угрозой для противника или некая особенность целевой аудитории. Это значит, что могут быть сообщения и без прямого упоминания вашего Объекта.

Противник тоже наблюдает

Ваши действия, если они будут достаточно эффективны, то обязательно спутают планы оппонента и он захочет реванша. В больших проектах в подобные атаки могут быть вложены значительные суммы и противнику будет очень жаль, что он их потратил просто так. Противник обязательно попробует восстановить контроль над ситуацией или банально отомстить. Такие действия могут проявляться по разному. Например:

Взлом сайтов (нужны копии информации и зеркала сайтов);

ДДОС атака (нужны зеркала и обузоустойчивые хостинги);

Физическое воздействие (нужна анонимность действий).

Или еще как-то, ведь изобретательность человеческая безгранична.

Чем мониторим

Организовать мониторинг можно вручную, если вы (или защищаемый объект) не слишком медийный, т.е. число новых его упоминаний в сутки не превышает сотни. Но уже в этом случае нужно будет тратить некоторое время на сбор и прочтение материалов. Сам же сбор можно организовать с помощью поисковых систем (Яндекс, Google). Один раз сформировав качественный запрос, чтобы свести информационный мусор в выдаче к минимуму, этот запрос сохраняете в виде закладки и при необходимости активируете.

Вручную – Самый простой способ мониторинга – вручную. Просматривая новости или ища нужную информацию в поисковых системах.

О том как правильно использовать поисковые системы, в том числе как правильно составлять сложные поисковые запрос, подробно рассказано в разделе «ПРИЛОЖЕНИЯ» – «Сбор информации» – «Ручной поиск информации».

Дзен.Новости (бывший сервис Яндекс.Новости)

Для наблюдения за ситуацией и ее изменениями можно использовать новостные сервисы, которые специализируются на агрегировании новостей. Например, такие как Дзен.Новости (бывший сервис Яндекс.Новости). https://dzen.ru/news

Сервис позволяет вести поиск нужной информации по 6887 СМИ (на 2023 год) и новостным агрегаторам, данные из которых очень быстро становятся доступны в поиске.

Самый простой способ – внести в поисковую строку запрос и получить ответ, который можно просмотреть, перейти на первоисточники и прочитать информацию в них.

Кроме того, можно сохранить ссылку на результаты поиска по интересующей теме в виде закладки. И таким образом сформировать небольшую библиотеку готовых запросов. В дальнейшем достаточно одного клика чтобы открыть актуальные новости по проблеме.

Полуавтомат – Современные решения позволяют пользователю частично автоматизировать процесс мониторинга без необходимости разбираться в программном коде или в сложных настройках систем.

RSS-ридеры

RSS-ридер – это интернет-сервис, десктопная программа, мобильное приложение или расширение браузера, где RSS-ленты из разных источников собираются, обрабатываются и

в едином формате представляются читателю.

Примеры RSS-ридеров (их гораздо больше):

–Feedly
–NewsBlur
–Inoreader
–The Old Reader
–rssLounge
–Selfoss
–Feed on feeds
–Managing news
–Lilina
–Tiny Tiny RSS
–ZebraFeeds
–Rnews
–NewsBlur

Бывает, что интересующий вас источник не имеет RSS-потока. В этом случае можно воспользоваться сервисами генерации RSS лент из интересующих источников:

–RSS.app,
–FetchRSS,
–mySitemapGenerator,
–PolitePol.

Таким образом можно организовать свою систему наблюдения определенных тем, событий или новостей в популяр-

ных поисковиках или настроить сбор появления всех записей от необходимых СМИ.

Google Alert

Полностью бесплатный и простой в использовании сервис. Что можно сделать с помощью Google Alerts по умолчанию:

Проводить простой мониторинг ключевых слов в блогах, на форумах, новостных сайтах и на YouTube (так как он принадлежит Google).

Настроить частоту отслеживания упоминаний – раз в неделю, раз в день или в режиме реального времени.

Просматривать уведомления внутри сервиса или настроить их отправку на почту.

Для работы в сервисе зарегистрируйтесь или авторизуйтесь в Google и перейдите по ссылке https://www.google.ru/alerts Перед вами откроется главная и, по сути, единственная страница сервиса с настройками:

Для того чтобы создать новое оповещение, введите запрос, который планируете отслеживать. Далее переходите к его настройкам.

Частота отправки. Эта настройка доступна только при выборе способа доставки по почте. Есть 3 варианта

–по мере появления результатов;

–не чаще, чем раз в день;

–не чаще, чем раз в неделю.

Первый вариант удобен для репутационных запросов, когда важна мгновенная реакция администрации. Для информационных запросов подойдет второй или третий вариант.

Источники. По умолчанию здесь стоит «Автовыбор». Но вы можете сузить круг отслеживания до новостей, блогов, видео и т. п.

Язык. Вы выбираете язык результатов поиска. Можно задать «Все языки» или только какой-то один.

Страна. Как и в случае с языками, вы выбираете все страны или интересующую вас.

Количество. Можно мониторить все результаты или только самые качественные.

Далее нажимаем «Сохранить». Новое оповещение появится в списке:

Есть дополнительные настройки (открываются по клику на значок шестеренки) можно:

–указать время отправки уведомлений

–задать отправку в виде сводки (одним письмом по всем оповещениям).

Каждое оповещение можно редактировать и удалять при необходимости.

Использование RSS читалки

После преобразования оповещения в ссылку на RSS-ка-

нал вы увидите значок RSS рядом с ним в разделе «Мои оповещения».

Кликните значок правой кнопкой мыши и выберите «Копировать адрес ссылки», чтобы скопировать URL-адрес RSS-канала в буфер обмена. Перейдите к любому RSS-ридеру, который вы используете, вставьте URL-адрес и добавьте оповещения Google в свой ридер.

Вы можете создать сколько угодно RSS-потоков по интересующим вас темам и читать их в вашем RSS-ридере.

Автоматизация с помощью Google Таблиц

Компания cloudHQ представила расширение для Chrome, позволяющее экспортировать письма в Google Таблицы, в том числе и оповещения Google Alerts (Export Emails to Google Sheets by cloudHQ). https://chrome.google.com/webstore/detail/export-emails-to-google-s/ibpbagbedfnlepijbnjeanihpoohkocm

Такой отчет будет автоматически обновляться при поступлении новых уведомлений. Кроме того, в нем содержится подробная информация по каждому оповещению:

–Дата и время упоминания ключевого слова

–Само ключевое слово Google Alerts (что означает, что их может быть несколько)

–Издатель контента

–Резюме содержания

–Ссылка на содержание

–Ссылка для публикации в соцсетях
–Ссылка для пометки оповещения как не релевантного
–Колонка для личных заметок

Создание отчета бесплатно. Таким образом, используя Google Alerts в связке с расширением cloudHQ можно получать данные об упоминании интересующего объекта или темы в удобной форме, и при этом сэкономить много времени и ресурсов.

Мониторинговые сервисы

Можно задействовать для мониторинга онлайн сервисы, которых немало. У такого способа есть свои преимущества. Первое – вам не нужно тратить время на сам процесс сбора – это всё сделают за вас. Второе – весь объем собранного всегда доступен вам из любого места, лишь бы был интернет.

Но есть и недостатки. Админы мониторинговой системы знают направление вашего интереса и у вас нет полной уверенности, что вам отдают весь контент по вашей тематике. Мало того, нужно всегда помнить о возможной связи мониторингового сервиса с вашим противником.

Подготовка на перспективу

Для решения задач предупреждения информационных операций противника необходим несколько иной подход. Нужно выявлять не начало информационных операций, а

признаки подготовки к информационной операции или возможности для проведения информационной операции с точки зрения противника.

В частности, нужно отслеживать и заранее выявлять:

–Уязвимости своей аудитории или ее элементов и их изменения;

–Уязвимости аудитории противника и ее изменения;

–Проявления интереса противника или иного субъекта к нашей аудитории;

–Подготовку к проведению информационной операции против нашей аудитории;

–Подготовку к проведению новой информационной операции противником;

–Изменение на в регионах интереса, могущие привести к информационным операциям.

Анализ информационной среды (анализ медиа-пространства) – процесс сбора и обработки информации о совокупности информационных ресурсов, информационной инфраструктуры, системы общественных коммуникаций, их сильных и слабых сторонах (уязвимых) для организации и проведения информационных операций.

Анализ информационной среды является решающей задачей для поддержки национальных стратегических целей. Это способствует достижению целей информационного противоборства вообще и конкретных информационных опе-

раций в частности. Вовремя понять уязвимость аудитории, сформировать под эту уязвимость ударный контент и донести его до аудитории, получить и проанализировать обратный отклик – главная задача, которую решает система стратегического мониторинга.

В процессе своей повседневной деятельности орган, занимающийся информационными операциями, осуществляет непрерывный мониторинг информационного пространства установленных зон ответственности и сопредельных зон, обеспечивает постоянную ситуационную осведомленность по этим направлениям, которая включает в себя:

1. Выявление стратегических угроз и их изменений;

2. Изучение стратегических угроз:

2.1. Целевой аудитории (особенностей, восприимчивости, уязвимостей);

2.2. Противника (сил, средств, приемов работы);

2.3. Особенностей инфо-пространства (источники, канал распространения, ЛОМы, специфичность контента…);

2.4. Общей ситуации (участники, центры влияния, конфликты, тенденции);

3. Выявление изменений по направлениям стратегических угроз:

3.1. У целевой аудитории;

3.2. У противника;

3.3. Инфо-пространства;

4. Выявление инфоповодов по направлениям стратегических угроз;

5. Накопление примеров чужого ударного контента;

6. Планирование возможных сценариев воздействия по направлениям стратегических угроз.

Оценка вызовов и угроз в информационной сфере – это детальное изучение информационного пространства с целью выявления, идентификации информационных угроз, возможных источников и методов их реализации с использованием определенных критериев (признаков).

Угрозы в информационной сфере классифицируются по направлениям:

1. Внешние негативные информационные влияния на сознание целевой аудитории через СМИ и Интернет, осуществляемые в ущерб государству и имеющие целью:

1.1. Попытки изменять психическое и эмоциональное состояние человека, его психологические и физиологические свойства;

1.2. Разжигание межрелигиозной, межэтнической и межнациональной розни, ненависти по этническим, языковым, религиозным и другим признакам;

1.3. Распространение призывов к сепаратизму, свержению конституционного строя или нарушению территориальной целостности государства;

2. Информационное влияние на население, в том числе на личный состав военных формирований, мобилизационный резерв с целью ослабления их готовности к обороне государства и ухудшению имиджа военной службы;

3. Распространение субъектами информационной деятельности искаженной, недостоверной и предвзятой информации для дискредитации органов государственной власти, вооруженных сил, дестабилизации общественно-политической ситуации, что значительно усложняет принятие политических решений, наносит ущерб национальным интересам или создает негативный имидж страны.

К общим признакам информационных вызовов и угроз следует отнести:

–Исключительно негативный характер тональности сообщений, чрезмерную детализацию и эмоциональность сообщений о негативных событиях, произошедших в стране;

–Плановость в предоставлении новостей по негативным тематикам;

–Увеличение интенсивности информационных сообщений по конкретной тематике (направлению) за короткий

срок;

–Манипуляция информацией, касающейся страны, ее органов власти и ее вооруженных сил и направленной на сознание общества, отдельных групп общества и личностей.

В ходе анализа информации нужно четко определиться на какие вопросы мы хотим получить ответы? Что мы хотим узнать в результате анализа? В общем виде это вполне очевидно:

–Что произошло или происходит?

–Какова опасность происходящего или какие возможности дает?

–Что делать чтобы было не так больно или как воспользоваться ситуацией?

Если же говорить предметно, то обычно нужно выявлять угрозы и их изменение, открывающиеся возможности и их изменение. Что касается угроз, то они могут сильно отличаться в зависимости от сферы ваших интересов. Но одна угроза важна для всех – это угроза репутации. И в рамах работы с этой угрозой мониторинг и анализ должны дать аналитику возможность автоматизировать следующие процесс:

–Выявление подготовки к атаке на репутацию;

–Выявление самой атаки на репутацию;

–Исследование инцидентов с репутацией.

Для общего понимания происходящего можно использовать трёх-шаговую схему анализа, в ходе которой вы последовательно отвечаете на три вопроса по поводу новой информации или потока информационных сообщений:

–Что произошло или происходит;

–Какова опасность происходящего или какие возможности дает;

–Что делать чтобы было не так больно или как воспользоваться ситуацией.

Что произошло или происходит – Для понимания что происходит нам как минимум нужно разобраться в том, на сколько искусственен изучаемый информационный процесс распространения информации. Применительно к распространению негативной информации это понимание того, что информация распространяется реальными пользователями и процесс носит естественный характер или информация распространяется искусственно, а за процессом стоит заказчик, оплачивающий весь этот театр. В зависимости от этого набор применимых инструментов будет разный.

Какова опасность происходящего или какие возможности дает – Не менее важно вовремя оценить потенциальную опасность происходящего или примерные возможности, которые нам дает судьба. По сути своей это прогнозирование, но в нашем случае – прогнозирования влияние на аудиторию распространяемого контента. Это оценка влиятельно-

сти контента, пластичности аудитории и скорости распространения ударных материалов.

Что делать чтобы было не так больно или как воспользоваться ситуацией – И третьей задачей является выработка вариантов дальнейших действий в связи с выявленными процессами. Для негативных процессов – как уменьшить негативное влияние на аудиторию. Для позитивных – как усилить позитивное влияние.

Выявление информационной операции

Первая проблема, которую надо решить – понять есть информационная операция или нет. Ведь это умышленное действие по распространению информации, это искусственный процесс, а например, обсуждение пользователями интересной новости с вашим упоминанием это не атака, это естественный процесс. А для снижения нежелательного влияния в ситуации искусственного разгона ударного контента можно и нужно использовать технологии не приемлемые в ситуации, когда идет естественное распространение контента.

Для информационных операций характерны некоторые особые свойства, по сочетанию которых атаку можно идентифицировать. Эти признаки относятся к трем направлениям:

–Особенности оформления источника, осуществившего вброс;

–Особенности контента вбрасываемой информации;

–Особенности распространения вброшенного контента.

И именно анализ по всем этим направлениям дают возможность точнее определять наличие вбросов.

Детальное описание признаков информационной операции:

1. Особый первоисточник вброса:

1.1. Источник, имитирующий известное СМИ, новостное агентство и т.п.;

1.2. Недавно созданный источник, например аккаунт в соцсети;

1.3. Аккаунт, обладающий признаками бота;

2. Отсутствие первоисточника:

2.1. В публикациях нет ссылок на первоисточник;

2.2. Ссылка на первоисточник битая (первоисточника нет или он удалён);

2.3. Ссылка на первоисточник ведёт совсем не туда;

3. Искусственное продвижение:

3.1. Продвижение (репосты, комментарии, лайки…) осуществляют боты, тролли, агрегаторы компромата или сливные бачки;

3.2. Высокая скорость дублирования распространяемого контента вплоть до нескольких публикаций в секунду;

4. Специфичный контент – ударный контент:
4.1. Крайне эмоциональный контент;
4.2. Контент содержит призывы;
4.3. Контент обладает признаками манипулирования;
4.4. Контент вводит в заблуждение.

Особый первоисточник вброса

Площадка для первичной публикации ударного контента обычно выбирается из числа тех, которые некритично относятся к содержимому публикуемого материала. В противном случае злоумышленник рискует не осуществить задуманное. Таковыми являются следующие типы площадок:

–«Сливной бачек» сайт, готовый за деньги опубликовать что угодно;

–Только-что созданная площадка;

–Площадка, имитирующая известную (обычно известные СМИ);

–Боты в соцсетях.

Крайне редко для первичной публикации ударного контента используются известные, авторитетные площадки вплоть до сайтов крупных международных организаций или аккаунтов руководителей транс-национальных корпораций. Это происходит в следующих случаях:

–Сайт или аккаунт взломали и осуществили вброс;

–Договорились с админом ресурса, который без ведома владельца опубликовал.

Отсутствие первоисточника

Автор не указывает ссылку на первоисточник или ссылка не открывает ничего (ошибка 404) или ссылка открывает что-то не по теме. В ряде случаев это связано с тем, что страница первичной публикации ударного контента намеренно удаляется злоумышленником после осуществления первичного распространения для сокрытия следов.

Искусственное продвижение

Для достижения нужного эффекта злоумышленник предпринимает усилия по искусственному распространению ударного контента. Это подразумевает использование специфических технологий по распространению ударного контента уже вброшенного в медиа-пространство.

Такие усилия могут выражаться в:

–Использование специфических площадок для продвижения;

–Использование специфических методов продвижения ударного контента;

–Скорости распространения ударного контента.

–Специфические площадки – это особые площадки обычно используемые в таких ситуациях:

–Агрегаторы компромата, сливные бачки;

–Боты – аккаунты в соцсетях, управляемые софтом;

–Группы связанных источников – группы площадок, управляемых одним админом или группой админов.

Специфические методы продвижения ударного контента:

1. Посев – многократное дублирование одного контента:

1.1. Публикациями на сайтах СМИ, информ-агентств или на сайтах, имитирующих такие площадки;

1.2. Публикациями на страницах подконтрольных злоумышленнику аккаунтов в соцсетях;

1.3. Публикациями в лояльных группах в соцсетях (от одного или разных аккаунтов);

1.4. Комментариями, содержащими ударный контент под разными публикациями;

2. SMM:

2.1. Накрутка соц активности для продвигаемой публикации (лайки, репосты, комменты…);

2.2. Организация вовлекающего обсуждения для продвигаемой публикации, в результате чего в распространение вовлекаются реальные пользователи;

2.3. Популярные теги для продвигаемой публикации (работает технология для Твиттера, Инст…);

2.4. Использование рекламных механизмов для распространения ударного контента – платное распространение через официальный рекламный кабинет или через биржи ре-

кламы.

Но в конечном счете продвижение сводится к многократному дублированию ударного контента. Именно по этой причине дублирование является одним из основных признаков продвижения контента.

Скорость распространения ударного контента подразумевает частоту его дублирования. В ряде случаев наблюдается такое дублирование с шагом в 1 секунду. Иными словами, каждую секунду появляется дубликат ударного контента на новой площадке (сайт, аккаунт, группа в сосцети и т.п..), а то и несколько.

Специфичность ударного контента подразумевает особенность самого материала, адаптированного именно для манипулирования аудиторией. При этом сам контент может быть как достоверным, так и не достоверным или частично достоверный.

Наиболее используемыми особенностями контента может быть:

–Ложь – материал является обманом частично или полностью;

–Правда в сочетании с особой подачей материала;

–Нарушение логики рассуждения или ее подмена идеологией;

–Отсылка к эмоциям;

Манипулирование может осуществляться с использованием любых типов контента:

–Текста;

–Изображения;

–Видео;

–Офисные документы (имитация утечки);

–Их сочетанием.

Как определить направление атаки

Вектор атаки в информационной операции это с помощью какой темы (нарратива) оппонент планирует достичь своей цели. В рамках контента нужно говорить о «темах», которые эксплуатирует оппонент, о темах, с помощью которых оппонент попробует спровоцировать действия или бездействия целевой аудитории.

В информационном потоке определение ударной темы дело непростое, особенно, когда интенсивность воздействия десятки тысяч сообщений в сутки. А именно такие «нагрузки» присутствуют в наиболее популярных темах. Поэтому ни о каком ручном анализе здесь речи быть не может – необходима автоматизация. Автоматизированная система должна делить весь поток по проблеме на «темы», т.е. объединять сообщения со схожей тематикой в некий отдельный поток. Например, при исследовании медийной активности вокруг политика чаще всего появляются темы «Коррупция»,

«Некомпетентность». «Аморальность» и т.п.. А изменения таких потоков (тем) позволяют понять на что-же нацелился оппонент.

В качестве явных признаков можно назвать рост негативных высказываний в какой-то теме, причем рост этот созданный за счет астротурфинга (ботами и троллями). Ведь боты и тролли стоят денег – бесплатно они не работают, а значит кто-то вложил деньги в распространение негатива по определенной теме. Значит можно предположить, что данная тема может стать основной в атаке против объекта.

Автоматизация

Автоматизация подготовки на перспективу возможна с помощью мониторинговых систем. Мониторинговая система в интересах подготовки на перспективу должна помогать оператору отслеживать и заранее выявлять:

–Уязвимости своей аудитории или ее элементов и их изменения;

–Уязвимости аудитории противника и их изменения;

–Проявления интереса противника или иного субъекта к нашей аудитории;

–Подготовку к проведению информационной операции против нашей аудитории;

–Подготовку к проведению новой информационной операции противником;

–Изменение в регионах интереса, могущие привести к ин-

формационным операциям.

Для решения этих задач мониторинговая система должна иметь возможность:

–Осуществлять автоматический перевод с языков;

–Собирать (парсить) информацию из особых типов источников;

–Выявлять информационные операции;

–Исследовать ЦА, указанную оператором;

–Подбирать ЦА по параметрам, указанным оператором.

Планирование информационных операций

Планирование информационной операции – это определение цели операции, и на ее основе определение деталей будущей операции вплоть до плана действий:

–Целеуказание – определение/уточнение цели мероприятия;

–Определение ЦА, с чьей помощью будет достигнута цель операции;

–Выявление уязвимостей аудитории;

–Определение общей стратегии и сценария воздействия на аудиторию;

–Формирования плана распространения;

–Определение показателей эффективности.

Осмысление поставленной задачи

После получения задания специалист по планированию информационной операции должен осмыслить цель мероприятия. И речь не столько о планируемой ИО, сколько о том какую проблему хочет решить постановщик задачи с помощью ИО. Этот этап требует сбора всех относящихся к делу фактов и данных, которые могут повлиять на выполнение миссии. По сути, задача состоит в том, чтобы не просто понять, чего нужно добиться, но и как это поможет «заказчику» в решении его задач.

Специалисту по планированию необходимо изучить, доступную справочную информацию и руководящие указания в отношении планируемой операции и театра военных действий.

Специалист по планированию ИО должен:

1. Запросить материалы по ТВД

1.1. Состояние военного, экономического, людского потенциала целевой территории (страны/региона)

1.2. Политические партии, ФПГ, ОПГ, их интересы, взаимоотношения, противоречия, конфликты

2. Запросить данные по будущей ЦА

2.1. Запросить данные по особенностям населения данной территории (национальности, языки, социальный уровень, кланы, группировки….)

2.2. Запросить данные о взаимоотношениях между группами, конфликтах, особенно застарелых

3. Запросить данные по медиапространству

3.1. Запросить информацию по анализу ключевых личностей и человеческих факторов.

3.2. Проанализировать источники информации ЦА в зоне ответственности (СМИ, ТВ, радио, интернет).

3.3. Получить данные опросов и анкетирования от других организаций или владельцев коммерческой информации в регионе.

По завершении осмысления задачи специалист по планированию должен ответить на следующие вопросы:

–Каковы «наши» интересы в зоне будущих действий?

–Какова «наша» стратегия по отношению к рассматриваемому Объекту (стране/региону, ЦА, лицу или организации)?

–Кто является основными лицами, принимающими решения в зоне интереса?

–Каков источник власти лиц, принимающих решения? От кого они зависят, кто зависит от них?

–Какова текущая социальная, политическая и экономическая ситуация, в самом широком смысле, в зоне интереса?

–Какова медийная ситуация в зоне интереса (источники новостей, Сми, их влиятельность и зависимость…)?

Анализ миссии

Анализ миссии – это понимание, что нам мешает для достижения наших глобальных целей в регионе интереса. Начинается такой анализ с рассмотрения намерений руководителя в отношении целей будущей операции. Результат анализа миссии станет основными источниками первоначальной информации о будущей операции, которая гарантирует, что разработанные цели ИО будут соответствовать как национальным, так и целям непосредственного руководства.

Результатом анализа миссии является определение проблемы и начало процесса определения ее возможных решений.

Оценка ситуации

Оценка должна быть как можно более подробной, и специалист по планированию ИО должен запросить помощь в подготовке этого документа у «соседей» и разведки. Чем точнее оценка, тем лучше можно интегрировать планируемую операцию в остальную часть планируемых шагов на данном ТВД. По оценки ситуации специалист по планированию ИО должен решить следующие задачи:

–Выявление ключевых целевых аудиторий (список потенциальных целевых аудитории в самом широком смысле).

–Анализ медиа-инфраструктуры района планируемой операции: Список источников по типу, политической принадлежности, охвату аудитории и влиятельности и т.д.; этот

анализ может представлять собой список с графическим наложением карты региона для получения оценки территориального охвата.

–Координация для оказания максимально возможной помощи в оценке и планировании информационной операции.

–Анализ влияния природных факторов: погоды, рельефа местности.

Определение прямых и вспомогательных задач

Прямые задачи – это те задачи ИО, которые непосредственно возлагаются руководством на подразделение ИО. Специалист по планированию ИО обычно находит прямые задачи в соответствующем приказе, плане вышестоящего штаба или устном указании.

Вспомогательные задачи – это те, которые должны быть выполнены для выполнения прямой задачи, но которые не указаны в приказе вышестоящего органа. Вспомогательные задачи определяются на основе детального анализа приказа вышестоящего органа, ситуации с противником и направлений действий, а также особенностей ТВД.

Ниже приведены некоторые возможные примеры прямых задач для информационных операций (они написаны не как Цели психологических операций, что будет сделано позже, а просто как соображения, которые необходимо учитывать при разработке Целей психологических операций):

–Создать условия для ввода войск.

–Изображать наркоторговцев и коррупцию в сфере наркотиков как угрозу, которая затрагивает все страны.

–Формировать глобальную информационную среду таким образом, чтобы способствовать восприятию того, что действия противника противоречат международному праву, договорам и резолюциям Совета Безопасности Организации Объединенных Наций (ООН).

–Ограничить эффективность враждебной пропаганды, дезинформации и других форм политической войны.

–Поощрять региональную стабильность и сотрудничество.

–Оказывать непосредственную информационную поддержку гуманитарным операциям.

–Снизить сопротивление местного населения операциям ВС.

–Повысить безопасность граждан.

–Способствовать установлению гражданского порядка.

–Повысить эффективность полиции и вооруженных сил.

–Увеличить поддержку народом правительства.

–Снизить обеспокоенность населения по поводу ухода войск.

А вот некоторые возможные примеры вспомогательных задач информационных операций:

–Убедите ключевых коммуникаторов выступить против агрессии сил Национальной безопасности.

–Убедить ЦА в том, что развертывание войск носит временный характер; силы находятся там только для подавления агрессии.

–Развивать заслуживающие доверия новостные агентства, тем самым информируя ЦА об истине.

–Способствовать военному и технологическому превосходству страны

–Убедить ЦА в том, что наше участие направлено на поддержку демократических правительств, свободных от манипуляций.

–Проинформировать ЦА о том, что акты агрессии против вооруженных сил недопустимы.

–Убедить ЦА сдаться или покинуть свой пост.

Специалист, планирующий информационную операцию будет использовать список прямых и вспомогательных задач, чтобы начать разработку Целей психологических операций. Результатом становиться формулировка, которая отражает желаемое поведение или изменение отношения выбранных ЦА в результате информационной операции.

Определение цели информационной операции

На данном этапе руководитель органа, реализующего ИО, должен ответить на вопрос о цели своего мероприятия – для чего она проводится. Применительно к аудитории – что должна сделать аудитория или воздержаться от какого дей-

ствия.

Задачу вам всегда ставят для чего-то, зачем-то, в связи с чем-то, для достижения чего-то… Всегда нужна понятная задача – даже когда ее вам не говорят. Ведь нельзя достичь цели, не зная в какую сторону идти. Поэтому важно цель сформулировать кратко и четко.

К сожалению, не всегда можно добиться точной постановки задачи от руководителя. Это не обязательно связано с попыткой что-то скрыть от вас. Чаще это проявление особенности психики: если знаю я, то подразумеваю, что это знает и собеседник, а значит незачем об этом говорить.

Для понимания какова цель планируемой ИО можно использовать несколько приемов.

Первый – последовательно задаем вопрос ЗАЧЕМ – на каждый абстрактный ответ заказчика задается вопрос «зачем это вам». Простой приём, но будьте аккуратны. Обычно после третьего зачем вас могут обвинить в тупости или начнут раздражаться.

Второй прием – беседуя с заказчиком посредством наводящих вопросов пытаетесь понять, что его беспокоит, почему беспокоит именно это и именно сейчас, где он видит угрозу или почему важно именно это.

Третий – самостоятельно анализируете поставленную задачу с точки зрения чем это поможет инициатору ИО. Поставьте себя на место заказчика и исходите из его целей и задач.

Если заказчик сопротивляется и не ставит четкой задачи, можно подыграть ему, сказав, что безусловно будет достигнута «победа во всем мире», но, какой результат хотелось бы получить в первую очередь?

Тем ни менее исходные формулировки задач иногда бывают недостаточно четко сформулированы и требуют уточнения, а в ряде случаев и серьезной корректировки. Некорректно обозначенная цель приводит к неверным действиям и расходованию ресурсов впустую. А сама формулировка проблемы задает дальнейший ход рассуждений. Поэтому важно самостоятельно изучить ситуацию и уточнить задачу, а также попробовать ее расширить.

Простой пример – сложилась довольно распространенная ситуация: «На парковке у офиса толчея, места не хватает. Руководство компании поручает группе сотрудников предложить способы перепланировки парковки, чтобы она вмещала больше авто».

Руководство изначально определило проблему так: «Как увеличить емкость парковки».

Но ведь проблему можно сформулировать иначе. Варианты:

–Избавиться от толчеи на парковке.

–Обеспечить всех желающих местами на парковке.

–Снизить нервозность в коллективе из-за споров из-за машиномест.

И каждый вариант, при единой общей направленности, открывает несколько разные подходы к решению проблемы. А значит и возможность использования разных инструментов.

Также не надо забывать, что у разных участников этой ситуации разные интересы. Основные участники:

–Руководство компании.

–Сотрудники компании, приезжающие на авто.

Попробуйте сформулировать проблему с точки зрения этих двух групп участников.

Руководство компании:

–Снизить нервозность в коллективе.

–Повысить эффективность сотрудников.

–Найти дополнительные рычаги влияния на сотрудников.

Сотрудники компании, приезжающие на авто:

–Создать более комфортные условия для себя.

В результате если заменить изначальную формулировку задачи «Как увеличить емкость парковки» на «Снизить нервозность в коллективе», то и подходы к пониманию проблемы, ее исследованию и предложения вариантов решения будут отличаться. Ведь «Снизить нервозность в коллективе» можно поставив всех в равные условия – закрыв всю парковку и лишив сотрудников машиномест. Предмет конфликта

устранен, ссор из-за мест на парковке больше не будет. А вот при подходе «повысить эффективность сотрудников» такой подход сработает только отчасти.

Другой пример. Задача, поставленная руководством в формате «растолкуйте этим ганд@#% что они сдохнут на@#» явно требует уточнения, дополнительного осмысления и преобразования в более точные и общепринятые формулировки. Можно, в формате «донесите до ЦА-1 информацию о негативных последствиях в случае продолжения сопротивления».

Но формулировка «донесите до ЦА-1 информацию о негативных последствиях в случае продолжения сопротивления» также не является целью информационно психологического воздействия, а является одним из инструментов достижения цели. Вероятно, конечная цель должна звучать так «мотивировать ЦА-1 к прекращению сопротивления». Именно такая формулировка цели для информационной операции позволяет адекватно определить не только аудиторию, но и особенности ударного контента, подобрать эффективные каналы доставки ударного контента, источники этого контента и определить интенсивность демонстрации ударного контента данной целевой аудитории.

Переосмыслив задачу, полученную от своего руководства, ответственный за информационную операцию проверяет свою гипотезу о конечной цели всего мероприятия. Например, уточнив это у того, кто ставил задачу. И если его ги-

потеза подтверждается, то именно такая формулировка становиться главной (генеральной) задачей операции, именно исходя из нее и будут формулироваться подзадачи. В итоге операция получает переформулированную цель: «мотивировать ЦА-1 к прекращению сопротивления».

Формат формулировки целей для ИО – это «глагол – объект». Глагол описывает направление желаемого изменения. Объект – это общее поведение или отношение, подлежащее изменению. Некоторые глаголы действия, обычно используемые в ИО – это сокращать, убавлять, предотвращать, увеличивать, приобретать и поддерживать.

Например, одна из целей, взятых из намерения командира, заключается в "создании безопасной среды для жителей города Н". Это не заявление об измеримой реакции, которая отражает желаемое изменение поведения или отношения. Если ее переформулировать как "снижение криминальной активности в городе Н", то теперь ее можно использовать в качестве цели психологических операций, поскольку теперь ее можно оценить (например число совершаемых преступлений за период), и она отражает желаемое изменение поведения или отношения в выбранной иностранной ЦА.

Определение ЦА

После разработки целей ИО и целевых действий аудитории специалисты по планированию приступают к определению потенциальных целевых аудиторий. Потенциал, как и те

аудитории, которые, по первоначальному мнению планировщика, обладают способностью выполнять целевое действие. Этот первоначальный список потенциальной целевой аудитории будет очень широким, поскольку у планировщика редко есть время для проведения исчерпывающего исследования в этой области.

Для определения целевой аудитории необходимо ответить на вопрос кто должен осуществить необходимое целевое действия. Кто те люди, которые должны что-то совершить? В нашем случае (мотивировать ЦА-1 к прекращению сопротивления) – кого именно нужно мотивировать (подтолкнуть) к прекращению сопротивления. Кто те люди, которые должны прекратить сопротивление. В некоторых случаях может оказаться, что это один человек. Например, командир войскового соединения или его жена. И тогда целевая аудитория сужается до этого одного человека.

После определения целевой аудитории ее необходимо изучить и описать. Делается это для понимания с помощью чего можно осуществить манипулирование данной целевой аудиторией. А на что ЦА может среагировать не так как вы планируете (разные табу в социуме, априорное отношение к чему-то и т.п..).

Обычно, на начальном этапе, об аудитории желательно знать:

–Пол и возраст;

–Национальность, язык;

–Семейное положение, есть ли дети;

–Место проживания и род занятий;

–Образование, воспитание;

–Уровень дохода;

–Социальный статус;

–Места, где человек проводит свободное время, чем увлекается.

Затем, с пониманием этих данных, углубляются в мотивацию аудитории, исследуя:

–Политические взгляды, убеждения, жизненная позиция;

–Как человек относится к интересующей вас проблеме;

–Что любит, что не любит, чего опасается или избегает;

–Как лучше или обычно воспринимает информацию (слух, зрение);

–Какой информации отдает предпочтение (аналитика, развлекательная, новости, публицистика…);

–Его желания, мечты, чаянья.

Анализ целевой аудитории

Анализ целевой аудитории – это детальное систематическое изучение информации, имеющей отношение к информационной операции, по отношению к выбранным ЦА, которые могут выполнить целевое действие. Целью анализа является определение того, как убедить одну ЦА провести одно целевое действие. Этот анализ представляет собой исследо-

вание, призванное определить, как вызвать нужную (запланированную) реакцию у конкретной ЦА.

Процесс анализа целевой аудитории направлен на ответ на четыре основных вопроса:

–Какие ЦА будут наиболее эффективными для достижения желаемой поведенческой реакции?

–Какие способы убеждения повлияют на ЦА для достижения цели?

–Какие каналы доставки ударного контента будут эффективно проводить выбранную линию убеждения?

–Какие события будут указывать на успех или провал информационной операции?

Факторы, влияющие на ЦА

Факторы – это те элементы окружающей обстановки, которые влияют на ЦА. Факторы, влияющие на конкретную ЦА, безграничны, и многие из них могут не иметь отношения к цели информационной операции. В ходе анализа целевой аудитории выявляются и рассматриваются только те факторы, которые влияют на ЦА и имеют отношение к достижению цели информационной операции. Факторы состоят из трех элементов:

–стимул,

–ориентация,

–поведение.

Стимулом может быть событие, проблема или характеристика, влияющие на ЦА. Событие – это все, что происходит, что влияет на ЦА. Это, например, повышение стоимости потребительских товаров, обстрел города ЦА или выборы нового мэра или депутата. Проблема – это существующий фактор, влияющий на ЦА. Это, например, текущая стоимость потребительских товаров, законы, правила, или текущая политическая структура. Характеристика – это любая демографическая характеристика ЦА, которую также можно рассматривать как слабость. Примеры включают средний возраст, уровень дохода, уровень подготовки, религию или этническую принадлежность. Аналитику не важно определять, какие типы стимулов существуют, важно только то, что они влияют на ЦА по отношению к достижению целей информационной операции.

Ориентация это то, что ЦА думает или чувствует по поводу определенного стимула. Чтобы понять ориентацию ЦА, аналитик информационных операций должен взглянуть на установки, убеждения и ценности. Установка – это устойчивая, приобретенная предрасположенность реагировать определенным образом на данный объект, человека или ситуацию. Убеждения – это убеждения о том, что истинно, а что ложно, основанные на опыте, общественном мнении, подтверждающих доказательствах, авторитетах или даже слепой вере. Ценности – это концепции конечных благ и зол. Отношения, убеждения и ценности формируются восприяти-

ем ЦА. Восприятие – это внутреннее представление сенсорной информации, получаемой от зрения, слуха, обоняния, вкуса или прикосновения. Аналитик в состоянии определить некоторые из этих установок, убеждений и ценностей, изучая, как ЦА реагировала на ситуации в прошлом.

Поведение– это реакция человека на стимул. Это внешне наблюдаемое действие или бездействие человека после того, как он подвергся воздействию стимула и отфильтровал его через свою личную ориентацию.

Все три элемента взаимосвязаны: один влияет на два других. Например, столкнувшись с определенным стимулом, ЦА проявит поведение или отсутствие поведения в зависимости от его внутренней ориентации на этот стимул. Чем сильнее их ориентация на стимул, тем сильнее поведенческая реакция ЦА.

Эту формулу можно использовать для прогнозирования поведения. Понимая ориентацию ЦА, аналитик может предсказать поведение ЦА, если будет введен определенный стимул. Этот метод чрезвычайно полезен для прогнозирования психологических последствий операций, таких, как например, ввод вооруженных сил в чужую страну.

Выявление и составление списка факторов, влияющих на ЦА в отношении достижения целей ИО, представляет собой поэтапный процесс.

Первый шаг – выявить проблему. Например, если текущая ситуация описана так: «ЦА голосует на выборах», про-

блема заключается в следующем: «Почему ЦА не голосует сейчас?».

Второй шаг – выбор метода исследования. Большинство первоначальных исследований целевой аудитории являются «кабинетными» с небольшим или вообще без прямого доступа к ЦА и, следовательно, требует дополнительных исследований. Однако, как только специалист по информационным операциям прибудет в зону проведения ИО, они смогут провести полевые исследования, чтобы дополнить и обновить отчет по ЦА.

Третий шаг – провести исследование. Существует бесконечное количество источников для исследования ЦА. Отчеты разведки, обзоры СМИ и оценки являются отличными источниками текущей информации о ЦА. Кроме того, Интернет нужно использовать для доступа к информации из открытых источников. Все источники должны быть оценены на предмет достоверности, точности и актуальности.

Четвертый шаг – классифицировать, атрибутировать и поместить каждую выявленную особенность, полученное в результате работы аналитика. Категории, как правило, классификация идет по следующим пунктам:

–Международные отношения (договоры, союзы, пограничные вопросы).

–Демография (возраст, раса, религия, грамотность, этническая группа, пол).

–Экономические (доходы, занятость, инфраструктура).

–Политические (законы, выборы, лидеры, проблемы).

–Экологические (качество почвы, кислотные дожди, засухи, землетрясения).

–Социальные (здравоохранение, преступность, образование).

–Военные (диспозиция, статус, отношение к ТА).

Пятый шаг заключается в том, что для каждого условия должен быть указан источник, чтобы рецензент мог проверить достоверность каждого фактора. Кроме того, этот шаг позволяет быстро и эффективно обновить анализ ЦА позднее. При перечислении условий в анализе ЦА также необходимо учитывать классификацию.

Определение восприимчивости аудитории

Аналитики оценивают каждый способ убеждения на предмет его способности повлиять на ЦА для достижения желаемого поведения. Как и в случае с любым аргументом, разные способы убеждения будут влиять на людей в разной степени. Рейтинги восприимчивости определяют, какая линия убеждения окажет наибольшее влияние на ЦА и почему. Аналитики используют рейтинги восприимчивости, чтобы выбирать между различными разработанными линиями убеждения.

Восприимчивость– это степень, в которой на ЦА можно повлиять, чтобы она отреагировала таким образом, ко-

торый поможет выполнить миссию информационной операции, или, проще говоря, насколько хорошо можно манипулировать уязвимостью. Чем сильнее уязвимость, тем более восприимчивым будет ЦА к линии убеждения, которая ее использует. Ниже приведены некоторые возможные способы убеждения, и при обычных обстоятельствах эти способы убеждения получают следующие оценки:

1. Долг солдата – следовать всем правилам и положениям. Эта линия убеждения не имеет очень высокой оценки, поскольку у ЦА еще не развилось сильное чувство гордости за принадлежность к армии. Это связано с их убеждением, что остальная часть армии воспринимает их просто как «стажеров или детей».

2. Несоблюдение правил и положений влечет за собой наказание согласно Законодательству. Рейтинг этой линии убеждения немного выше, потому что ЦА знает, что правила их гражданской жизни изменились, и теперь они несут больше ответственности за свои действия, но они также видели солдат, нарушивших правила, которые не были строго наказаны. Другими словами, их можно наказать, но это не имеет большого значения.

3. Студенты, соблюдающие правила, награждаются повышенными привилегиями. Студентов лишили всего того, что напоминает им об их жизни до армии, включая гражданскую одежду, радиоприемники, проигрыватели компакт-дисков и доступ к телевидению. Они находятся под постоянным кон-

тролем кадрового состава и не имеют полномочий принимать решения. Им обещали пропуска и доступ к их личным вещам, если они будут следовать правилам, что делает этот способ убеждения очень влиятельным.

По мере изменения условий меняется и восприимчивость ЦА к определенной линии убеждения. Общее правило состоит в том, что линия убеждения, направленная на удовлетворение критической потребности, будет очень эффективной и, следовательно, обычно получит более высокий рейтинг. Способы убеждения, направленные на удовлетворение нескольких потребностей, также, вероятно, будут оценены выше.

Изучение подобранной аудитории на предмет её восприимчивости – это определение ключевых особенностей аудитории с целью выбора наиболее эффективного метода воздействия на нее в рамках текущей информационной операции.

Определение восприимчивости аудитории подразумевает выявление того, какая информация и в каком виде, где и когда наиболее сильно воздействует на выбранную аудиторию:

1. По каким каналам аудитория получает информацию, чему отдает предпочтение:

1.1. Радио;

1.2. Телевидение;

1.3. СМИ;

1.4. Интернет;

1.5. Еще что-то;

2. Из каких источников информация воспринимается более благосклонно:

2.1. Какие именно СМИ;

2.2. Какие ТВ-программы;

2.3. Какие сайты новостей;

2.4. Кого из ЛОМов предпочитают;

2.5. Еще что-то;

3. К какому типу информации аудитория более привычна:

3.1. Текст;

3.2. Картинка;

3.3. Видео;

3.4. Документ;

3.5. Еще что-то;

4. Контентные предпочтения аудитории:

4.1. На какие темы публикуют материал в группах концентрации аудитории;

4.2. На публикации по каким темам аудитория реагирует активее (лайки, репосты, комментарии);

4.3. На какой тип материалов больше реакций (текст, картинка, видео);

4.4. Еще что-то;

5. Какой формат подачи информации наиболее приемлем для аудитории:

5.1. Ток-шоу;

5.2. Новости;

5.3. Аналитика;

5.4. Схемы, инфографика;

5.5. Демотиваторы;

5.6. Еще что-то;

6. На что табу в обсуждениях аудитории (чтобы случайно не нажать не на ту «кнопку»):

6.1. Из каких источников;

6.2. Каких авторов;

6.3. На какую тему;

6.4. Еще что-то.

Определение уязвимости аудитории

После определения целевой аудитории и ее особенностей приступают к выявлению ее уязвимостей. Уязвимости целевой аудитории – это те ее особенности, используя которые можно спровоцировать нужное поведение аудитории. Без правильного выявления уязвимостей ЦА будет не получится повлиять на нее.

Есть два подхода к определению уязвимостей аудитории. Первый основан на потребностях человека – на «пирамиде Маслоу». Второй на противоречиях внутри аудитории. Оба

подхода имеют свои особенности и есть смысл использовать каждый из них в зависимости от особенностей ситуации.

В соответствии с первым подходом:

Уязвимости – это потребности, возникающие у ЦА, которые они будут стремиться удовлетворить или извлечь из них выгоду, как только они будут удовлетворены.

Уязвимость – это проявление неудовлетворенной или предполагаемой потребности ЦА. Ключевое слово в этом определении – «потребность».

Именно эти потребности будет использовать для воздействия на ЦА.

Потребности и желания – все это выражения одной и той же концепции. ЦА, у которого есть одно из этих качеств, будет стремиться их удовлетворить, прилагая различные усилия. Для целей информационной операции они все одинаковы. Если ЦА стремится удовлетворить потребность или желание, в рамках информационной операции можно это использовать. Желание ЦА удовлетворить, облегчить или устранить потребность дает ей мотивацию изменить и свое поведение.

Социологи выделяют два основных типа потребностей – биологические (или физиологические) и социальные. Биологические потребности – это те элементы, которые необходимы для поддержания жизни: пища, вода, воздух, кров и размножение. Эти потребности являются общими для всех культур, хотя разные культуры будут стремиться удовлетво-

рить эти потребности по-разному. Социальные потребности – это потребности, усвоенные обществом в процессе инкультурации (процесс, посредством которого человек усваивает традиционное содержание культуры и усваивает ее обычаи и ценности). Каждая культура будет иметь разные социальные потребности и разные приоритеты для удовлетворения этих потребностей.

Иерархия потребностей Маслоу является наиболее широко известным объяснением удовлетворения потребностей. Используя пирамиду, Маслоу объяснил, что человек должен удовлетворить основные потребности, прежде чем перейти к социальным потребностям. Он также утверждал, что каждый человек должен удовлетворить потребности на каждом уровне, прежде чем продвигаться вверх.

Теория Маслоу – лишь один из способов определить потребности ЦА, и в некоторых случаях ее довольно легко разбить. Большинство людей будут действовать в соответствии с его иерархией в обычное время, но могут значительно изменить свое поведение в другое время, особенно если они находятся в состоянии сильного стресса, который можно определить как умственное, эмоциональное или физическое напряжение. Например, военнослужащие во время конфликта испытывают высокий уровень стресса и обучены преодолевать основные потребности для достижения групповых целей. При оценке этих участников как ЦА необходимо учитывать это обучение, и поэтому они не будут точно вписы-

ваться в иерархию потребностей Маслоу.

В разных культурах определенные потребности расставляются по-разному, и аналитик должен применить свой региональный опыт, чтобы соответствующим образом скорректировать категории потребностей.

Другой способ разработки иерархии потребностей состоит в том, чтобы немного изменить Маслоу следующим образом. Как только потребности установлены они классифицируются как

–критические,

–краткосрочные,

–долгосрочные.

Критические потребности обычно связаны с биологией или, возможно, с безопасностью, в зависимости от серьезности ситуации с безопасностью.

Краткосрочные потребности часто относятся к тому, что Маслоу считал потребностью в безопасности и принадлежности. К ним относятся потребности, которые не обязательно удовлетворять немедленно для поддержания жизни. Серьезные экономические трудности, чрезвычайно высокий уровень преступности, отсутствие какой-либо политической свободы или острая нехватка медицинских учреждений являются примерами краткосрочных потребностей.

Долгосрочные потребности включают то, что Маслоу считал потребностью в уважении и самоактуализации. Примерами могут быть стабильная и справедливая государствен-

ная система, в которой возможна свобода выражения мнений, сильная экономика, справедливая система правосудия или свобода заниматься различными делами.

Расстановка приоритетов среди выявленных потребностей должна отражать силу желание ЦА удовлетворить потребность. Потребность, которая касается нескольких условий, обычно имеет более высокий приоритет, поскольку ЦА будет выполнять ее с большими усилиями. После определения приоритетов потребностей их необходимо классифицировать как критические, краткосрочные и долгосрочные, что поможет аналитикам определить приоритеты своих усилий.

Когда ЦА пытается удовлетворить потребность, нередко возникает конфликт. Существует три типа конфликта потребностей:

1 Конфликт подхода возникает, когда есть два или более способов удовлетворить одну потребность, но у ЦА есть средства, чтобы выбрать только один. Пример: ЦА нуждается в представительстве в правительстве. Из трех кандидатов двое апеллируют к ЦА, но могут проголосовать только за одного кандидата.

2 Конфликт избегания возникает, когда удовлетворение одной потребности вступает в противоречие с необходимостью избегать чего-то неприятного или опасного. Пример: потребность есть мороженое противоречит потребности не набирать лишний вес.

3 Конфликт выбора из двух зол возникает, когда ЦА стал-

кивается с двумя вариантами выбора, ни один из которых не является желательным; однако ЦА должен выбрать один или другой. Пример: ЦА хочет избежать похода к стоматологу из-за связанной с этим боли и дискомфорта. Тем не менее, они также хотят избежать любых проблем с зубами. Затем им приходится выбирать между «меньшим из двух зол».

Теперь поговорим о последовательности анализа при определении уязвимостей целевой аудитории для целей информационной операции. Это пятиэтапный процесс.

Первым шагом является определение потребностей ЦА на основе условий, влияющих на эту ЦА.

Второй шаг – классификация и определение приоритетов потребностей. Цель на этом этапе – определить, какие потребности наиболее важны и какие следует попытаться использовать в первую очередь в рамках информационной операции.

Третий шаг – определить, есть ли конфликты потребностей и какой тип конфликта существует. Затем аналитик предполагает, как ЦА попытается разрешить конфликт, что может дать аналитику представление о том, как лучше всего удовлетворить конкретную потребность.

Четвертый шаг заключается в определении взаимосвязи между потребностями и целями психологических операций. Если потребность связана с целью психологической операции, ее можно сохранить в анализе целевой аудитории. Если это не связано, его следует удалить из анализ ЦА.

Наконец пятый шаг, каждая потребность или уязвимость исследуются, чтобы определить необходимое действие по ее использованию для манипулированию. Уязвимости с высоким приоритетом и прочной связью с цели психологических операций могут быть использованы для воздействия на ЦА для достижения цели психологических операций. Любая уязвимость, которая при ее удовлетворении будет препятствовать выполнению цели психологических операций, должна быть сведена к минимуму. Другие уязвимости с низким приоритетом, но имеющие сильное отношение к цели психологических операций, могут быть улучшены и затем использованы.

Каждая уязвимость, указанная в анализе целевой аудитории (отчет по ЦА), должна иметь подробное объяснение следующих моментов:

–Аналитик начинает с краткого описания уязвимости, включая приоритет потребности и то, сколько усилий ТА прилагает или затрачивает для удовлетворения потребности.

–Аналитик описывает любой конфликт потребностей и то, вероятность того, что ЦА разрешит этот конфликт.

–Аналитик описывает связь между уязвимостью и целями психологических операций.

–Аналитик описывает, насколько прямыми или сильными являются отношения между членами ЦА.

–Наконец, аналитик объясняет, какие действия необходимо предпринять, чтобы использовать эту уязвимость для

влияния на ЦА.

Еще один подход к выявлению уязвимостей аудитории связан с выявлением противоречий внутри социума. При таком подходе выявить уязвимость аудитории – это определить те темы (сюжеты), которые могут вызвать спор в аудитории и дальнейший «раскол» на два и более конфликтующих лагерей, или темы, по которые вызывают у аудитории наиболее сильные эмоции. Особый интерес вызывают темы, вызывающие негативные эмоции. Так как негативные эмоции с большей вероятностью мотивируют аудиторию к действию.

Для выявления уязвимостей аудитории по такой схеме необходимо выявлять публикации (новости), которые вызывают наибольший отклик у аудитории (комментарии, лайки, репосты). В комментариях к таким публикациям можно найти дополнительную информацию по проблеме:

–Смысл противоречий и их историю;

–Степень поляризации мнений в аудитории;

–Аргументацию сторон;

–Еще что-то…

Определение каналов доставки

Аналитики изучают все доступные каналы доставки ударного контента, чтобы определить лучший способ общения с ЦА. Доступность определяется как наличие аудитории для целевого воздействия – аналитик пытается ответить на во-

прос: «Какое сочетание средств массовой информации будет эффективно доносить до ЦА развитые линии убеждения и соответствующие символы?» Медиа-анализ – это процесс, который позволяет аналитикам оценивать каждую форму медиа для конкретной ЦА. Шаги включают в себя следующее:

–Оценить, как ЦА в настоящее время получает информацию.

–Определить текущие источники, оценив охват и частоту.

–Проанализируйте использование ЦА для каждого источника.

–Определите, является ли контакт ЦА с каждым источником активным или пассивным.

–Анализировать динамику ЦА при доступе к каждому конкретному источнику.

–Определить любые новые источники, которые могут быть эффективными для ЦА.

Первым шагом в медиа анализе является определение того, как ЦА в настоящее время получает информацию. В частности, к каким типам источников имеет доступ ЦА и в каком формате? Ответив на несколько вопросов, касающихся различных форм источников, можно решить эту задачу. Ниже приведены примеры первого шага:

Имеет ли ЦА доступ к радио? Это FM, AM или короткие волны? Получают ли они чаще всего сообщения в виде ре-

кламных роликов, ток-шоу или документальных фильмов? Какова продолжительность этих роликов, ток-шоу или документальных фильмов? Какие форматы радиостанций они слушают: новостные или развлекательные?

Газеты, которые они получают, черно-белые или в них есть цветные фотографии и реклама? Получают ли они информацию через статьи, редакционные статьи, рекламу или все это? Какого размера объявления: 1/4, 1/2 или целая страница? Используют ли они вставки?

Как ЦА получает информацию через телевидение? Какой формат наиболее распространен: реклама, документальные фильмы, комедии или другие программы? Какова нормальная длина каждого типа?

Вторым шагом в медиа анализе является определение текущих моделей использования источников информации. Это позволит аналитику выбрать лучшие источники из тех, которые использует ЦА. Двумя основными методами оценки медиа-моделей являются охват и частота.

Охват – это общее количество членов ЦА, которые получают ударный контент хотя бы один раз в течение определенного периода. Большинство маркетологов и рекламодателей используют четырехнедельный период. Однако можно использовать любой период времени, но он должен быть одинаковым для всех средств массовой информации, и поэтому аналитик должен выбрать стандарт и использовать его для

всех форм оцениваемых средств массовой информации. Для печатных материалов, таких как газеты, журналы или информационные бюллетени, охват равен читательской аудитории, которая представляет собой сумму подписки плюс другие продажи плюс вторичную читательскую аудиторию. Например, при расчете стоимости подписки семья будет учитываться только один раз. Однако если бы помимо подписчика ту же газету читали еще три человека, то это привело бы к 4-м показателям читательской аудитории. Распространенной ошибкой при работе с радио и телевидением является подсчет количества принадлежащих радиоприемников и телевизоров. В некоторых частях мира на каждые пятьдесят человек может приходиться только один телевизор. Однако если 25 человек регулярно смотрят этот телевизор, это соответствует охвату в 50 процентов. Таким образом, количество зрителей телевидения и слушателей радио более важно, чем количество принадлежащих радио и телевизоров.

Частота – это количество раз, когда отдельный член ЦА получает определенное сообщение в течение определенного периода времени. Если член ЦА подписывается на газету пять дней в неделю и данный период времени составляет четыре недели, то частота этого средства массовой информации для члена ЦА будет равна 20. Большинство людей являются созданиями привычек, и поэтому определенный ЦА будет регулярно видеть определенные типы медиа. Это важная информация для аналитика, поскольку повторение и

подкрепление линии убеждения необходимы для изменения поведения.

Третий шаг в медиа анализе – определить, как ЦА использует эту среду. Необходимо определить, имеет ли ЦА доступ к среде и почему, и если да, то почему. Имеет ли ЦА доступ к этому средству для развлечения или для получения новостей и информации? Если они получат доступ к нему для развлечения, они могут не услышать серьезные сообщения. Если они получат доступ к средствам массовой информации для получения новостей и информации, более длинное, более серьезное сообщение может быть хорошо воспринято.

Четвертый шаг в медиа анализе – определить, насколько вовлечена в процесс получения информации. Если ЦА активно получает доступ к средству информации для получения новостей, существует большая вероятность, что ему будет легче привлечь и удержать их внимание, и более вероятно, что ЦА усвоит и поймет сообщение. Если ЦА пассивно обращается к средствам массовой информации, например, слушает радио во время работы, ему будет труднее привлечь и удержать внимание, и ЦА может не усвоить сообщение.

Пятый шаг – оценить, имеет ли ЦА доступ к источникам индивидуально или совместно с другими. Доступ к источнику в присутствии других повлияет на их восприятие сооб-

щения. Некоторые материалы могут показаться неподходящими для маленьких детей, и родители могут не захотеть слышать определенные сообщения в их присутствии. Однако доступ к средствам массовой информации в присутствии других может привести к дальнейшему обсуждению сообщения. Если сообщение, вброшенное в рамках информационной операции, далее обсуждается после получения ЦА, тем больше шансов, что ЦА удастся убедить.

Доступные ресурсы

Как только цели и ЦА определены, специалист по планированию информационных операций анализирует все доступные ресурсы и разрабатывает организацию задач с учетом ресурсов. Это включает в себя:

–персонал, задействованный в операции;

–оборудование;

–где будут располагаться персонал и оборудование;

–оперативный канал связи с поддерживаемым подразделение.

Крайне важно выделить надлежащие ресурсы для выполнения миссии, не тратя впустую ценные и ограниченные ресурсы. Такой перечень доступных ресурсов позволяет персоналу составить представление об имеющихся средствах для выполнения его предварительно сформулированной миссии.

Когда задача информационной операции определена, ана-

литики рассматривают силы, необходимые для:

–планирования, управления и контроля;

–обеспечения разведки;

–разработки программ информационной операции;

–взаимодействия с средства массовой информации;

–распространения ударного контента;

–обеспечения материально-технической поддержки.

Расположение этих сил имеет решающее значение. Должны ли эти силы работать с основного места дислокации, или находясь непосредственно в театре военных действий, или из места расположения командования объединенной оперативной группы или его тактических подразделений или из других мест, – это решение командира подразделения информационных операций, основанное на текущей ситуации имеющихся данных.

Ограничения

Существуют разные факторы, налагающие некоторые ограничения на стратегию, на подчиненных и ограничивают их свободу действий или ограничивают доступность активов в связи с конкретными задачами.

Ограничения могут принимать форму требования что-то сделать (например, снять видео о минной опасности) или запрета на действие (например, не нападать на командиров корпусов). Общие ограничения включают в себя:

–размер сил ИО, разрешенных на театре военных действий;

–доступные стратегические транспортные средства (это ограничение усиливает важность организации задач, адаптированных к миссии);

–темы, на которые следует обращать внимание и которых следует избегать;

–доступную пропускную способность каналов доставки ударного контента.

Аналитик ИО должен определить и понять, как эти ограничения влияют на проведение операции.

Специалисты по планированию ИО должны четко сформулировать требования к операции и ограничения. Эти данные позволяют определить, как лучше всего предоставить поддержку.

Необходимо учитывать следующие области, в которых обычно возникают ограничения:

–Темы, на которые следует обращать внимание и которых следует избегать.

–Целевые аудитории, которых следует избегать.

–Предполагаемые или фактические нарушения национального суверенитета, которые могут произойти.

–Стратегические транспортные ресурсы для развертывания.

–Ограничения финансирования.

–Ограничение с базированием.
–Логистические ограничения.
–Временные ограничения.
–Использование стратегических коммуникаций.
–Мобилизационные ограничения.
–Ротация сил и ограничения передислокации.
–Ограничения трансграничного вещания.
–Политические ограничения.

Сценария воздействия на ЦА

Сценарий воздействия на ЦА – это общее описание последовательности действий, с детализацией важных особенностей и напоминает пьесу с описанием сцен и диалогов действующих лиц с ремарками.

Сценарий воздействия на ЦА основывается на тактике убеждения аудитории. Тактика убеждения – это аргумент, используемый для получения желаемого действия ЦА. Тактики убеждения используются для эксплуатации уязвимостей аудитории. Тактика убеждения – это подробный, тщательный и краткий аргумент, который убедит ЦА вести себя желаемым образом.

Четыре шага по разработке сценария воздействия:

–Сформулируйте основной аргумент.

–Определите любые необходимые подтверждающие аргументы (какие доказательства должны быть предоставлены, чтобы аудитория поверила основному аргументу).

–Определите, какой тип апелляции будет полезен для данной ЦА.

–Определите, какая техника влияния имеет наибольшую вероятность успеха (как сотрудники представят свои аргументы в поддержку).

Аргумент

Основным аргументом является ключевая идея или вывод, в который нужно, чтобы ЦА поверила. Если ЦА верит ключевой идее, она будет вести себя желаемым образом. Основной аргумент обычно называют тезисом. Если правильно выбрана апелляция и представлены подтверждающие аргументы с использованием эффективных методов, ЦА должен согласиться с основным аргументом.

Поддерживающие аргументы – это ряд аргументов, которые должны убедить ЦА доверять основному аргументу. Это доказательства, представленные для влияния на ЦА. Как и в убедительном эссе, поддерживающие аргументы представлены в логичной и простой для понимания форме.

Апелляция

Апелляция (призыв, обращение) – это общий подход, используемый для представления аргумента. Это скорее тон аргумента. Апелляции привлекают внимание ЦА и поддерживают ее интерес на протяжении всего спора. Апелляции отбираются с учетом условий и уязвимостей ЦА. Например,

ЦА, которая не верит в легитимность правительства своей страны, не будет подвержен влиянию апелляции к легитимности, тогда как на военную ЦА может сильно повлиять апелляция к власти.

Существует бесконечное количество апелляций, которые можно использовать. Ниже приводится список апелляций, наиболее часто используемых в информационных операциях:

–Легитимность.

–Неизбежность.

–В группе – вне группы (принадлежность группе/социуму).

–Победитель.

–Ностальгия.

–Самосохранение (корысть).

Призывы к легитимности используют закон, традиции, историческую преемственность или поддержку народа. Ниже приведены типы апелляций по поводу легитимности:

Авторитет: апелляция к законам, нормам поведения или к людям, занимающим более высокие позиции в социальной иерархии. Например, Конституция или Кодекс, генерал и офицеры, полицейские, родители или государственные чиновники (в зависимости от особенностей ЦА). Чтобы апелляция подействовала, ЦА должен признавать полномочия авторитета. И именно это нужно выяснить на этапе анализа

ЦА.

Почтение: Обращение к религиозному учреждению или к человеку, которого почитают или которому поклоняются. Например, Библия, Далай-лама, католическая церковь или даже такой спортивный деятель, как Майкл Джордан.

Традиция: обращение к тому, к чему ЦА уже привык. Это поведение, которое повторяется постоянно и без вопросов. Потому что так было всегда.

Лояльность: обращение к группам, к которым принадлежит данной ЦА или тесно с ней связанным. Примерами являются воинские части, семья или друзья. Этот призыв обычно используется для подкрепления уже имеющегося поведения.

Призывы к неизбежности чаще всего основаны на эмоциях страха, особенно страха смерти, ранения или какого-либо другого вида вреда. Например, если вы не сдадитесь, вы умрете, или если вы не заплатите налоги, вы попадете в тюрьму. Это также может быть обращение к логике. Оба варианта требуют доказательства того, что обещанный результат действительно произойдет. Поэтому крайне важно, чтобы доверие было завоевано заранее и поддержано на протяжении всего процесса убеждения аудитории.

Апелляция «свой-чужой» (своя-группа-вне группы) направлена на разделение социума своих и чужих. Это создает внешнего врага группы и побуждает ЦА восставать против этого «внешнего врага» или «внутреннего врага». В этом

призыве часто указываются основные различия между двум ЦА или фракциями одной ЦА (если врага нужно определить внутри ЦА и «вытолкать» во вне). Если в ходе манипулирования не получится эффективно изобразить внешнюю группу (врага) в негативном ключе, апелляция потерпит неудачу.

Апелляция принадлежности к группе играет на потребности ЦА принадлежать к групповым стандартам или соответствовать им. Два основных типа такого типа призыва – это призыв к товариществу и призыв к соответствию.

Призывы к ностальгии относятся к тому, как дела обстояли в прошлом. Этот призыв можно использовать для поощрения или препятствования определенному поведению. В позитивном свете это относится к «старым добрым временам» и призывает ЦА вести себя так, как будто они возвращаются в те времена. В отрицательном смысле оно указывает на то, насколько плохо было в прошлом и как изменение поведения позволит избежать повторения тех времен.

Призывы, основанные на личных интересах, – это те, которые напрямую связаны с желаниями и чаяниями людей, входящих в состав ЦА. Этот тип апелляции может сыграть на уязвимости ЦА в плане приобретения, успеха или статуса.

Прием манипулирования

Да этом шаге определяем какая техника манипулирования ЦА с учетом выдранных аргументов и апелляций имеет наибольшую вероятность успеха.

Детально эти технологии описаны в разделе «2.3.1. Методы воздействия на аудиторию». Наиболее часто используемые из них в информационных операциях следующие:

–Дискредитация
–Авторитетный источник
–Ярлык
–Отвлечение внимания
–Высмеивание
–Сравнение

Пример формирования сценария воздействия

Предположим, **Аргумент** (ключевая идея, в которой должна поверить ЦА) найден и смысл его в следующем:

«из-за некомпетентности или коррупции министров от партии «Развитие без справедливости» из бюджета пропадают не менее 3 млрд в год, которых с запасом хватит для организации питания и образования детей за счет государства»

Определяем к чему будем обращаться (апеллировать), предлагая ему выбранный аргумент (идею). Наиболее используемые апелляции: самосохранение, личные интересы, ностальгия, принадлежность группе, легитимность, значимость, зависть…

А в нашем случае это апелляция к:

К личным интересам – по тому, что растрата бюджетных средств (денег налогоплательщиков) прямо затрагивает лич-

ные интересы граждан;

К страху – по тому, что из-за этого страдают дети, которым не дают нормального образования и питания;

К легитимности, точнее в нашем случае к НЕ легитимности тех самых министров, из-за которых пропадают деньги.

Выбираем приём манипулирования – с помощью какой технологии будем предъявлять ЦА аргумент (технология манипулирования). Какой прием манипулирования задействуем в нашей ситуации:

Через ЛИЧНЫЕ ИНТЕРЕСЫ: **дискредитация** через богатых родственников, которые всячески демонстрируют свой достаток;

Через СТРАХ: **сравнение** завышенных прогнозов о детской смертности, беспризорниках и детской преступности «у нас» с ситуацией в благополучных странах;

Через НЕ ЛЕГИТИМНОСТЬ: **высмеивая** некомпетентность министров;

Стратегия информационной операции

Вначале нужно определить общую стратегию – общий, не детализированный план, охватывающий длительный период времени, а способ достижения сложной цели. Стратегия включает в себя искусство комбинировать подготовку к информационной операции и последовательные действия для достижения цели информационной операции. Стратегия решает вопросы, связанные с использованием для победы над

противником всех имеющихся ресурсов.

Стратегия может быть сформулирована например так: «финансово ослабить конкурента за счет формирования недоверия к нему у его крупных партнеров, клиентов и кредиторов».

Или для цели «мотивировать ЦА-1 к прекращению сопротивления» стратегия может быть сформулирована следующим образом: «сформировать у целевой аудитории недоверие к своему руководству, ощущение безвыходности и желание сдачи в плен».

Основываясь на понимании конечной цели операции, кто является целевой аудиторией, ее особенностей и уязвимостей, необходимо сформулировать сценарий воздействия.

Сценарий воздействия – это общее описание последовательности действий, с детализацией важных особенностей и напоминает пьесу с описанием сцен и диалогов действующих лиц с ремарками.

Пример упрощенного сценария для коммерческой задачи «финансово ослабить конкурента за счет формирования недоверия к нему у его крупных партнеров, клиентов и кредиторов»:

–Анонимная публикация в местных СМИ, что в компании «ККК» какие-то проблемы, воруют, не хотят работать и т.п.;

–Материал подхватывают пользователи соцсетей и обсуждают что-же там, домысливая новые подробности;

–Через день в местной прессе появляется материал о злоупотреблениях у основного клиента «ККК»;

–Параллельно появляется публикация о возможных родственных связях в «ККК», кумовстве и бездарности родственников;

–Неизвестный, на основе этих данных, публикует «расследование» о воровстве в «ККК» и проблемах с правоохранительными органами, с вкраплением информации о серьезных финансовых проблемах.

Сценарий отвечает на вопросы – какие смыслы, какой аудитории и по каким каналам нужно донести.

Пример упрощенного сценария для задачи «мотивировать ЦА-1 к прекращению сопротивления»:

–Сформировать у целевой аудитории недоверие к своему руководству – через публикацию в Телеграмм-канале «Звери в форме» фактов воровства, коррупции, кумовства;

–Сформировать у целевой аудитории ощущение безвыходности – через распространение в компроматных Телеграм-каналах материалов о некомпетентности, об аморальном поведении родственников, о предательстве интересов страны;

–Сформировать у целевой аудитории желание сдачи в плен – показать аудитории, что они умирают за чужие интересы, что на этой стороне гораздо лучше через разгон соответствующих материалов в соцсетях, телеграм-каналах;

–Предложить аудитории вариант самооправдания сдачи в плен (спасти Родину, позаботиться о семье, восстановить справедливость);

План информационной операции

После определения цели информационной операции, особенностей целевой аудитории и сценария воздействия, составляется план информационной операции с указанием необходимых ресурсов и возможных ограничений. По сути, это перечень последовательности действий с кратким описанием времени и места действия, ресурсов, необходимых для каждого действия.

Например, для коммерческой задачи:

–Первичная публикация в газете «Местные кривотолки» материала о проблемах в компании «ККК» (тезисы, время и место публикации);

–Разгон материала о проблемах управления в «ККК» ссылками, комментами и лайками в местных группах соцсетей (тезисы комментов, число лайков, репостов и их интенсивность);

–Публикация в газете «Всезнайка прикамья» материала о злоупотреблениях у основного клиента «ККК» (тезисы, время и место публикации);

–Публикация на портале «Компромат прикамья» о возможных родственных связях в «ККК» (тезисы, время и место публикации);

–Публикация в личном блоге некоего «расследования» о воровстве в «ККК» и проблемах с правоохранительными органами (тезисы, время и место публикации);

–Разгон в соцсетях и телеграм-каналах «расследования» о воровстве в «ККК» тезисы, время и место публикации);

–Вброс в местных группах соцсетей тезиса о неплатежеспособности «ККК»;

–Публикация в газете «Местные кривотолки» обзорного материала о слухах о неплатежеспособности «ККК», обязательно с интервью и пояснениями гендира «ККК».

План содержит предварительную информацию о том какой контент нужно продемонстрировать аудитории, с какой интенсивностью и от каких аккаунтов (источников). План отвечает на вопросы – где, когда, какой материал разместить, как его продвигать, какие ресурсы для этого нужны:

–В какое время (точное или с привязкой к событию);

–Где (СМИ, паблик в соцсети, телеграм-канал…)

–Какое действие совершить

Пример плана операции для задачи «мотивировать ЦА-1 к прекращению сопротивления»:

1. Подготовка информационной операции:

1.1. Создание рабочей группы

1.2. Выделение ресурсов

1.3. Определение ЦА

1.4. Определение сценария воздействия
1.5. Создание ударного контента

2. Активная фаза информационной операции:
2.1. Сформировать у целевой аудитории недоверие к своему руководству
2.1.1. Публикация о воровстве, коррупции, кумовстве руководства в газете «Вестник рядового и сержантского состава»;
2.1.2. Поддержка распространения в соцсетях (соцсеть Хххх. группы 1, 2, 3…, паблики 1 и 2, публикация со ссылкой на газету);
2.1.3. Добавление «фактов» от как-бы простых граждан в формате вводной фразы для репостов в соцсети Хххх, 35 уникальных репостов);
2.2. Сформировать у целевой аудитории ощущение безвыходности
2.2.1. Публикация «независимого эксперта» Иванова-Петрова в своем блоге о некомпетентности руководства, об аморальном поведении их родственников, о предательстве интересов страны;
2.2.2. Поддержка публикации Иванова-Петрова в профильных Телеграмм-каналах (25 репостов);
2.2.3. Призыв правозащитника Сидорова-Козлова в своем блоге о необходимости проведения открытого расследования данного факта;

2.2.4. Поддержка призыва о расследовании в соцсетях (300 лайков, 200 комментов, 100 репостов), регистрация петиции от имени Иванова-Петрова о проведении расследования и ее накачка «сторонниками» (3 тысячи сторонников);

2.3. Сформировать у целевой аудитории желание сдачи в плен

2.3.1. Заявление правозащитника Сидорова-Козлова о том, что люди с той стороны умирают за чужие интересы, что «у нас» их понимают и ценят и вообще гораздо лучше;

2.3.2. Поддержка заявления Сидорова-Козлова репостами (200 шт), лайками (500 шт), комментариями (100 шт);

2.3.3. Предложение целевой аудитории варианта самооправдания сдачи в плен в формате «вы сохраните свои жизни для своих родных» через публикации в профильных телеграм-каналы и группы соцсетей;

2.3.4. Призыв к сдаче в плен в формате рассылки в мессенджерах и публикациях в группах соцсетей и в телеграм-каналах;

3. Завершение информационной операции:

3.1. Закрепление нарративов (при необходимости) – обзорные публикации в локальных СМИ;

3.2. Разгон публикаций в виде репостов (500 шт) в профильных телеграм-каналах и в группах соцсетей;

3.3. Сокрытие следов инфо-воздействия (при необходимости).

В зависимости от масштабов компании, вбросов может быть несколько, в том числе идущих параллельно. К примеру, первая история сообщает о событии, а последующие – развивают тему. Нередко к ним примешиваются и настоящие новости, которые дополняют картину основной ударной истории.

Многофакторный анализ для планирования информационной операции – планирование информационных операций строится на основе многофакторного анализа. Многофакторный анализ – совокупность методов одновременного рассмотрения воздействия многих переменных. Используются для того, чтобы учитывать эффекты множества исследуемых переменных для выявления действия каждого фактора на процесс и построения возможных вариантов развития ситуации.

Возьмем простую почти бытовую ситуацию – вам нужно у незнакомого человека на выставке/конференции получить номер его мобильного телефона. На старте у вас есть две «точки». Начальная, когда вы не знаете номер телефона. И конечная – желаемая цель. Далее описываете пошагово оптимальный по вашему мнению сценарий. Например, он состоит из 4 пунктов:

–Поинтересоваться делами;

–Предложить помощь;

–Узнать, как связаться;

–Получить телефон для связи.

Далее определяем, что на каждом шаге может пойти не так. Например, под воздействием внешних или внутренних факторов. Предположим, на попытку поинтересоваться делами ваш визави сразу просит о помощи. Тогда вы, минуя шаг 2 сразу переходите к шагу 3. Или другой вариант – ваш собеседник в качестве вежливости интересуется вашими делами. В этом случае вы говорите о массе свободного времени и возвращает ситуацию в удобное для вас русло, предложив помощь.

В результате вы получаете перечень действий с возможными отклонениями от основного сценария и шагами по исправлению ситуации.

Методика планирования защиты репутации

Планирование защиты репутации Объекта (противодействия информационной операции противника) может выглядеть так:

–Выявление атаки и ее атрибутирование (вектор, тема, приемы…);

–На основе атрибутирования принятие решения чем и как нейтрализовать;

–Реализация этих контр мероприятий;

–Отслеживание реакции аудитории;

–Корректировка если что-то пошло не так;

–Добавление (по необходимости);
–Реализация «призыва» к действию.

Далее осуществляется проработка возможных вариантов реакций оппонента на ваши шаги и что вы сделаете для нейтрализации активности оппонента.

Например, при начале реализации контр-распространения, противник точно увидит ваши усилия и постарается восстановить ситуацию. Поэтому важно правильно предположить какие действия он может предпринять для восстановления своего сценария воздействия. А затем ответить на вопрос ЧТО вам нужно будет сделать если он поступить таким или иным образом. И так по каждому пункту.

Работа на опережение

Для эффективного отражения информационной агрессии, недостаточно только размещать статьи и интервью, даже если это размещение в топовых изданиях, а заодно в брендированной группе в соцсети. Но чтобы понять почему так происходит и что нужно делать, поставьте себя на место вашего противника, посмотрите на происходящее в интернете его глазами.

Вот вы (то есть ваш противник) видите какую-то публикацию с вашим упоминанием. Как ваш противник ее воспримет? Как отреагирует? Что может предпринять? Например, он увидел, что вышло интервью вашего руководителя в

Форбс, где он делится достижениями и рассуждает об развитии отрасли. Что из этого оппонент может использовать вам во вред? Как он может переврать факты? Может-ли что-то из этого интервью вызвать у оппонента сильные эмоции? А как он может ответить? Именно взгляд на будущие события вот с такого ракурса и лежат в основе общего медиапланирования, а не только что, где и когда разместить.

Вначале, на основании своего общего плана мероприятий (выступления, открытие объектов, проведение переговоров, участие в мероприятиях, еще что-то), составляется план угроз. Это прогнозирование того, как противник может использовать такую новость во вред вам. Какие аргументы или голословные обвинения может озвучить, куда может написать, кому пожаловаться какие еще действия может предпринять. В результате получится – план-график значимых мероприятий с перечнем возможных негативных сценариев реагирования противника на каждое событие. Данный прогноз не является статичным. Но по мере изменения общей ситуации он также может меняться – в него вносятся правки, дополнительные варианты и иные изменения.

Далее, под каждый вариант возможных реакций противника готовится минимум два сценария реагирования:

Что можно противопоставить если противник так поступит;

Что можно сделать заранее чтобы у противника не было возможности использовать инфоповод или эффективность

такого использования была минимальной.

Что можно противопоставить если противник так поступит – при подготовке к возможным реакциям оппонента, возможные варианты реагирования фиксируются и в виде тезисов, что позволит на их основе быстро составить темник для создания ударного контента. Далее под каждый сценарий создается законченный материал (статья, новость, картинка, видео…). Теперь в случае прогнозируемой реакции противника на какое-то связанное с вами событие у вас есть готовый контент для мгновенной публикации и тезисы (возможно с незначительной корректировкой) для составления задания копирайтерам, которые быстро напишут новые материалы.

Что можно сделать заранее – при работе на опережение берутся сценарии возможного реагирования оппонента и прорабатываются с точки зрения «а что можно озвучить заранее чтобы у противника не было аргументов». Это первый уровень противодействия. Гораздо сложнее подготовить «ловушку» для противника. Вы предполагаете, как среагирует оппонент и заранее размещаете в интернете материалы, показывающие его не правоту, а лучше некомпетентность.

Например, вы планируете реконструкцию некоего знакового сооружения. Логично, что СМИ обязательно опубликуют соответствующие сообщения, а значит оппонент узнает и попробует использовать инфоповод. В результате изучения ситуации вы приходите к выводу, что наиболее вероятный

сценарий для оппонента – это заявить о фактическом уничтожении этого сооружения под видом его реконструкции и его перепрофилировании.

Для простого противодействия вы готовите развернутые материалы о том, что функционал сооружения сохраняется, а его технические возможности сильно возрастают.

Для работы на опережение вы до обнародования информации о реконструкции публикуете материалы о сохранении функциональности объекта, например в виде согласования неких условий с руководством города и т.п.. В результате оппонент лишается возможности атаковать, а в случае ожидаемого «выпада» оппонента достаточно дать ссылку на заранее размещенный материал с кратким комментарием о неосведомленности уважаемого оппонента.

Такой подход требует создания специализированного ситуационного центра, работающего круглосуточно с соответствующим набором специалистов и планомерной работы с аудиторией с целью превентивного формирования отношения.

Планирование контр-мероприятий

В ситуации реагирования, когда противники совершил какое-то действие, а вы предпринимаете ответные действия, планирование этих самых действий осуществляется по следующей схеме:

1. Анализ действий противника

1.1. Какую тему эксплуатирует ударный материал
1.2. Какой прием использует для манипулирования
1.3. Кто целевая аудитория атаки
1.4. Цель атаки

2. Прогнозирование последствий (оценка опасности, угрозы)
2.1. Сопоставление восприимчивости аудитории с эффективностью ударного контента
2.2. Предположение о воздействии на аудиторию

3. Выработка вариантов противодействия
3.1. Чем и как можно нейтрализовать воздействие «в лоб»
3.2. Чем и как можно нейтрализовать воздействие опосредованно

На этапе «Анализ действий противника» необходимо понять, что именно предпринял противник. Для этого изучить выявленный ударный контент (сообщение) и понять какую мысль (тему) противник хочет донести до аудитории. Поняв это можно предположить кто именно составляет целевую аудиторию данной информационной операции. Важно – аудиторий может быть несколько и влияние на них может быть разное. И уже исходя из понимания этого, можно спрогнозировать цель информационной операции противника.

Поняв цель информационной операции, можно предпо-

ложить и ее последствия – оценить опасность операции. Для этого нужно сопоставить восприимчивость целевой аудитории с особенностями использованного противником ударного контента:

–Доступен-ли ударный контент аудитории (читают ли эти источники);

–Понятен-ли материал аудитории (язык, символ, смыслы);

–Не вызовет ли контент отторжения у аудитории (табуированные темы, неприязнь к автору);

–На сколько аудитория разделяет точку зрения, представленную в ударном контенте.

–На основе этих данных можно предположить воспримет-ли аудитория информацию данного ударного контента, согласится-ли и совершит-ли провоцируемые противником действия.

И вот только после этого можно приступать к разработке контр-мер. Для чего нужно понимать и учитывать:

1. Уязвимости ударного контента противника:

1.1. Наличие обмана в контенте – позволит дискредитировать сам контент

1.2. Наличие обмана в истории автора контента – позволит дискредитировать противника

1.3. Наличие в контенте непонятного – позволит дискредитировать противника, указав на его глупость

1.4. Наличие в контенте неприятного для аудитории – позволит дискредитировать противника, указав на его глупость

2. Уязвимости источника контента противника:

2.1. Наличие обмана в истории этого источника – позволит дискредитировать противника

2.2. Малоизвестность источника – позволит подорвать доверие к нему

2.3. Принадлежность источника противнику – указать на его ангажированность

На основании этого разрабатываем сценарий противодействия – что, в какой последовательности и с какой интенсивностью нужно донести до атакуемой целевой аудитории.

Для начала нужно пройтись по уязвимостям операции противника. Если есть таковые, то их нужно обязательно использовать. Дискредитация ударного контента, его автора, канала доставки или источника позволяют достаточно быстро нейтрализовать негативное влияние на атакуемую аудиторию.

Если уязвимостей не нашлось, то переходим к непрямому воздействию, которое может быть осуществлено с помощью следующих технологий:

–Высмеивание

–Доведение до абсурда

–Троллинг

–Отвлечение внимания
–Модификация

Важно – прямое противодействие по схеме «дурак – сам дурак» всегда малоэффективно, так-как при всех равных условиях у атакующего преимущество, основанное на эффекте первого впечатления. Поэтому желательно использовать не прямые методы отражения.

Если упущено время, то нужно уже работать с последствиями негативного влияния на аудиторию, а не с самим вбросом.

Разберем на другом примере. Не забывайте, что информационных операций и ударного контента, использующих только одну технологию, практически не бывает. Всегда присутствует в разных пропорциях сочетание транслируемых нарративов, преследуемых целей, аудиторий-мишеней и технологий воздействия. Поэтому и при анализе будут проявляться разные стороны манипулятивных процессов. Предположим, появилась новость:

«Беспилотник морского типа подорвал в Керченском проливе танкер страны-агрессора».

Этап 1. Анализ действий противника

Какую тему эксплуатирует ударный материал? Вероятно следующие:

1. Явные:

1.1. Россия не способна или не хочет защитить своих гражданских.

1.2. Россию можно бить, причем безнаказанно.

2. Скрытые:

2.1. Военная техника России отсталая и не способна противостоять западной.

Какой прием использует для манипулирования (воздействия на аудиторию)? Видимо в разном соотношении:

–Провоцирование страха из-за незащищенности.

–Провоцирование чувства беспомощности.

–Дискредитация ВС, руководства страны и России в целом.

Цель атаки? Кто целевая аудитория атаки?

1. Российская аудитория:

1.1. Снижение боевого духа личного состава МО (отказ от сопротивления):

1.1.1. Формирование негативного отношения гражданского населения к руководству МО.

1.1.2. Формирование чувства безысходности у личного состава МО.

1.1.3. Формирование недоверия личного состава МО к командованию.

1.1.4. Формирование чувства незащищенности и беспомощности.

1.2. Дезорганизация гос-управления (нежелание поддерживать):

1.2.1. Формирование негативного отношения к руководству страны.

1.2.2. Формирование негативного отношения к своим вооруженным силам.

1.2.3. Формирование чувства незащищенности и беспомощности.

1.2.4. Формирование чувства неполноценности.

2. Украинская аудитория:

2.1. Повышение боеспособности ВСУ:

2.1.1. Формирование чувства превосходства.

2.1.2. Формирование чувства уверенности в победе.

2.2. Повышение лояльности населения:

2.2.1. Формирование чувства превосходства.

2.2.2. Формирование чувства уверенности в победе.

2. «Западная» аудитория (в случае трансграничного распространения):

3.1. Повышение лояльности своего населения:

3.1.1. Формирование образа России как врага.

3.1.2. Формирование восприятия России как технологически отсталой.

3.1.3. Формирование восприятия ВС России как недееспособных.

Этап 2. Прогнозирование последствий (оценка опасности публикации, угроз)

Это предположение о том какие будут последствия воздействия на аудиторию данного ударного контента.

1. По российской аудитории:

1.1. Снижение боеспособности ВС из-за:

1.1.1. Снижения авторитета командного состава.

1.1.2. Сомнений в правильности их приказов.

1.1.3. Подозрений в некомпетентности.

1.2. Дезорганизация гос-управления из-за:

1.2.1. Недоверия населения к руководству страны и к госинститутам.

1.2.2. Некорректного принятия решений и формирования не корректных управляющих сигналов;

1.2.3. Промедления в выполнении управляющих сигналов или саботирования их выполнения;

2. По украинской аудитории:

2.1. Повышение эффективности действий ВС в следствии:

2.1.1. Формировании уверенности в своем превосходстве и победе;

2.1.2. Повышения авторитета командного состава;

2.2. Повышение поддержки населения:

2.2.1. Формирование уверенности в своем превосходстве и победе;

2.2.2. Формирование чувства своей правоты в данном конфликте;

3. По западной аудитории:

3.1. Формирование лояльности населения за счет:

3.1.1. Восприятия России как отсталого, нецивилизованного врага;

Этап 3. Выработка вариантов противодействия

И вот только после этого можно переходить к выработке сценариев противодействия. Это ответ на вопрос с помощью чего можно нейтрализовать негативное воздействие данного ударного контента.

Разберем на примере одной целевой аудитории – Российской. Итак – что нужно сделать чтобы данный ударный контент не оказывал негативно воздействия на выбранную аудиторию? В общем виде стратегий противодействия не много:

1. Сделать так, чтобы аудитория не обращала внимание на данный ударный контент;

1.1. Сделать так, чтобы данная ЦА не видела ударный контент:

1.1.1. Организационно-технические мер

1.1.1.1. Цензура

1.1.1.2. Блокировка источников

1.2. Сделать так, чтобы ЦА не обращала внимание на ударный контент:

1.2.1. Отвлечь внимание на более яркое, интересное событие

2. Сделать так, чтобы данный ударный контент не воздействовал на эту ЦА;

2.1. Сформировать недоверие у аудитории к этому контенту, автору или источнику;

2.1.1. Опровержение

2.1.2. Дискредитация источника, автора, канала доставки контента

2.1.3. Высмеивание и доведение до абсурда

2.2. Сделать контент неприятным данной ЦА;

2.2.1. Троллинг

2.2.2. Срач

С организационно-техническими мероприятиями (цензура и блокировка) думаю понятно – это специальные технические мероприятия. Отвлечение внимания аудитории это создание такого инфоповода, на который гарантированно будет переключено внимание аудитории, что приведет вначале к вытеснению, а затем и к потере интереса к новости, по которой работаем в данный момент.

Обращаю внимание, что «прямые» методы противодей-

ствия (опровержение) наименее эффективны в силу ряда причин:

–Официальным источникам аудитория всегда меньше доверяет, чем альтернативным;

–Опровержение всегда попадает в ловушку «первого впечатления», когда первой информации больше доверия;

–Опровержение традиционно эмоционально нейтрально, а ударный контент чаще задействует эмоции, что действеннее на аудиторию.

Дискредитация источника, автора или канала доставки ударного контента это формирование у аудитории недоверия к указанным объектам. В результате такого воздействия срабатывает эффект переноса и аудитория не верит и самому сообщению. В данном случае прием не применим так как подобная информацию будет быстро распространена по неконтролируемым каналам (соцсети, телеграмм и т.п..).

Высмеивание и доведение до абсурда подразумевает «обогащение» ударного контента такими данными, которые либо укажут на его бредовость либо вызовут смех у аудитории. Например:

«Беспилотник морского типа подорвал в Керченском проливе танкер страны-агрессора. Еще 127 аналогичных дрона были уничтожены в море, 14 взорвались при выходе из порта Одессы, а 2 ушли в Турцию и попросили политического убежища.»

«Беспилотник морского типа подорвал в Керченском проливе танкер страны-агрессора. Экипаж беспилотника в составе капитана и бортинженера были подняты на борт танкера. Им оказана необходимая помощь.»

Троллинг и срач близкие технологии, сводящиеся к тому, что вокруг нейтрализуемой новости организуется обсуждение с огромным числом публикаций (комментариев), которые скрывают (топят) основной контент под собой так, что обычный пользователь не захочет докапываться до исходного сообщения.

В информационном противоборстве отражение атаки «в лоб» чаще всего малоэффективно. Тем ни менее это необходимо осуществлять, так как благодаря этому часть аудитории всё же будет защищена от воздействия. Тем ни менее гораздо продуктивнее осуществлять противодействие не прямыми действиями и в несколько шагов, плавно подводя аудиторию к нужному выводу. В результате таких действий аудитория как-бы сама приходит к нужным выводам и по тому доверяет им полностью. Применительно к разбираемому примеру это может выглядеть следующим образом:

1. Подготовить аудиторию к нужным выводам:

1.1. Материалы о наших инновациях:

1.1.1. Активизировать распространение материалов о поставке в войска и использовании современных вооружений.

1.1.2. Разогнать информацию как-бы с передовой о достаточном объеме новых вооружений.

1.1.3. Материал (репортажи и интервью) о том, что и где у нас разрабатывается (без раскрытия гостайны конечно).

1.2. Материалы об отставании противника:

1.2.1. Разогнать тезис об устаревшем западном оружии, его неэффективности на поле боя, больших потерях и постоянных сбоях.

1.2.2. Вбросить и разогнать инфу об интересе стран НАТО к нашим новым образцам и безрезультатных попытках получить их для изучения в силу неспособности придумать что-то похожее.

1.2.3. Вбросить инфу о провалах западных программ разработки нового оружия и перевооружения воск.

1.2.4. Публикация как-бы с той стороны с истерикой на тему, что ничего не получается, всё ломается, личный состав бежит с передовой;

2. Сделать основной модулирующий вброс:

2.1. Об отставании запада в разработках вооружений и не способности в ближайшее время догнать нас

Схема распространения и ресурсы

После проработки общего плана, прорабатывается схема распространения контента (какой контент, когда, через какие ресурсы, с какой интенсивностью демонстрировать аудитории). По сути своей это создание медиаплана данного проекта – составление перечня действий по распространению

ударного контента на каждом шаге плана.

В ходе такого медиапланирования нужно определиться по каким каналам наиболее эффективно доставлять контент до целевой. Тут нужно учитывать особенности аудитории, особенности ударного контента и особенности канала доставки ударного контента. Следующая задача, которую нужно решить это сколько раз необходимо инициировать взаимодействие аудитории с ударным контентом чтобы достичь нужного эффекта. Здесь свои нюансы в зависимости от того, какие психологические приемы вы используете, какова восприимчивость и устойчивость аудитории.

Показатели эффективности

Необходимо также определить критерии, по которым будет приниматься решение о достижении целей информационной операции либо не достижении. Эти критерии нужны для того, чтобы определить нужно вносить корректировку в сценарий операции и повторять воздействие на аудиторию или нет.

Задача крайне непростая, так как нет возможности измерять некоторые параметры, и приходится полагаться только на непрямые методы исследований. Самый «точный» из которых это социологический опрос. Но даже его не всегда есть возможность использовать.

Определение показателей эффективности имеет ряд ограничений, которые необходимо учитывать:

–Невозможность в реальности проникнуть в мысли целевой аудитории измерить произошедшие в результате воздействия изменения;

–Ограниченность в доступе к выбранной ЦА для проведения опросов, а в некоторых случаях и невозможность прямо контактировать с ЦА;

–Если-же в качестве единственного источника информации является интернет, то мы сталкиваемся с еще одним ограничением, существенно влияющим на качество результатов исследования. Это астротурфинг – искусственная активность. Речь об искусственном продвижение контента и накручивании социальных действия (лайки, репосты, комментарии, публикации….).

Обычно в политических или социально-значимых темах таких активностей не просто много, а их объем доходить иногда до 80%. При таких показателях говорить о хоть сколько-нибудь обоснованных выводах, построенных на соответствующих показателях, невозможно. Выходов два:

–Использовать другие показатели – какие?

–Использовать эти-же показатели, но с предварительной очисткой от астротурфинга.

Критериями эффективности воздействия в зависимости от особенностей каждой конкретной операции могут быть:

1. Число пользователей, совершивших целевое действие

1.1. Число вышедших на протестную акцию
1.2. Число посетивших некое мероприятие
1.3. Число проголосовавших определенным образом
1.4. Число подписавших петицию

2. Число пользователей, изменивших поведение в соцсети
2.1. Число реакций «контрольной группы» на тестовую публикацию
2.2. Число публикаций «контрольной группы» на определенную тему
2.3. Число «изменивших мнение» – изменивших тематику своих публикаций и участие в тематических сообществах

Подготовка инфраструктуры

В ходе подготовки инфраструктуры для информационной операции необходимо решить следующие задачи:

–В соответствии с выбранной стратегией информационной операции, определить необходимые силы и средства;

–В соответствии с выбранным сценарием воздействия и уязвимостями аудитории, создать ударный контент под операцию;

–В соответствии с выбранным сценарием воздействия и особенностями восприятия аудитории, подготовить инфраструктуру распространения.

И решить ряд технологических и технических вопросов до начала распространения:

–Какие соцсети будем использовать;

–Сколько нужно аккаунтов для реализации проекта в этих соцсетях;

–Особенности этих аккаунтов;

–Как (с помощью чего) будем управлять этими акаунтами.

Подготовка инфраструктуры распространения ударного контента – В соответствии с выбранным сценарием информационной операции и особенностями восприятия аудитории, готовиться инфраструктура распространения.

Формирование инфраструктуры подразумевает следующие действия:

–Принятие решения о каналах доставки ударного контента;

–Выбор аккаунтов для публикации ударного контента;

–Выбор готового ударного контента (если есть);

–Подбор писателей, копирайтеров, дизайнеров, видео-монтажеров… для создания ударного контента.

Процесс создания структуры для распространения ударного контента в соответствии с планом операции выглядит следующим образом:

1.Выбираем площадку для вброса (первичной публикации);

2.Выбираем площадки для дальнейшего разгона;

2.1. Свои аккаунты;

2.2. Биржи найма аккаунтов;

3.Создаем на выбранных площадках аккаунты/группы/паблики;

4.Адаптируем существующие аккаунты/группы/паблики;

5.Организуем взаимодействие (управление);

5.1. Создаем управляющий аккаунт;

5.2. Настраиваем репостинг;

5.3. Создаем координационную группу.

Принятие решения о канале распространения – это выбор, исходя из особенностей выбранной аудитории и поставленной задачи:

–Место первичного распространения (вброса);

–Канал дальнейшего распространения ударного контента до аудитории;

–Метод разгона ударного контента;

–Метод маскировки.

Выбор места первичного распространения ударного контента (вброса) – это принятие решения о том, где и когда осуществить первое обнародование ударного контента. Такое решение может зависеть от следующих факторов:

–Планируется-ли удаление стартового материала для сокрытия следов;

–Особенности восприятия аудитории;

–Какой вариант маскировки вброса планируется;

–Какой вариант дальнейшего разгона ударного контента планируется;

Доступные способы распространения ударного контента в интернете:

1.Вброс, и последующий посев

2.Скрытное распространение в личных сообщениях

2.1. В соцсетях

2.2. В мессенджерах

3.Публикация в группах

3.1. В «профильных»

3.2. В не «профильных»

4.Методы кибер-преступников

4.1. Дефейс

4.2. Киберсквотинг

4.3. Спам

4.4. Массовый обзвон по IP телефонии

5.Реклама

5.1. В СМИ

5.2. В соцстях

Доступные методы разгона ударного контента:

1.Поисковая оптимизация

1.1. Ссылочная оптимизация

1.2. Накрутка поведенческих факторов

1.3. Накрутка подсказок

2.SMM

2.1. Накрутка соц активности (лайки, репосты, комменты…)

2.2. Организация вовлекающего обсуждения

2.3. Популярные теги (для Твиттера, Инст…)

3.Посев

3.1. Публикациями от себя

3.2. Публикациями в группах

3.3. Комментариями

Принятие решения о методах маскировки ударного контента призвано исходя из особенностей выбранной аудитории и поставленной задачи, выбирать оптимальный метод маскировки воздействия на ЦА:

–Без маскировки – прямое утверждение;

–Имитацией общения;

–От «авторитетного» источника (от ЛОМа);

–Имитацией утечки «секретно» инфорации;

–Имитацией отзывов и высказываний мнений;

–Еще каким-то способом…

Исходя из особенностей выбранной аудитории и поставленной задачи, оператор выбирает подходящий вариант разгона вброшенного ударного контента:

1.Посев;
2.Разгон методами SMM;
2.1. Разгон лайками;
2.2. Разгон комментариями;
2.3. Разгон репостами;
2.4. Разгон ссылками;

3.Массовая рассылка;
3.1. В личных сообщениях;
3.2. В почте;
3.3. В мессенджерах;

4.Публикация на НЕ профильных площадках;
5.Методы кибер-преступников;
5.1. Дефейс;
5.2. Киберсквотинг;
5.3. Спам;
5.4. Массовый обзвон по IP телефонии;

6.Реклама;
6.1. Реклама официальными инструментами сервиса;

6.2. Реклама через биржи рекламы;
6.3. Реклама прямой покупкой;

Исходя из постановки задачи (конечной цели мероприятия), особенностей аудитории, выбранных методов маскировки и разгона ударного контента выбираются наиболее подходящие аккаунты из пула доступных для разгона ударного контента:

–Подобрать под задачу аккаунты, которые будут осуществлять распространение ударного контента и его разгон из имеющихся в управлении;

–Создать новые аккаунты под текущий Проект (дать задание на создание);

–Приобрести и адаптировать аккаунты под текущий Проект (дать задание на приобретение).

Подбор аккаунтов под конкретные действия в рамках определенной информационной операции нацелен на соблюдение следующих условий:

–У ЦА не должно быть отторжения информации от выбранных аккаунтов;

–Выбранные аккаунты должны отвечать специфике информационной операции и распространяемого контента;

–Выбранные аккаунт не должны дезавуировать конечную цель информационной операции.

Чтобы у ЦА не возникало отторжения информации, получаемой от задействованных в информационной операции аккаунтов, эти аккаунты не должны вызывать негативные эмоции у ЦА. Для этого аккаунты необходимо адаптировать под выбранную аудиторию. Такая адаптация может подразумевать изменение:

–Локации аккаунтов под локацию аудитории;

–Язык аккаунтов под язык аудитории;

–Связи аккаунта (френды, группы, паблики) под соответствующие показатели аудитории;

–Профиль аккаунта (увлечение, взгляды, места работы и учебы…) под мировоззрение аудитории;

–Аватар и опубликованные изображения под мировоззрение аудитории;

–Публикации аккаунта под взгляды аудитории.

Своя система распространения

Можно создать собственную систему автоматизации распространения ударного контента. Есть несколько путей технической реализации управления сетью аккаунтов, за исключением ручного варианта:

–Сеть управляемых Android-устройств с единой локацией;

–Сеть управляемых Android-устройств с локацией погруппно в каждой интересующей стране;

–Сеть аккаунтов, управляемых с одного сервера;

–Сеть аккаунтов, управляемых погруппно одним севером для одной страны

–Использование эффекта трансграничного распространения контента (локальные сервисы и связи стран);

–«Внешний» провайдер распространения;

–Использование хакерских технологий.

Сеть управляемых Android-устройств с единой локацией

Сеть управляемых Android-устройств (или IOs-устройств) это набор смартфонов с установленными на них официальными приложениями нужных соцсетей и зарегистрированными с них аккаунтов в этих соцсетях. Эта сеть устройств управляется выделенным сервером управления, который и распределяет задачи между аккаунтами по распространению ударного контента. Размещение такой «бото-фермы» должно быть в месте с устойчивой мобильной связью.

Главный недостаток такого подхода в том, что несмотря на высокое человекоподобие аккаунтов, они все имеют IP одной страны и быстро будут идентифицированы как «русские тролли».

Сеть управляемых Android-устройств с локацией погруппно в каждой интересующей стране

Сеть управляемых Android-устройств (или IOs-устройств) и сервер управления ими расположенные в каждой интересующей юрисдикции. Дополнительно нужен сервер для об-

щего дирижирования всей распределенной структурой.

Наиболее эффективны подход с точки зрения сокрытия координат центра правления и человекоподобия аккаунтов.

Сеть аккаунтов, управляемых с одного сервера

Сеть аккаунтов в нужных соцсетях, координируемых с одного управляющего сервера. На API в нашем случае рассчитывать нельзя, в силу активной борьбы с российским влиянием. Поэтому автоматизация управления возможна только эмуляцией действий пользователя.

Сеть аккаунтов, управляемых погруппно одним севером для одной страны

Создание своей сети управляющих серверов в идеале – в каждой интересующей юрисдикции каждый со своей группой подконтрольных Android-устройств в этой-же юрисдикции. Как минимум одна связка сервер + группа Android-устройств в каждой группе «родственных» юрисдикции (по активности борьбы с «русскими троллями»).

Автоматизация

Автоматизация рутинных процессов в информационных операциях связана с большим числом непрогнозируемых факторов, которые нужно учитывать и со значительной неопределенностью контента как текстового так и визуального.

В основном решения в данной области сосредоточены на следующих направлениях:

Мониторинг, анализ, выявление угроз;

Управление распространением ударного контента;

Создание ударного контента.

При этом направление планирования информационных операций и формирование сценария воздействия на аудиторию под конкретную задачу остаются без соответствующих решений. Это связано с большой вариативностью и неформализованными зависимостями сценариев воздействия от исходных данных по аудитории и цели операции.

Создание ударного контента под операцию

В соответствии с выбранным сценарием информационной операции, восприимчивостью и уязвимостями аудитории, нужно создать ударный контент под данную информационную операцию.

Восприимчивость целевой аудитории определяет то, какой контент, из каких источников и от чьего имени аудитории воспринимает более благосклонно:

–Тип ударного контента (текст, звук, картинка, видео);

–Способ подачи ударного контента (аргументация, эмоции…);

–Оформление ударного контента;

–Автор, от чьего имени подается контент;

Уязвимость целевой аудитории определяет то, какие будут использоваться:

–Варианты тем, используемых для манипулирования аудиторией;

–Приемы манипулирования аудиторией;

–Особенности подачи ударного контента;

–Особенности оформления ударного контента.

–Сценарий информационной операции определяет то:

–Как адаптировать ударный контент под выбранные каналы доставки ударного контента;

–Как адаптировать ударный контент под его будущий «первоисточник».

Традиционные требования к ударному контенту включают следующее:

–Контент должен быть на понятном аудитории языке;

–Контент должен содержать понятную аудитории терминологию, сленг, афоризмы, лексику;

–Контент должен оперировать понятными аудитории тезисами, аргументами;

–Контент должен не вызывать отторжения у аудитории по содержанию, по оформлению, по источнику, за исключением особых случаев, когда цель именно в провоцировании;

–Контент должен располагаться доступных аудитории площадках, а лучше на площадках, которыми аудитория предпочитает пользоваться;

–Площадки с ударным контентом не должны вызывать у аудитории опаски, отторжения;

«Автор» контента должен вызывать у аудитории доверие (за исключением особых случаев):

–Ударный контент должен соответствовать теме и логике информационной операции;

–Ударный контент должен иметь запланированный психологический приём воздействия на аудиторию;

–Быть по теме понятной аудитории и интересной для неё.

Для создания ударного контента обычно используют нанятых или штатных исполнителей. Дело в том, что ударный контент должен вызывать определенные эмоции у аудитории, сделать это может пока только человек.

А вот для многократного «дублирования» с частичным или полным пере формулированием текстового ударного контента уже можно задействовать нейросети.

В масштабных мероприятиях разнопланового ударного контента нужно много так как это не только первичный вброс, но и вспомогательный контент для поддержки основного вброса, а в мероприятиях с использованием фейков нужно много разнообразного контента на одну тему для создания иллюзии массовости.

Исходя из постановленной задачи ответственный за информационную операцию формирует требования к ударно-

му контенту. Для этого вначале выбирается психологический приём воздействия на ЦА с учетом ее особенностей, выявленных на предыдущих этапах. Наиболее используемые приёмы воздействия на аудиторию:

1.Дискредитация;
1.1. Автора;
1.2. Источника;
1.3. Канала;
1.4. Контента;

2.Отвлечение внимания ЦА или привлечения внимания;
3.Отвлечение ресурсов противника;
4.Доведение до абсурда в т.ч. высмеивание;
5.Информационная «прививка»;
6…..

Конечно-же это далеко не все психологические приёмы манипулирования, но наиболее используемые.

Ударный контент, созданный человеком, при наличии опыта у автора, гораздо более эффективен с точки зрения воздействия на аудиторию. Но он-же и наиболее дорог с точки зрения затрат ресурс на его создание. Создание ударного контента вручную живыми исполнителями (авторами, контент-менеджерами, дизайнерами…) требует наличия в оперативном управлении людей соответствующей квалификации. Это может быть организовано приёмом их в штат или

за счет договорённостей с внешними исполнителями.

Для придания человекоподобия автоматическим репостам, помимо технической маскировки, нужна и смысловая. Самый простой способ такой маскировки – это добавление к публикуемому материалу небольшой вводной фразы от короткой «ух-ты» или «Интересное» и подобных до более развернутых вплоть до нескольких предложений типа «Смотрите что тут случайно нашел. Не знаю как вы, а я изучу это подробнее, мало-ли что». Такая вводная фраза не несет определенной смысловой нагрузки, но «меняет» восприятие основного контента и маскирует аккаунты, осуществляющие посев.

Способы создания ударного контента

На этом же этапе создаётся контент, который будет использоваться в качестве ударного. Для чего на основе данных об аудитории и о нужном целевом действии определяется какой тип контента будет использован и определяется содержимое самого контента. После чего выдаются задания на создание ударного контента писателям, дизайнерам, операторам и иным исполнителям.

Вручную

«Ручное» создание ударного контента – это самостоятельное написание нужного объема текстов, создание картинок, видео. В небольших проектах, когда нужна одна статья на

2,5 тысячи знаков и десяток комментов к ней на 100 – 300 знаков, это можно сделать и самостоятельно. Когда нужно два десятка разных статей на одну тему и полторы тысячи уникальных комментов становится уже затруднительно осилить объемы в одиночку. А уж в больших проектах, где нужно на старте полсотни развернутых статей, далее еще по десятку статей ежедневно в течении двух недель, да комментов и вводных фраз для соцсетей тысяч десять, без «писателей» никак.

В этом случае обычно нанимают внешних исполнителей. В не секретных работах такой найм проще всего сделать на соответствующих биржах в интернете, но для наиболее важных или неафишируемых проектов лучше иметь несколько заранее подобранных исполнителей из числа журналистов или пиарщиков.

Бредогенератор

Для коротких, простых текстов в одно предложение, например для поддержки публикации комментариями, можно использовать так называемый «бредогенератор». Его работа основывается на том, что простые предложения имеют простую, заранее определенную структуру, которую можно наполнить перемешивая синонимы. Например, такая структура: подлежащее – сказуемое – всё остальное. Подлежащее – это разные варианты именования Объекта и может иметь следующий вид: «Иван Иванович», «Иван Иванович Ива-

нов», «Гендир завода реактивных косилок». Сказуемое это разные варианты действий Объекта: «встретился», «переговорил», «провел переговоры», «пообщался» и т.п.. А всё остальное в нашем случае с кем Объект совершил это действие: «с трудовым коллективом», «с работниками завода», «с сотрудниками предприятия».

Далее программа берет случайное значение «подлежащего», добавляем случайное значение «сказуемого» и случайное значение «всего остального» и формируем предложение. Из данного набора можно сформировать 4 х 4 х 4 = 64 уникальных вариантов предложений.

БД шаблонов

В интернете непрерывно и параллельно идет множество компаний манипулирования, в рамках которых создается разнообразный ударный контент. Важно организовать выявление и накопление таких ударных материалов. А затем осуществить их классификацию, шаблонирование и хранение для дальнейшего использования в своих информационных операциях.

По оценочным суждениям профессиональных сценаристов уникальных сценариев всего 40, а всё остальное это вариации. А раз так, то вполне можно описать эти варианты – сформировать систему признаков. Далее нужно собрать ударные материалы из разных инфосхваток, классифицировать в соответствии нашим пониманием сценариев и «очи-

стить» от идентифицирующих признаков. Например названия или имена объектов атаки, заменив их на указание места вставки нужного значения (в нужном падеже, числе, времени и т.п.). В результате такого накопления собирается база шаблонов под самые разные варианты атак и контратак.

Классификация таких материалов осуществляется по психологическим приемам, используемым в материале:

–Дискредитация Объекта
–Отвлечение внимания ЦА или привлечения внимания
–Отвлечение ресурсов противника
–Доведение до абсурда
–Информационная «прививка»

Параллельно возможна классификация по сценариям, использованным в ударных материалах (не путать со сценарием информационной операции). Дополнительно, для облегчения поиска подходящего шаблона, нужно тегирование каждого материала по следующим типам тегов:

–Люди
–Организации
–Локация
–Дата-время

Автогенерация

Генеративные нейросети – нейросети, которые генерируют тексты, изображения, видео, аудио, презентации и другие

произведения.

Для создания текста

ChatGPT – это разговорный чат-бот на основе искусственного интеллекта, который может создавать текст на основе любого введенного вами запроса.

OpenAI GPT-4 одна из самых мощных нейронных сетей для генерации текста. GPT-4 способна создавать качественные статьи, ответы на вопросы, продуктовые описания и многое другое.

BERT (Bidirectional Encoder Representations from Transformers) представляет собой предобученную нейронную сеть, которая понимает семантику и контекст текста. Она может использоваться для задачи классификации, извлечения информации и многих других задач обработки текста.

Для создания изображений

DALL-E 2 стала интернет феноменом раньше других нейронных сетей. Это усовершенствованная нейронная сеть, разработанная OpenAI, которая может генерировать высококачественные изображения из текстовых описаний.

Midjourney – это генеративная нейронная сеть, разработанная компанией Artie, специально разработанная для создания 2D и 3D анимаций.

Stable Diffusion – нейронная сеть, генерирующая изоб-

ражение из текстового описания. Важное отличие Stable Diffusion от ранее описанных инструментов состоит в том, что это нейронка с открытым кодом.

Craiyon – люди часто называют ее DALL-E mini, поскольку она выполняет то же самое, что и DALL-E 2 только с менее точным воспроизведением.

DeepDream – это нейронная сеть, разработанная Google, которая позволяет создавать психоделические искусственные изображения, искажая их на основе визуальных шаблонов, выявленных нейронной сетью.

Приемы дискредитации Объекта

Дискредитация самый распространенный и наиболее простой в реализации способ воздействия на аудиторию. Поэтому данную технику рассмотрим детально. Отмыться от негатива, даже если это ложь, условно требует в десять раз больше ресурсов, чем облить грязью. Особенно если у аудитории нет дополнительной информации и нет возможности проверить эти обвинения.

Через указания на слабость (уязвимость)

Допустим у «мишени» есть известная слабость, которая может выражаться в страхах, незначительном, но нежелательном свойстве и т.п.. И об этой слабости атакующий в каждом своем высказывании напоминает аудитории тем самым каждый раз добавляя негатива в восприятие «мишени».

Помните, как 27 моряков с эскадренного миноносца «Дональд Кук» дружно подали рапорты об увольнении с флота? Это произошло через пару дней после того, как при приближении к нашим территориальным водам данного корабля, Су-24 береговой авиации совершил его облет. Рядовое в общем-то событие, американская сторона позволяет себе куда более провокационные выходки, вызвало значительный переполох у моряков, которые должны обладать стрессоустойчивостью в силу своей профессии. Данный инцидент был использован в коллажах дискредитирующих флот США.

Через указание на ошибку

Все рано или поздно совершают ошибки. И эти ошибки, совершенные мишенью в прошлом, атакующая сторона вполне может использовать для воздействия на аудиторию, высмеивая мишень, выставляя мишень в неприглядном виде, показывая эту ошибку как основную и единственную особенность мишени.

Обнародование переписки

Обнародование переписки или телефонных переговоров Объекта, содержащих явно дискредитирующие его данные давно и эффективно используются для удаления неугодных. Примеров очень много от Доминика Стросс-Кана до Вайнштейна и Криштиану Рональду.

Сравнение

Сравнение Объекта дискредитации с заведомо позитивно-воспринимаемым персонажем выпячивает негативные черты мишени и подспудно формирует соответствующее отношение аудитории. Особенно если правильно подобрать изображения. Так в ряде коллажей сравнивали жену Обамы и жену Асада, подобрав соответствующие фотографии. Не самые удачные для Мишель и весьма приличные для Асмы.

Скажи кто твой друг

Обнародование порочащей связи в прошлом или настоящем эксплуатирует эффект переноса негативного отношения с одного объекта на другой. Тем самым формируется нужное отношение аудитории.

Так, в свое время, была представлена общественности видеозапись, на которой лидеры наркокартеля "Los Rastrojos" доставляют Хуана Гуайдо (лидер оппозиции венесуэллы) к вертолету правительства Колумбии, где их встретил губернатор колумбийской приграничной области и глава колумбийских спецслужб. По сути это обвинение в тесной связи с наркобизнесом, что уничтожает репутацию любого политика. После этого скандала Хуан превратился из борца за права и свободы в злодея и потерял большую часть поддержки населения.

Негативная похвала

Такое действие подразумевает публичную похвалу объекта дискредитации. Специфика заключается в том, как похвалили или кто похвалил. По поводу КАК похвалили – явное перехваливание. Например, чрезмерное употребление разных хвалебных эпитетов без подтверждения фактами, хвала за то, чего не делали, хвала с вкраплениями негатива…

Вторая составляющая – это КТО хвалит. Если хвала исходит от негативно воспринимаемого аудиторией объекта, то, скорее, она будет иметь также негативный характер.

Так, недавно, после протестных акций в Москве, в соцсетях получило распространение «благодарственное письмо» телеканалу Дождь от руководства Следственного Комитета за столь качественную трансляцию, что удалось идентифицировать всех провокаторов со стороны протестующих. Учитывая, что телеканал называет себя чуть ли не основной площадкой для работы оппозиции, такая благодарность мягко говоря очень неоднозначно может быть воспринята либеральной аудиторией. Но, по слухам, это фейк, я про «документ».

Косвенная дискредитация

Более «тонкий» способ очернения Объекта атаки это не прямые обвинения, а обвинения чего-то тесно связанного с Объектом. Например, одного из клиентов, который вызывает негативные эмоции у окружающих, а лучше постоянно появляющихся подобных клиентов. Очень похоже на при-

ём «скажи кто твой друг…», но работает не на связи человек-человек, а на любых сочетаниях. Организация-человек, событие-организация, территория-территория и т.п..

Как вариант «прекрасный магазин, широкий ассортимент, приемлемые цены, но в торговом зале постоянно появляются неадекватные личности, которые пристают к покупателям, оскорбляют, всячески мешают…»

Разновидность данного приема – дискредитация через тёзку. Если очень хочется прямо указать на Объект атаки, но это по каким-то причинам невозможно, то создают контролируемый клон, на которого и обрушивают все возможные обвинения. Но читающие о клоне не знают))) Или используют для идентификации объекта в ударном контенте один из нескольких признаков. Например, только имя, а не ФИО полностью.

Подстава

Еще один приём из числа используемых манипуляторами это клонирование сайта жертвы (человека или организации). Если у жертвы нет сайта, то его создают заново. А далее этот сайт используют для распространения информации прямо или опосредованно дискредитирующей жертву. Это может быть просто распространение явной чернухи, а может быть более тонкая работа. Например, для политиков – комментирование новостей с периодическим вкраплением мыслей несколько отличных от позиции жертвы. Иногда такой

ресурс создают для разового вброса компромата.

Разновидность данной технологии – это создание клона некоего авторитетного источника и разовое или периодическое распространение от его имени манипулятивной информации. Нечасто, для повышения эффективности, блокируют сайт, который клонировали. То-ли DDoS, толи жалоба провайдеру, толи взлом…. В результате постоянные посетители в поисках любимого ресурса, с большей вероятностью попадают на сайт-клон.

Еще одна разновидность подставы в управлении репутацией – это создание видимости, что мишень (объект атаки) использует нечто аморальное или противоправное. Например, перед некими уличными мероприятиями, продвигаемыми чиновниками, в соцсетях вдруг появляется информация, о том, что бюджетников отправляют на это мероприятие принудительно и в подтверждение фото такого приказа с замазанными местами, чтобы не наказали того смелого гражданина, кто выложил этот приказ.

Можно и не создавать клоны сайта, а создать видимость некоего действия, которое вроде как совершила «мишень». Но действия, которое будет воспринято аудиторией явно негативно. При этом лучше если это придуманное действие не напрямую связано с основной деятельностью мишени, а косвенно. Частые примеры такого вида атак – это обвинение в аморальном поведении, не связанном с проф-деятельностью, сотрудников организации, репутацию которой надо

уничтожить. В идеале конечно обвинить в аморалке руководителя, но это бывает сложно и опасно, а вот рядовых сотрудников проще. При чем без «обвинительных текстов», достаточно указания на совершение действия, которое аудиторией будет воспринято негативно. И аудитория сама всё додумает.

Теперь чуть посложнее схема. Рассылаем письма блогерам с предложением поддержать идею/мероприятие/человека, который для нас является мишенью (объектом атаки). Тут важно чтобы среди них были те, кто скорее всего не поддержит. А лучше ярые противники. Вот они-то и сделают основную работу – выложат скриншоты этого письма с комментариями типа «вот так с помощью блогеров хотят поддержать/нагнать/усилить».

Еще один вариант – заказываем на биржах публикации с явной и грубой поддержкой мишени, скриншотим, замазываем идентификационные данные (теперь понимаете зачем их на самом деле замазывают) и публикуем от имени анонима с гневным постом вроде «за эту сволочь в соцсетях топять тысячи ботов и троллей, нанятых на биржах».

Опровержение

Кто оправдывается…. Именно так срабатывает большинство опровержений. А если опровержение создал не оправдывающийся, а его противник, то оно будет еще сильнее дискредитировать объект.

Если же удалось спровоцировать противника на оправдательное заявление, то это подарок судьбы, который нельзя упускать – нужно сразу контент такого оправдания разбирать на цитаты и высмеивать, доводить до абсурда, дискредитировать указывая на обман, подтасовку фактов и т.п..

Фейки

Фейк (англ. fake – подделка) – что-то ложное, недостоверное, сфальсифицированное, выдаваемое за действительное, реальное, достоверное с целью ввести в заблуждение.

Как используют фейки

Фейки используют для обмана, для дезинформирования противника. А вот с какой целью вы его обманываете это уже тактика конкретной информационной операции:

–Заманить в подготовленную ловушку;

–Отвлечь внимание от чего-то важного на ложный объект;

–Отвлечь ресурсы противника, ослабив его на нужном вам направлении;

–Дезорганизовать управление противником за счет непонимания ситуации.

Пребывая в неведении относительно того, что вы хотите предпринять, противник не сможет обеспечить себе защиту. Заведите его подальше по ложному следу, напустите тумана, и к тому времени, как он осознает ваши намерения, будет

уже слишком поздно.

Один из эффективных способов скрыть свои намерения – постоянно разглагольствовать о собственных планах и чаяниях, но только не об истинных. Вы будете выглядеть открытым, завуалируете свои намерения и отправите противника в погоню за несбыточным, что отвлечет его ресурсы на бессмысленные действия.

Фейковые фото

Фейковые изображения создаются давно. Одно время для этого был популярен Photoshop. Но последнее время поступают более технологично и используют нейросети.

Сферу внесения изменений в изображения осваивают стартапы, которые создают продукты для оптимизации процессов производства контента: Dowell (проект компании Everypixel Group, Россия), Synthesia (Великобритания), а также ReфaceAI – создатели приложений Doublicat и Reflect (Украина).

Есть несколько сервисов вроде Reflect, Doublicat или Morhine, которые работают в реальном времени со статичным форматами или GIF.

Фейковые видео (DeepFake)

Последнее время созданы программы, позволяющие в видеоролике заменить лицо персонажа на лицо нужного человека. В результате можно в любое видео (хоть документал-

ка, хоть порно) вставить нужного человека и заявить, что это реальная съемка. Такая технология получила название DeepFake.

Из простых пользовательских: FaceSwap, Deep Fake LAB, FakeApp – это десктопное приложение, которое позволяет легко создавать фотореалистичные видеоролики, в которых оригинальные лица заменены на лица других людей.

В 2017 году в интернете начали появляться порнофильмы с участием Галь Гадот, Эммы Уотсон, Скарлетт Йохансон и других известных актрис, не имеющих отношения к индустрии кино «для взрослых». Дальше больше – в Сеть попали фейковые ролики с политиками: Бараком Обамой, Дональдом Трампом, Ненси Пилоси.

Мало того, нейросети уже оперируют и всем видеоконтентом в кадре – генерируют движущиеся пейзажи, убирают объекты или же заставляют двигаться на изображении людей:

–Технология традиционная deepfake (лицо в картинке): Doublicat, FaceApp, Deepfakes web β, DeepFaceLab, Zao;

–Технология face swap (лицо в видео): Reflect, Doublicat, Morhine, Corridor Crew, Ctrl Shift Face;

–Технология GAN (искусственное создание всего кадра): Face Swap GAN, FSGAN.

Фейковые аудио

Недавно компания Тимура Бекмамбетова придумали и

реализовала технологию синтеза голосов знаменитостей, с помощью которой голосом нужного человека можно озвучить любой текст. А значит технически вполне возможно очень достоверно имитировать голос любого человека и сделать «запись» того, что он никогда не говорил.

В 2021 году в ОАЭ мошенники с помощью аудиодипфейка «клонировали» голос директора крупной компании и обманули менеджеров банка, которые перевели на их счет $35 млн.

Фейковые тексты

Также есть решения для создания текста в стиле интересующего персонажа. Нейросеть анализирует авторские текста объекта, под который нужно подстроится, и на основе этих данных корректирует текст под заданный стиль. Так недавно Яндекс показал нейросеть для генерации текста «Зелибоба». А Центр безопасности и новых технологий Джорджтаунского университета на протяжении 6-ти месяцев использовал GPT-3 для генерации дезинформации, включая выдуманные истории, измененные новостные статьи и твиты с определенной степенью дезинформации. И проверял как аудитория их воспринимает. Эффект насторожил всех – ни одна публикация ИИ не была распознана пользователями как дезинформация.

Распространение ударного контента

Активная фаза информационной операции – воздействие на целевую аудиторию заключается в распространении ударного контента, его разгона, отслеживании реакции аудитории и действий противника, корректировки если нужно и сокрытии следов операции.

Здесь нужно реализовать намеченное воздействие на аудиторию, то есть продемонстрировать выбранной целевой аудитории соответствующие ударные материалы с задуманной интенсивностью и используя заранее определенные каналы доставки.

На данном этапе необходимо решить следующие задачи:

Продемонстрировать ударный контент целевой аудитории с заданной интенсивностью;

После демонстрации определить эффективность воздействия на аудиторию;

Скорректировать воздействие на аудиторию если эффективность признана низкой.

Способы реализации распространения

Реализовать распространение ударного контента можно разными способами.

Вручную

Распространение контента, при его незначительных объемах, возможно вручную через подконтрольные аккаунты. Но это при условии, если небольшие объемы контента и не значительная интенсивность распространения. Иначе в одиночку справиться проблематично и нужно нанимать исполнителей и управлять ими.

Другой подход – арендовать чужие аккаунты в соцсетях, формируя соответствующие задания биржах. Это позволяет не тратить время на поддержку аккаунтов и сводит к минимуму взаимодействие с исполнителями (операторами этих аккаунтов). Но нужно внимательно и осторожно формировать задания для них.

Используя рекламные механизмы в соцсетях

Гораздо эффективнее распространять ударный контент эксплуатируя уже готовые механизмы. Например, рекламные механизмы сервисов интернета. В тех-же социальных сетях есть очень развитые и адаптируемые практически под любые задачи механизмы управления таргетированной рекламой внутри соответствующих соцсетей.

Эти встроенные (штатные) механизмы разные в разных соцсетях и потребуется некоторое время для освоения. Да и сами соцсети с разным усердием ведут борьбу как с недобросовестной рекламой, так и с распространением дезинформации. Но при наличии некоторого опыта и креативного подхода вполне возможно использование такой рекламы для рас-

пространения и манипулятивного контента.

Кросспостинг

Некоторую автоматизацию процесса распространения позволяют сделать сервисы кросспостинга. Эти сервисы созданы для упрощения взаимодействия с контентом при условии, что у вас аккаунты в нескольких соцсетях и переключение между ними отнимает время. В результате вы получаете возможность с «одного экрана» видеть, что и где вам написали и также без переключений отвечать от нужного аккаунта в нужной соцсети. Или планировать свои публикации в разных соцсетях.

Кросспостинг – публикация постов в различных социальных сетях и мессенджерах из одной админки. Вам нужно создать только один пост, и он автоматически будет опубликован во всех пабликах и аккаунтах. Например, вы можете разместить новую статью на сайте и сообщить об этом во всех соцсетях, рассказать о новой акции или запустить опрос.

С помощью встроенных инструментов соцсетей

Простейший функционал для кросспостинга есть в самих социальных сетях.

Например во Вконтакте настройки кросспостинга находятся в настройках личной страницы ВК в разделе «Контакты». В других соцсетях есть свои подобные механизмы.

С помощью специализированных сервисов

Есть ряд сервисов, предоставляющих услуги по продвижению вашего контента в соцсетях. Вот некоторые из них:

SMMplanner
SmmBox
Amplifr
Pur Ninja
NovaPress
KUKU.io
INSMM

Использование внешних добровольных помощников

Создание «внешнего» решения, которое используется всеми желающими для своих рекламных целей: продвижение их контента, управление репутацией брендов, маркетинг и т.п..

Решение должно иметь два функциональных уровня. На первом уровне предоставляется всем желающим предоставляется услуга по продвижению их контента в целях PR, управления репутацией брендов, маркетинга и т.п.. На втором уровне, закрытом от внешнего наблюдателя, мы используем систему для решения своих задач, эксплуатируя накапливаемые ресурсы сторонних пользователей. Такой подход позволят:

–Легендировать свою деятельность в данном направле-

нии;

–Знать об устремлениях и планах вероятного противника;

–Изучать ресурсы противника;

–Привлекать «в темную» внешних исполнителей для решения наших задач;

–Управлять своими доверенными исполнителями за пределами контура безопасности;

–Использовать при необходимости чужие ресурсы без ведома их владельцев.

Такое решение может быть реализовано в нескольких форматах:

–Биржи традиционные

–Биржи взаимного продвижения

Использование специализированных сервисов

Подобные внешние сервисы уже есть на просторах интернета и их можно и нужно использовать. Но с учетом того, что к данным ваших проектов могут получить доступ третьи лица….

Биржи традиционные

Биржи традиционные представляют из себя специализированную торговую площадку, где одни желающие могут предоставить за оплату в аренду подконтрольные им аккаунты в социальных сетях для выполнения разных действий

(публикация, репост, комментарий, лайк). А другие желающие могут за оплату нанять эти аккаунты для выполнения этих действий (публикация, репост, комментарий, лайк). Примеры таких бирж:

Блогун
GetBlogger
Sociate
Social Trade
Prolog.yt
Plibber

Взаимное продвижение

Взаимное продвижение отличается от традиционных бирж тем, что оплата услуг осуществляется встречной услугой. Например, за разрешение разместить у себя ударный контент партнера вы получаете возможность разместить свой ударный контент на его площадках.

Эти решения могут быть реализованы разными способами:

1. Традиционный сайт-маркетплейс;
2. Группа/канал в соцсети;
3. Приложение внутри конкретной соцсети;
4. Внешнее приложение для интересующей соцсети.

Такие сервисы позволяют без вложения денег накрутить активности вокруг своих публикаций и френдов своему ак-

каунту. Обычно это используют в самом начале «жизни» бота, когда он выглядит явным суррогатом и реальные пользователи не хотят с ним взаимодействовать.

Использование эффекта трансграничного распространения контента

Для распространения ударного контент не обязательно использовать топовые соцсети в сложной юрисдикции. В сервисах, где ведется активная борьба с «русскими троллями», аккаунты с российскими корнями не дадут создать, а если будут создан, то первая же попытка продвижения токсичного контента с точки зрения силовиков приведет к блокировке такого аккаунта. Для преодоления данного препятствия можно использовать следующие варианты реализации:

1. Использование мелких соцсетей в интересующей стране;

2. Распространение в соцсетях страны с тесными экономическими и социальными связями с интересующей страной.

Использование мелких соцсетей в интересующей стране

Во многих странах есть свои локальные социальные сервисы, которые значительно менее популярны чем глобальные, но зато по этой-же причине и не интересны правоохранителям. А по тому администрация таких сервисов менее критично относится к размещаемым материалам и возника-

ющим дискуссиям. Но материал, заинтересовавши пользователя в такой «мелкой» соцсети, очень быстро отправляется самим пользователем в популярную соцсеть или мессенджер.

В результате вы получаете «ретранслятор» для распространения своего контента. И главное в этой ситуации, что распространителем ударного контента является реальный житель данной страны, а не мифические «русские тролли».

Распространение в соцсетях страны с тесными экономическими и социальными связями с интересующей страной

В ряде случаев сложились устойчивые экономические и социальные связи между странами в силу исторических или иных причин. Например Великобритания – Индия, США – Мексика, Франция – ЧАД, Италия – Алжир, Испания – Аргентина и т.п. Если нужно распространить ударный контент в Великобритании, то можно это сделать через Индийскую аудиторию. Информация, размещенная в Индии и заинтересовавшая аудиторию, очень быстро будет транслирована в Великобританию. Причем распространителем ударного контента является реальный житель данной страны.

Распространение ударного контента проходит в несколько последовательных этапов:

–Вброс – стартовая публикация ударного контента;

–Первичное распространение ударного контента;

–Поддержка самораспространения;
–Закрепление;
–Сокрытие следов если нужно.

Вброс это первичное обнародование ударного контента. Чаще не совсем корректной информации или абсолютного фейка, или реальной информации, но с вкраплениями дезы. Наиболее яркий и известный пример вброса это выступление Колина Пауэла в ООН с демонстрацией некой пробирки с якобы образцом отравляющего вещества, вроде как привезенного прямиком из хранилищ Ирака. Вдумайтесь, стеклянная пробирка с дико-токсичным отравляющим веществом в аудитории с не последними людьми численностью человек двести.

Осуществляя вброс, нужно соблюсти ряд правил чтобы не навредить самому себе. Первая задача – анонимность. Она подразумевает сокрытие личности атакующего и следов, которые могут на эту личность указать. Вторая задача – придание авторитетности, значимости первичному вбросу, чтобы не тратить много ресурсов на искусственную поддержку интереса. Не редко для решения обеих задач прибегают к размещению стартового вброса на иностранной площадке. В зависимости от цели и уровня атаки такой площадкой может выступать все что угодно от простой блог-платформы или форума до известного СМИ или новостного агентства.

Проще всего первую публикацию осуществляется на фей-

ковом сайте новостей или на любой другой площадке, где содержимое публикации никак не контролируются. Далее используется лидер общественного мнения для нужной злоумышленнику целевой аудитории, который публикуя новость у себя осуществляет первичное привлечение внимания и распространение. Такими некритичными к контенту площадками могут быть:

–Фейковый аккаунт в соцсети

–Сайт, имитирующий СМИ или новостной агрегатор

–Сайты агрегаторы компромата

Вброс может быть без маскировки манипулирования или с таковой:

–Создание иллюзии общения (в комментариях к публикации в соцсети, на форуме, под статьей в СМИ…);

–Имитация авторитетного источника;

–Утечка информации;

–Отзыв;

–Петиция;

–Соцопрос…

Первичное распространение

Первичное распространение ударного контента, нацелено не столько на охват аудитории, сколько на подготовительные действия, которые могут выражаться в:

–Информировании задействованных в ИО исполнителей;

–Маскировке воздействия на аудиторию;
–Имитации естественных процессов;

Основное распространение ударного контента

Далее сообщение распространяют боты, тролли, созданные/привлечённые специально для распространения вброса. Помимо распространения, они выявляют и изолируют тех, кто сомневается или пытается вразумить аудиторию.

Сервисы распространения

Для распространения могут использовать специализированное программное обеспечение или сервисы. В качестве таких сервисов могут выступать:

–Биржи
–Кроспостинговые сервисы
–Группы «взаимной поддержки»

Поддержка само-распространения

После того, как вброс доходит до целевой аудитории, начинается его «самораспространение». Пользователи знакомятся с ударным контентом, лайкают и репостят сообщение, делятся им в мессенджерах. В идеале возникает вирусный эффект, который привлекает внимание ещё более широкой аудитории – журналистов и других профессиональных участников медиаполя.

Закрепление

Этот этап используется в долгосрочных кампаниях, призванных осуществить коренные изменения отношения целевой аудитории к чему-то. Для этого запускается несколько последовательных новостных кампаний с использованием разных вбросов. Обычно финальная кампания имеет целью закрепления в сознании аудитории нужных манипулятору идей.

Сокрытие следов

В завершении злоумышленник скрывает следы своей деятельности. Самый простой и самый распространенный способ – удаление стартовой публикации после начала самораспространения вброса. Иногда, вместе с сообщением, удаляется и площадка, на которой был осуществлен первичный вброс.

Реже противник использует для сокрытия следов отвлекающую новость. Используя уже созданную инфраструктуру из ботов, злоумышленник вбрасывает новое сообщение. По своей тематике оно должно совершенно отличаться от прежней фейковой истории, быть ещё более громким, ярким и резонансным. Такая новость переключает внимание аудитории на новую проблему. В результате аудитория «забывает» скрываемый вброс.

Контроль результативности

В ходе информационной операции необходимо понять правильно ли воздействует ваш ударный контент на аудиторию, насколько сильно воздействует и ведет-ли он к достижению цели информационной операции, т.е. совершению аудиторией целевого действия.

Для этого отслеживается изменение в поведении целевой аудитории, изменения в ее контентных предпочтениях. Также отслеживаются действия оппонента для понимания видит ли он наши усилия по манипулированию аудиторией и не предпринимает ли каких-то действий по нейтрализации. По результатом такого наблюдения принимается решение о необходимости внесения корректировки в план информационной операции:

–Нужна-ли смена стратегии;

–Нужна ли корректировка сценариев;

–Нужен ли новый ударный контент;

–Нужны ли иные каналы доставки ударного контента;

–Нужно ли как-то воздействовать на силы и средства противника…

Чтобы понять это необходимо организовать системное наблюдение по следующим направлениям:

–Отслеживание реакции аудитории;

–Отслеживание действий противника;
–Отслеживание распространения информации.

Отслеживание реакцию аудитории

Максимально достоверная оценка возможна только в случае реального контакта с выбранной аудиторией, что может фактически де-анонимизировать как саму информационную операцию, так и сотрудников, в ней участвующих. По этой причине часто невозможен прямо физический контакт с целевой аудиторией.

Поэтому нужна иная возможность ответственному за информационную операцию провести оценку ее результативности. Такую оценку реакции аудитории можно осуществить по косвенным признакам:

1.По действиям аудитории в соцсети;

1.1. По действиям аудитории с нашим ударным контентом;

1.2. По действиям аудитории с контентом по «контрольным темам»;

1.3. По изменению тематики публикаций целевой аудитории;

2.По изменениям в «реале»;

2.1. Изменение числа негативных публикаций по защищаемой теме;

2.2. Увеличение числа запросов к поисковикам по про-

двигаемой проблеме;

Отслеживание действий аудитории с ударным контентом, распространяемым в рамках информационной операции, подразумевает фиксацию лайков, комментариев, и репостов данного контента. Сравнение этих показателей в начале мероприятия и по его окончании позволяет сделать вывод об изменениях настроения аудитории.

Отслеживание действий аудитории с контентом по контрольным темам – это фиксация действий аудитории со специально подготовленным для этих целей контентом. Лайкают или нет, репостят или нет контент, который был выбран в качестве контрольного. До начала информационной операции фиксируется реакция аудитории на контрольный контент. Затем по окончании операции и сопоставляется, что позволяет сделать вывод об изменениях в исследуемой аудитории.

Изменения тематики публикаций целевой аудитории требует отслеживания публикуемых данной аудиторией сообщений с целью выявления изменения отношения к выбранной проблеме:

–Улучшение отношения к проблеме;

–Ухудшение отношения к проблеме;

–Игнорирование проблемы.

Отслеживание действий противника

Противник обязательно заметит чужое воздействие на свою или на атакуемую им аудиторию и предпримет меры чтобы никто не помешал реализации его планов. Вот эти действия, а лучше подготовку к ним и нужно вовремя выявить, чтобы не позволить уже противнику помешать вам.

Для этого нужно отслеживать изменения в медиа-поле соответствующих аудиторий (атакуемой и защищаемой) на следующие развед-признаки:

1.По тезисам (нарративам):

1.1. Новые тезисы (нарративы), которые распространяют в аудитории;

1.2. Модификация этих тезисов;

1.3. Исчезновение тезисов;

2.По площадкам (сайтам):

2.1. Задействование новых площадок;

2.2. Прекращение активности на определенных площадках;

3.По используемым технологиям:

3.1. Использование новых технологий распространения ударного контента.

При изучении изменения в тезисах (нарративах), продвигаемых противником, необходимо обращать внимание на появление тех, которые нейтрализуют тезисы, задействован-

ные нами в рамках нашей информационной операции. Это прямое указание на то, что противник оценил угрозу и предпринимает усилия по ее нейтрализации.

Изменение в используемых площадках и технологиях это указание на изменение сценария противника. Но таковое изменение может быть связано с попытками нейтрализовать наше воздействие, а может быть лишь следствием перехода на новый этап информационной операции.

Отслеживаем распространение информации

В условиях максимальной неопределенности, когда нет возможность «измерить» реакцию аудитории противника, то в качестве ориентиров могут выступать вторичные факторы, например признаки искусственного распространения ударного контента.

Такие данные по вражескому ударному контенту позволяют оценить ресурсы, используемые противником для распространения ударного контента:

–Число задействованных площадок;

–Число действий этих площадок (публикация, лайк, коммент…);

Те-же данные по своему ударному контенту дают возможность оценить интерес аудитории к контенту по скорости его вторичного распространения и действиями с контентом (лайки, комментарии). И в какой-то мере степень влияния на

аудиторию по изменению содержания комментариев к этом контенту.

Вносим коррективы в план

На основании выявленных изменений в инфо-пространстве делается вывод о том предпринимает-ли противник усилия по «стабилизации» ситуации. Если усилия противника выявлены, то они оцениваются на предмет результативности. Оценивается угроза нашей информационной операции от таких усилий и предлагаются варианты изменения уже плана нашей информационной операции.

Такими изменениями могут быть:

1.Изменения в целевой аудитории:

1.1. Выбор новой целевой аудитории;

1.2. Расширение/сужение уже выбранной;

2.Изменения в нарративах – смыслах ударного контента:

2.1. Добавление новых тезисов (нарративов), нейтрализующих или корректирующих воздействие противника;

2.2. Модификация уже используемых тезисов под изменившуюся обстановку;

2.3. Изъятие из сценария неподходящих тезисов;

3.Изменения в технологиях распространения ударного контента:

3.1. Добавление новых технологий распространения и

воздействия;

3.2. Изменение задействованных технологий;

3.3. Изъятие неэффективных технологий из текущего сценария;

4.Изменения в площадках, используемых в рамках информационной операции:

4.1. Добавление новых;

4.2. Изменение задействованных;

4.3. Изъятие неэффективных из текущего сценария;

После внесения изменений в план информационной операции процедура воздействия на целевую аудиторию повторяется с учетом внесенных изменений.

Оценка эффективности операции

Пожалуй, одной из самых сложных задач, является оценка эффективности информационной операции. Сложность заключается в том, что считать показателем эффективности ИО.

Если исходить из целей информационной операции (целевое действие), то совершение этого действия и является показателем достижения цели информационной операции. Вот именно возможность фиксации или измерения целевого действия не всегда бывает простой задачей.

Если целевое действие – это «выход на протестную акцию», то число вышедших и есть показатель эффективности

– их можно посчитать по головам. Если-же целевое действие НЕ выход на такое мероприятие, то это уже сложнее. А если целевое действие – это «проголосовать против кандидата», то во-первых оценить это до подсчета итогов голосования весьма проблематично, а во-вторых всегда есть неопределенность вокруг того как проголосовала ваша ЦА если только она не 100% электората.

Предпосылками правильной оценки результативности являются обозначенные базовые условия и показатели результативности, четко определенные критерии эффективности информационной операции, обозначенные до начала планирования информационной операции.

Во время определения критериев эффективности особенное внимание следует уделить отслеживанию таких показателей, как:

1.Изменения в поведении целевой аудитории:

1.1. совершении или не совершении целевых действий;

1.2. уменьшение работоспособности;

1.3. дезорганизация аудитории;

1.4. заторможенная реакция;

1.5. значительное изменение в поведении;

1.6. значительное изменение в бытовых предпочтениях;

2.Изменения настроений целевой аудитории:

2.1. изменение предпочтительного контента;

2.2. изменение реакции на раздражающий контент;

2.3. изменение тематики публикаций;
2.4. изменение в аргументации своей позиции;

3.Политическая активность аудитории и тому подобное:
3.1. изменение участия в полит-мероприятиях;
3.2. изменение риторики полит-заявлений;
3.3. изменение в предпочтительных источниках информации.