Технологии информационных войн США

1. Определение психологической операции

Современные технологии информационных войн, основанные на манипулятивном управлении политическим сознанием и поведением граждан, исключительно опасны: их главная задача – разделить и поляризовать общество, разорвать его на множество клочков и фрагментов, заставить эти фрагменты искренне ненавидеть друг друга с тем, чтобы затем столкнуть их между собой, инициировав борьбу на уничтожение, или объединить их агрессию в единый поток и направить его против действующей власти. При этом цель информационной войны – сломить волю противника к сопротивлению и подчинить его сознание своей воле. Высокая эффективность информационных атак и растерянность, являющаяся типичной реакцией большинства стран на акции информационной войны, делает информационные войны одним из основных элементов современных гибридных войн, таких как война в Сирии или конфликт в Украине.

Информационная война (ИВ) – это вооруженный конфликт, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия.

Структурно современная информационная война состоит из последовательности информационных операций, объединенных единым замыслом и согласованных по целям, задачам, формам и методам информационного воздействия.

В Соединенных Штатах Америки термин «информационная операция» официально закреплен в полевом уставе Армии США «Психологические операции» FM 33-1. Согласно этому источнику, информационная операция – это «проводимая в мирное или военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные дружественные, враждебные или нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных целей».

В российской практике противодействия информационным войнам под информационной операцией следует понимать последовательность информационных вбросов, разделенных периодами экспозиции, объединенных единым замыслом и согласованных по времени, целям, задачам, объектам и инструментам информационного воздействия.

Американские военные – авторы устава FM 33-1. - выделяют три уровня ведения информационных войн: стратегический, тактический и оперативный. Уровень информационных операций – это именно тактический уровень ведения информационной войны. Оперативный уровень ведения ИВ – это уровень отдельных информационных атак, совокупность которых

составляет одну информационную операцию. Стратегический уровень соответствует собственно информационной войне – особому виду вооруженного конфликта.

С мнением американских военных можно согласиться, добавив к их трехуровневой классификации дополнительно четвертый уровень ведения информационной войны – инструментальный (уровень применения отдельных способов, методов и технологий информационно-психологического воздействия).

Цель информационной войны

Каждому уровню ведения информационной войны соответствует собственная цель.

На стратегическом уровне цель информационной войны ничем не отличается от цели войны традиционной: ее главная цель – военное поражение противника. Которое, в свою очередь, может достигаться либо путем его уничтожения, либо путем подчинения его воли своей (капитуляции). В том случае, если перед организаторами информационной войны ставится задача сохранить потенциал и ресурсы противника, сломив его волю к сопротивлению и, тем самым, подчинив его, целью информационной войны становится обеспечение добровольной подчиняемости противника, выражающейся в его безусловной готовности следовать воле своего куратора. Именно эта формулировка цели ИВ («обеспечение добровольной подчиняемости») впервые появляется в 1990-х гг. в работах Г.В. Грачева и И.К. Мельника[1], сохраняющих свою актуальность и в настоящее время.

На тактическом уровне целью информационной войны является внедрение в сознание и подсознание человека программных установок на следование определенной модели поведения, выгодной организаторам информационной операции. Тем самым достигается базовый для ИВ принцип добровольной подчиняемости, выражающийся в готовности личности, ставшей объектом информационной войны, следовать внедренной в ее сознание модели поведения, причем делать это добровольно, без явно выраженного принуждения.

Моделей поведения, внедряемых в сознание объекта организаторами информационных операций, может быть великое множество. Наиболее известные из них – это модель протестного поведения, используемая для подрыва позиций действующей власти, и модель лояльного поведения, используемая для поддержки власти и проводимого ею политического курса. При этом внешние формы проявления и той и другой модели могут быть схожими: и представители протестного электората, и лоялисты ходят на митинги, устраивают пикеты, демонстрации, иные виды массовых акций, и, в

[1] Грачев Г.В., Мельник И.К. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М.: ИФ РАН, 1999.

общем и целом, ведут себя похожим образом. Только при этом у одних лозунги, направленные «против», а у других – «за», и на митинги лоялисты ходят только на законные и согласованные (они же выступают в поддержку действующей власти).

На оперативном уровне цель информационной войны выражается во внедрении в сознание и подсознание личности программных установок на совершение немедленного ответного действия – как правило, в ответ на сигнальный импульс со стороны какого-либо внешнего раздражителя. Таким действием может быть возникшее здесь и сейчас в ответ на какой-либо информационный повод желание пойти на митинг, приять участие в манифестации, шествии, «марше несогласных», поддержать политическую инициативу, присоединиться к майдану.

На инструментальном уровне цель информационной войны выражается в получении немедленной рефлексивной ответной реакции на внешний информационный импульс-раздражитель (по принципу «стимул-реакция»): например, вступиться за участвующих в драке (услышав призыв «наших бьют!») или немедленно выйти на улицу, влившись в формирующийся поток недовольных и рассерженных граждан, готовый превратиться в политическую толпу. При этом в подсознание человека внедряются установки на совершение именно неосознанных действий строго определенного характера, которые он должен совершить до того, как его сознание включится в процесс и начнет оценивать совершаемые личностью действия с рациональной точки зрения.

В США технологии управления сознанием и поведением людей, основанные на действии внешних раздражителей-«стимулов», вызывающих немедленную рефлексивную реакцию объекта информационного воздействия, изучаются в рамках теории рефлексивного управления, разработанной В.А. Лефевром и др. еще в 60-х гг. XX века.

Роль СМИ в информационных войнах и психологических операциях

Особую роль в современных информационных войнах играют средства массовой информации и коммуникации (СМИ). Они являются, с одной стороны, каналом доведения информационного воздействия до конкретной целевой аудитории (политических элит, лидеров мнений, широких слоев общественности, политически активной молодежи), с другой – выступают непосредственным участником конфликтного взаимодействия. В современных конфликтах СМИ активно используются как средство дезинформации и пропаганды, как инструмент манипулирования общественным мнением, массовым сознанием и поведением граждан, как инструмент прямого давления на оппонентов. Именно через так называемые «независимые» СМИ спецслужбы осуществляют вбросы («контролируемую утечку») информации, компрометирующей их соперников,

дестабилизирующей политическую обстановку в различных странах, инициирующей массовые протесты в стиле цветных революций.

СМИ имеют обыкновение выдавать непроверенную информацию за достоверную, если в ней содержатся элементы сенсационности, тем самым способствуя ее легализации. Экстремисты часто используют СМИ для усиленного разжигания националистический, экстремистский настроений даже в тех регионах, где эти противоречия уже давно не проявлялись; именно прозападные, демократические СМИ формируют романтический образ цветных революций в тех странах, где осуществляются «цветные» государственные перевороты, они же затем легитимируют «хунты», пришедшие к власти. Западные СМИ активно участвуют в формировании образов «стран-изгоев» (в эту категорию попадают все страны, проводящие независимую от США внешнюю политику), провоцируя новые международные конфликты и столкновения.

Организационно-технологическая схема операции информационной войны

Стандартная англосаксонская операция информационной войны представляет собой последовательность информационных вбросов, разделенных периодами экспозиции (информационной «тишины») и согласованных по времени, целям, задачам и объектам воздействия.

С помощью вбросов, содержащих заведомо провокационную информацию, объект информационной атаки пытаются вывести на эмоции и совершение необдуманных поступков, которые затем становятся предметом острой критики и, в конечно итоге, ведут к его дискредитации.

> **Определение:** Информационный вброс – блок специально подготовленной информации, стимулирующей объект информационного воздействия на совершение немедленных ответных действий (в качестве реакции на полученный внешний стимул).

> **Комментарий:** ошибочно считать, что информационный вброс должен содержать только компрометирующую информацию. Содержанием информационного вброса может быть любая информация стимулирующего характера, способная вывести объект атаки из состояния равновесия и побудить его к немедленному совершению спонтанных, неосознанных, необдуманных действий. Если грубая лесть воздействует на психоэмоциональное состояние объекта атаки сильнее, чем компромат или шантаж, заставляя его под наплывом эмоций «терять голову» (временно утрачивать над собой контроль), то вброс будет насыщен именно такого рода информацией.

Любая операция информационной войны начинается с информационного вброса, направленного на объект (мишень) атаки или на его ближайшее окружение. Если одного вброса недостаточно для того, чтобы сломить противника или подчинить себе его волю, в операциях ИВ используют серию информационных вбросов, вбрасываемых в публичное информационное пространство по очереди, последовательно, через заранее намеченные промежутки времени, обеспечивающие эффект экспозиции.

> **Определение:** Период экспозиции – период информационной «тишины», разделяющий два последовательных вброса, предназначенный для считывания и анализа реакции объекта (мишени) воздействия на вброшенную в его адрес стимулирующую информацию (с помощью обязательно присутствующего в схеме операции ИВ механизма положительной обратной связи). В схеме операции ИВ периоды экспозиции - это технические паузы; их присутствие обязательно.

Роль периодов экспозиции («информационной тишины»)

Помимо функции технической паузы, отведенной на считывание ответной реакции объекта атаки, у периода экспозиции есть еще **два дополнительных (специальных) функциональных предназначения**.

Во-первых, период «информационной тишины» дает возможность объекту атаки, не отвлекаясь на посторонние инфоповоды (шумы), захватить и полностью усвоить весь объем вбрасываемой в его адрес информации. Если бы периодов экспозиции не было, множественные информационные вбросы накладывались бы друг на друга и создавали бы «белый шум». При этом вероятность того, что какой-либо элемент «белого шума» «зацепил» бы объект атаки, была бы сведена к минимуму. Если вброс произошел, надо обязательно дать время объекту атаки полностью сосредоточиться на восприятии содержащейся в этом вбросе стимулирующей информации, не отвлекаясь на сторонние инфоповоды и раздражители, не имеющие отношения к проводимой операции ИВ.

Во-вторых, период экспозиции необходим для того, чтобы объект (мишень) атаки, захватив инфоповод, перешел в возбужденное («пограничное») состояние и сам себя психологически «накрутил» до потери сознания. Дело в том, что ничто так не пугает человека, как неизвестность и недосказанность, нечеткость понимания того, что именно ему угрожает, и в какой степени следует этого бояться. И никто так не может напугать человека, как он сам, используя безграничные возможности своего воображения. Столкнувшись с нечетко выраженной, непонятной и неизвестной «экзистенциональной» угрозой, человек начинает метаться, достраивать в своем воображении образ предполагаемой угрозы, дополняя реальные факты вымышленными, еще больше пугается результатов своей «аналитической реконструкции» и в итоге довольно быстро впадает в панику

или прострацию (ступор). В нем происходит психологический надлом, который делает человека послушным, пластичным (как пластилин), управляемым. Он, даже не успев столкнуться с угрозой лицом к лицу и вступить в борьбу, уже готов сдаться.

Напротив, определенность, даже в отношении серьезной угрозы, всегда успокаивает: человек понимает, что ему грозит, видит границы этой угрозы и, осознавая всю серьезность своего положения, тем не менее, начинает мобилизовывать все свои внутренние и внешние ресурсы на борьбу с тем, что ему реально угрожает – с реальными, не выдуманными, угрозами.

В этом плане информационный вброс относится как раз к той категории информации, которая никогда не содержит полной характеристики угрожаемой ситуации, сложившейся вокруг объекта атаки – только намеки. Даже в том случае, если в отношении объекта атаки в ход идет вполне определенный, конкретный компромат, он никогда не выкладывается в публичное информационное пространство сразу, в полном объеме. Напротив, организаторы информационных атак предпочитают держать объект атаки в постоянном, нарастающем с течением времени напряжении, выкладывая компромат частями – для того, чтобы объект не знал, что именно ждет его в следующий раз, какие именно сведения будет содержать очередной вброс. В результате объект атаки начинает ощущать себя «подвешенным на тонкой ниточке», которую в любой момент неизвестный ему недоброжелатель может «перерезать». В этой ситуации, при строгом соблюдении полной информационной тишины в промежутках между вбросами, объект атаки способен сам, без посторонней помощи, накрутись себя до полностью «разобранного» состояния, да еще и совершить в приступе паники множество неадекватных поступков.

Для срабатывания этого эффекта информационная тишина в промежутках между вбросами должна быть полной: любая, даже самая незначительная информация, просочившаяся (случайно или преднамеренно) от организаторов информационной операции, способна внести в ситуацию элементы определенности и тогда объект, не владеющий всей полнотой информации о происходящем и поэтому интенсивно «варящийся в собственном соку», нащупав точку опоры, может неожиданно успокоиться и начать действовать разумно и рационально. Что, в свою очередь, может привести к системному сбою в самой операции и свести на нет ожидаемый результат.

Основная итерационная схема

Для более тонкой настройки на психологические особенности объекта (мишени) воздействия в современных операциях информационной войны используется **многокаскадная итерационная схема с коррекцией**, позволяющая многократно применять метод вбросов по отношению к одному и тому же объекту, последовательно (с каждым новым итерационным циклом) подводя его к искомому психоэмоциональному состоянию,

обеспечивающему продуцирование объектом определённых реакций на внешние стимулы-раздражители.

> **Определение:** Широко применяемый в математике **метод итераций** (последовательных приближений) предполагает организацию поиска точного решения математической задачи путем многократной (циклической) подгонки параметров уже известных ее приближенных значений под наилучший результат, обеспечивающий (в пределах ошибки вычислений или измерений) тождественность обеих частей исходного математического уравнения.

В основе **итерационной схемы**, применяемой в операциях ИВ, лежит принцип многократного (циклического) повторения тактической последовательности действий вида «информационная атака (вброс) - техническая пауза (период экспозиции)» с обязательной коррекцией исходной схемы вброса информации (равно как и содержания вброса) после каждого прогона исходной итерационной схемы (после каждой итерации).

Механизм коррекции

Механизм коррекции, обеспечивающий тонкую подгонку структуры и содержания вброса под индивидуальные особенности психики объекта атаки, обеспечивает обязательное изменение (корректировку) базовых параметров вброса (содержания, установок, стимулов) в зависимости от конкретных особенностей реакции на него объекта (мишени) атаки. Цель вносимых корректировок – выявление уязвимостей в психоэмоциональном состоянии и рефлекторных реакциях поведении объекта атаки («болевых точек») и точное фокусирование поражающего информационного воздействия (параметров вброса) на указанные «болевые точки». Эта цель достигается присутствием в итерационной схеме операции ИВ специального **механизма коррекции**, позволяющего тонко настраивать схему информационного воздействия под индивидуальные особенности ответной психологической реакции объекта (мишени) атаки.

Механизм положительной обратной связи

Действие применяемого в стандартной англосаксонской операции ИВ механизма коррекции основано на **принципе положительной обратной связи**, связывающей объект воздействия с организаторами информационной атаки.

Реализованный в современных операциях ИВ **механизм положительной обратной связи** предполагает обязательное «считывание» и анализ ответной реакции объекта атаки после каждого информационного вброса (которых в операции информационной войны может быть несколько)

и внесение соответствующих корректирующих изменений в исходную схему информационной атаки.

Ответные реакции объекта атаки считываются и анализируются в течение периодов экспозиции, разделяющих вбросы. Конечным результатом работы механизма обратной связи в рамках каждого итерационного цикла становится вычисление **параметров «невязки»** - математических отклонений ключевых параметров проявленных объектом атаки поведенческих реакций от их искомых (ожидаемых) значений, заданных на этапе планирования информационной операции (по существу, это **план/факт** реализации схемы операции ИВ, оценивающий ее эффективность на каждом цикле или этапе).

«Невязки» - это качественный показатель (индикатор) того, что что-то в реализации схемы ИВ пошло не так. Ориентируясь на считываемые значения этих индикаторов, инженеры ИВ корректируют первоначальную схему информационной атаки таким образом, чтобы, с точки зрения соответствия реальных и ожидаемых психоэмоциональных реакций и поведения, демонстрируемых объектом атаки в отчет на очередной вброс в его адрес, каждая последующая итерация (повторение приема «информационный вброс - период экспозиции – коррекция – формирование содержания нового вброса») давала лучший результат, чем предыдущая.

Особенность американского стиля ведения информационных войн заключается в том, что американцы просто не могут нормально работать без обратной связи с мишенью атаки: считывая ее реакции, организаторы операции понимают, что они все делают правильно (если мишень демонстрирует именно те формы поведения, которые являются ожидаемыми и вписываются в сценарий атаки) и что «все идет по плану». Если обратная связь, по каким-либо причинам, разрывается, американских политтехнологов охватывает состояние истерии и паники.

> **Пример:** Накануне Олимпиады в Сочи Президент Российской Федерации В.В. Путин на десять дней пропал из публичного пространства. Он не делал официальных заявлений, не совершал официальных визитов и даже рабочих поездок, не выступал перед СМИ. В результате на третий день «молчания» в американских СМИ началась паника: пропав из публичного пространства, В.В. Путин оборвал канал обратной связи, по которому технологи информационных операций считывали реакции главного объекта атаки и по его реакции убеждались, что «все идет по плану». А здесь канал обратной связи исчез, и одновременно с его исчезновением начала рассыпаться вся схема операции информационной войны, построенная на дискредитации Олимпиады в Сочи. Схем англосаксонской операции информационной войны дала первый очевидный сбой.

Принцип действия многокаскадной итерационной схемы с положительной обратной связью

Действие схемы операции информационной войны представляет собой многократно повторяющийся (циклический) процесс, в ходе которого объект подвергается прямой информационной атаке (в форме вброса информации, провоцирующей объект атаки на немедленное действие). Его ответная реакция (со всеми характерными для данного человека индивидуальными особенностями) считывается по каналам обратной связи, анализируется и поступает в механизм коррекции. На основании выявленных индивидуальных особенностей реагирования объекта атаки на внешние информационные раздражители определяются его «болевые точки», темы и поводы, выводящие человека из состояния равновесия и способные мгновенно его возбудить и довести до крайне неустойчивого «пограничного» психо-эмоционального состояния, в котором он теряет способность контролировать себя и свои действия.

С учетом выявленных «болевых точек» содержание исходного информационного вброса корректируется таким образом, чтобы сфокусировать информационное воздействие именно на этих проблемах, воспринимаемых объектом атаки наиболее болезненным образом. Затем этот вброс вновь вводится в публичное информационное пространство - по референтным (для объекта атаки) каналам связи, и снова бьёт по психике объекта атаки, ломая ее волю к сопротивлению. Только теперь уже – более болезненно. Так продолжается до тех пор, пока объект атаки своими ответными реакциями полностью себя не скомпрометирует, либо до тех пор, пока его воля не окажется полностью сломлена или подчинена источнику внешнего управляющего воздействия – вплоть до полного «удушения» воли противника путем «затягивания на его шее» «петли анаконды».

«Пограничное» психоэмоциональное состояние

Сценарий любой англосаксонской операции информационной войны основан на эффекте эмоциональной накачки объекта воздействия (для этого используются вбросы, содержащие раздражители, болезненно воспринимаемые объектом атаки) с целью перевода его в так называемое «пограничное» состояние.

> **Определение:** «Пограничным» называется состояние, соответствующее высшей точке эмоционального напряжения человека, в котором он практически полностью утрачивает контроль над своими эмоциями. «Пограничное» состояние не относится к расстройствам психики, но и нормой уже не является. Продолжительное пребывание в «пограничном» состоянии ведет к истощению нервной системы, неврозам, предрасположенности к

реактивным проявлениям в поведении (срывам, немотивированной агрессии, истерикам и т.д.) и к разного рода патологиям.

Перейдя в это состояние, человек в течение определенного времени (до реактивной разрядки) находится в крайне нестабильном психическом состоянии, из которого он с легкостью может в любую секунду под влиянием любого, даже самого незначительного, внешнего раздражителя скатиться либо в состояние агрессии, либо в состояние паники или истерии. Часто таким раздражителем становится случайно попавший под горячую руку журналист или журналистка, задавший не вовремя и не к месту не очень удобный вопрос.

Находясь в пограничном состоянии, то есть, в состоянии высочайшего эмоционального напряжения, человек очень быстро растрачивает на поддержание этого состояние все свои внутренние ресурсы и затем начинает судорожно искать «громоотвод» (канал стока) для сброса накопленного им внутреннего напряжения, необходимый ему для разрядки. В результате у объекта информационной атаки возникает новая жизненно необходимая потребность – в немедленной разрядке, здесь и сейчас, поскольку дольше находиться под пиковыми нагрузками он не может. Разрядившись на любом подходящем объекте (журналисте, подчиненном, члене семьи, случайном прохожем), человек получает временное облегчение, но при этом демонстрируемое им девиантное поведение становится информационным поводом для нового вброса.

Структура и основные этапы операции информационной войны

Структура операции информационной войны состоит из мероприятий подготовительного этапа и серии двухкаскадных итерационных циклов, включающих в себя:

- первичный информационный вброс, сопровождаемый вспомогательной операцией по легализации вбрасываемой информации (с этого момента в операции информационной войны начинается I полукаскад);
- следующий за вбросом первый период экспозиции;
- механизм положительной обратной связи, считывающий реакцию объекта атаки на первичный вброс;
- механизм коррекции, формирующий пул информации (для повторного вброса), основанной на вторичных комментариях и оценках исходных фактов (истинных или сфабрикованных), содержащихся в первичном вбросе, а также субъективных оценках эмоциональной реакции объекта атаки на данный вброс;
- повторный вброс информации, основанной на субъективных оценках эмоциональной реакции объекта атаки на предыдущий вброс (с этого момента в операции информационной войны начинается II полукаскад);
- следующий за повторным вбросом второй (в рамках одного итерационного цикла) период экспозиции;

- механизм положительной обратной связи, считывающий реакцию объекта атаки на повторный вброс, в ходе которой у объекта атаки возникает очень сильная настоятельная потребность «немедленно, очень мощно ответить» на атаку в его адрес;

- механизм коррекции, формирующий пул информации (для третьего по счету информационного вброса, с которого начнется новый итерационный цикл), основанной на субъективных комментариях и оценках эмоциональной реакции объекта атаки на повторный вброс;

- вбрасывание в публичное пространство нового информационного вброса, основанного на субъективных комментариях и оценках эмоциональной реакции объекта атаки на предыдущий вброс, сопровождаемый вспомогательной операцией по легализации вбрасываемой информации (в этот момент в операции информационной войны завершается II полукаскад предыдущего итерационного цикла и начинается I полукаскад нового итерационного цикла);

- в операции информационной войны начинается новый итерационный цикл, схема которого идентична предыдущему, только что завершившемуся, циклу.

Далее последовательность операций, описанная выше, повторяется по циклическому принципу до тех пор, пока объект атаки не откажется от сопротивления и подчинится требованиям организаторов информационной операции, либо – «сломается» и, тем самым, «выйдет из игры» - потеряет свою оперативную ценность как для своих, так и для чужих.

Субъективные оценки и комментарии, на базе которых формируются повторный (второй) и третий информационные вбросы, возникают в информационном пространстве в следствие инициирования (организаторами информационной операции, имеющими оперативные контакты в СМИ и «новых медиа») публичной открытой дискуссии относительно адекватности (или, напротив, неадекватности) эмоциональных поведенческих реакций объекта атаки на вбрасываемую в его адрес информацию, способствуя формированию в обществе позиции нетерпимости как по отношению к жертве вбросов, так и по отношению попыток его себя защитить. При этом для участия в открытой дискуссии организаторы информационных операций привлекают подконтрольных им лидеров мнений, блогеров, обозревателей, профессиональных критиков, несистемных оппозиционеров. В результате через некоторое время все информационное пространство оказывается переполнено субъективным оценками, версиями, обвинениями и разоблачениями эмоционального поведения объекта атаки, за которыми полностью теряется исходная причина – фактура, содержащаяся в вбросе. В результате объективная реальность подменяется реальностью сконструированной, а объективные оценки – продуктами социального инжиниринга.

Каскады

Стандартная организационно-технологическая схема англосаксонской операции информационной войны состоит из повторяющихся итерационных циклов (каскадов); при этом каждый из каскадов (итераций), в свою очередь, состоит из двух полукаскадов. **Первый полукаскад** рассчитан на получение первичной (немедленной), сверхэмоциональной реакции объекта (мишени) атаки на только что обнаруженный им информационный вброс. На этой реакции его «ловят» в первый раз.

В стадию **второго полукаскада** начинается операция информационной войны переходит в тот самый момент, когда объект атаки, придя в себя после первого каскада, немного остывает и, осознав то, что его нарочно, умело вывели на эмоции, принимает для себя решение «немедленно и мощно ответить», причем – здесь и сейчас. При этом желание ответить немедленно становится для объекта атаки главной целью и жизненно-важной потребностью, вытесняя при этом другие потребности на второй план и, одновременно, блокируя адреналином «голос разума». В результате объект снова взвинчивает себя до перехода в пограничное состояние и, нуждаясь в немедленной эмоциональной разрядке (сбросу накопившегося напряжения), бросается в контратаку, как правило, абсолютно не подготовленную. На этом его ловят второй раз, после чего операция переходит на новый уровень – в начало следующего итерационного цикла.

Подготовительный этап информационной операции

Началу любой операции информационной войны предшествует стадия подготовки – так называемый подготовительный этап, в ходе которого решается основной объем задач стратегического планирования:

- формируется замысел информационной операции;
- определяются цели, задачи, главный и второстепенные объекты воздействия, которым предстоит стать мишенями для информационных атак;
- определяются каналы доведения управляющего информационного воздействия до объектов атак и иных целевых аудиторий, которые затем будут использованы для информационных вбросов.

Помимо решения задач стратегического планирования, на этапе подготовки разворачивается активная деятельность по:

- формированию вокруг личности и поля деятельности будущего объекта атаки, а также – вокруг его ближайшего окружения, негативного информационного фона, состоящего из различного рода вбросов и утечек компромата (в том числе сфабрикованного), «фреймов» и «ярлыков»;
- сегментации и изучению целевых аудиторий, включающая в себя выявление информационных потребностей и предпочтений будущего объекта атаки, устоявшихся привычек, проявляющихся в работе объекта с информацией, референтных источников получения информации, которым объект привык пользоваться и которым он доверяет;
- тестированию стандартных (типичных) реакций объекта атаки и связанных с ним целевых аудиторий на внешние раздражители и стимулы

(считывание и анализ особенностей ответной реакции объекта атаки на «легкие уколы» в виде зондирующих «пробных шаров»);

- применению социологических методов изучения информационного поля, общественного мнения;

- отдельных мероприятий челночной дипломатии, направленных на предварительное изучение ближайшего окружения и доверенных лиц будущего главного объекта информационной атаки.

В тех случаях, когда это представляется возможным, активно применяются и оперативные методы: к главному объекту атаки (на предмет его изучения) подводится действующая агентура спецслужб.

Выбор объекта (мишени) информационной атаки

Подготовительный этап любой информационной операции включает в себя выбор объекта (мишени) атаки.

Наиболее часто объектом информационной атаки становятся первые лица государства – президент и премьер: с них, как правило, информационная война и начинается. Причина этого предельно проста: первые лица всегда находятся под прицелом, они ведут публичный образ жизни, каждый их шаг, каждое их действие или движение рассматривается сквозь лупу. То, что прощается любому публичному политику, даже самому высокопоставленному и известному, никогда не прощают лидерам государства: они часто просто не имеют права на ошибку, что в определенном смысле роднит их с саперами. В силу своей публичности именно первые лица государства выступают главными ньюсмейкерами и производят большинство резонансных инфоповодов, которым затем дают свою интерпретацию национальные и зарубежные СМИ. Информационная война всегда разворачивается вокруг первых лиц, их действий, реакций на те или иные события, которые на первоначальном этапе тщательно прощупываются и тестируются с помощью заведомо провокационных вбросов ложной информации, запуска в социальных сетях вирусного контента, распространения слухов и сплетен, способных эмоционально «зацепить» хотя бы одного из первых лиц государства и вызвать его ответную резкую, эмоционально окрашенную реакцию.

Однако в качестве объекта информационной атаки может быть выбрана и групповая мишень: например, политическая элита, входящая в окружение президента – тот самый «ближний круг» доверенных лиц, на которых лидер страны опирается. В этом случае целью атаки становится внесение раскола в ряды элиты, стремление заставить их забыть об интересах государства и полностью переключиться на спасение своих личных капиталов. В результате лидер страны в самый ответственный момент может оказаться без поддержки и проиграть.

Информационная атака на окружение президента может быть направлена как напрямую, так и опосредованно, используя «отраженный» эффект. Нередко лидер страны, отбивая информационную атаку, сам

становится ретранслятором информационного воздействия: защищая себя, он отражает информационную волну на свое окружение, своими комментариями многократно усиливая ее поражающий эффект.

Выбор референтных каналов доведения информационного воздействия

Для доведения управляющего воздействия до объекта (мишени) атаки в операциях информационной войны используют только те каналы распространения информации, которым объект доверяет. Такие каналы называются референтным. Именно из референтных каналов объект атаки получает основной поток информации о событиях, происходящих в стране и в мире; именно к этим каналам (источникам) информации он обращается в рабочих и экстренных ситуациях; информацию, поступающую из этих каналов, объект привык считать достоверной, даже если это не так. Информацию, идущую по любым другим каналам, объект просто не воспринимает, не видит и не захватывает.

Если информационный вброс будет осуществлен через нереферентный канал информации, объект на него не среагирует. Более того, вброс пройдет мимо внимания объекта даже в том случае, если в нем содержится компрометирующая информация, разглашение которой представляет для объекта атаки реальную угрозу. В результате, даже располагая качественным, надежным и проверенным компроматом, организаторы информационной атаки могут полностью провалить всю операцию, выбрав не тот канал, обеспечивающий доставку этой информации до «клиента». Это еще раз подчеркивает тот факт, что в информационных войнах мелочей не бывает.

У различных людей референтные каналы получения информации могут быть абсолютно разными. Точнее, у каждого человека есть собственные референтные каналы, которым он доверяет. Во многом доверие к тому или иному каналу определяется не только качеством контента, но и выработанной годами устоявшейся привычкой. Если речь идет о высокопоставленном государственном чиновнике, то, как правило, он получает информацию из внешнего мира из федеральных газет, входящих в президентский пул (таких как «Коммерсант», «Известия» и др.). Этот перечень небольшой, но личные предпочтения чиновника могут свести его вообще к двум-трем источникам, которые чиновник и читает; на изучение других источников у него просто нет времени.

К газетам могут добавляться федеральные телевизионные каналы, особенно, такие, которые чиновники имеют обыкновение крутить в своих кабинетах в режиме нон-стоп. Но и здесь проявляется избирательность, зависящая от конкретных особенностей личности: так, чиновник может игнорировать федеральные сводки новостей на первой тройке каналов (1TV, Россия-1 + Россия 24, НТВ), но при этом чутко реагировать на резонансные информационные поводы, появляющиеся в эфире телеканала «Life» или РБК. Есть такие чиновники, которые доверяют только газетам или только

федеральным телеканалам. При этом многие из них активно в качестве источников информации пользуются сетью интернет, но при этом источники из сети не считают релевантными (то есть, заслуживающими доверия). Исключение составляют чиновники относительно молодого возраста, выросшие в субкультуре смартфонов, планшетов, гаджетов и мобильных приложений. Но даже в этой среде предпочтение отдается довольно узкому кругу источников информации, среди которых могут быть как электронные СМИ, так и блоги, форумы, чаты «живущих в сети» виртуальных профессиональных сообществ.

В категории интернет-источников политической информации особняком стоят крупные международные информационные агентства типа «Блумберг», «Associated Press» или российского «Интерфакс», которые часто первыми дают первичную информацию в виде «голой» фактуры. У этой категории источников также есть свой ядерный электорат, в том числе в чиновничьей среде. Но он, вопреки ожиданиям, сравнительно невелик: в референтных источниках чиновники ищут не установочные данные и чистые факты, а готовые решения, возникающие в результате аналитической обработки первичных материалов.

Вместе с тем, довольно большое количество высокопоставленных чиновников вообще не доверяет традиционным СМИ и «новым медиа», а верят только той информации, которую они с определенной периодичностью получают в виде кратких сводок непосредственно из рук своих особо доверенных лиц. В этом случае вброс любой, даже самой резонансной, информации в СМИ не приведет к результату: даже если СМИ подхватят эту тему и начнут комментировать, организаторы информационной операции не получат от объекта атаки ни одной спонтанной, эмоционально окрашенной реакции. Вывести объект на эмоции помешает фильтр, который отсекает любой неформат (далеко не всякая информация способна вписаться в строгие рамки информационной справки, имеющей свой стиль, формат и максимальный полуторастраничный объём), а также мнение доверенных лиц, способных взглянуть на ситуацию со стороны, спокойно и взвешенно.

В современных информационных вонах эти факторы должным образом учитываются еще на стадии планирования операции, выбора и изучения объекта воздействия, выявления его референтных каналов получения информации о внешнем мире. Под эти выявленные особенности восприятия объектом информации и настраиваются структура, содержание и стилистика информационного вброса, формы визуального, аудиального и кинестетического представления резонансной информации, провоцирующей объект атаки на немедленные эмоциональные действия в публичном пространстве. Если объект предпочитать получать информацию из новостных передач строго определенных телевизионных каналов, вброс будет иметь вид видеосюжета, насыщенного быстро сменяющимися планами, суггестивными приемами и резкими заявлениями разоблачительного характера, «срывающими покровы» с «тайной» политической или личной жизни объекта атаки. Если объект атаки привык

читать утренние газеты (за чашкой кофе или первой выкуренной сигаретой) и этот процесс получения политически значимой информации превратился у него в ежедневный ритуал, вброс появится именно в виде газетной статьи или репортажа, с броским, провокационно звучащим заголовком, с вынесенными в отдельные врезки обвинительными выводами. Если объект привык перепроверять информацию, идущую из традиционных СМИ, через ресурсы сети Интернет и при получении первого же сигнала тревоги сразу же лезет в блогосферу – информационная атака на него начнется именно оттуда, а вброс компроментирующей информации будет осуществлен через блоггеров или лидеров мнений (групп, сообществ) в социальных сетях.

В том случае, если объект атаки является высокопоставленным федеральным чиновником, который не верит никому, кроме очень узкого круга особо доверенных лиц, и получает информацию только из их рук, ситуация с получением доступа к референтному каналу немного усложняется, но не слишком.

Вброс всегда можно осуществить, используя доверенных лиц объекта как ретрансляторов информации: доверенные лица также имеют свои референтные каналы получения информации, на которые можно настроиться. В этом случае вбрасываемая информация обязательно попадет в сводку, ложащуюся на стол «первому», при этом сам автор сводки приложит усилия для того, чтобы переформатировать вброс под стандарт, с которым привык работать объект атаки (то есть сам тонко настроит вбрасываемую информацию под индивидуальные особенности психики «первого лица», обеспечив точное попадание информационного заряда в цель). Для того чтобы вброс был захвачен вниманием доверенного лица, не обязательно в отношение этого человека проводить отдельную активную информационную операцию: достаточно поместить вбрасываемую информацию в поле зрения интересанта, так, чтобы он не мог на нее не наткнуться, работая с собственными референтными источниками (то есть подстав ить ее под «клиента»). Тогда он будет считать, что сам лично эту информацию нашел, и поспешит ее донести «первому лицу», причем как можно скорее. В свою очередь, «первый», получив эту информацию из рук особо доверенного лица в виде привычной ему справки, то есть, из собственного рефератного источника, автоматически воспримет ее как достоверную и не станет относиться к ней критически: доверие «первого» к его личному референтному источнику (особо доверенному лицу) перенесется (спроецируется) и на саму полученную из этого источника информацию.

Какой должна быть информация в вбросе, чтобы ей поверили

Информация, входящая в вброс, должна быть такой, чтобы ей сразу и безоговорочно поверили, без размышлений. В свою очередь, для того, чтобы ей поверили сразу, информация должна быть:

- достоверной;
- полной и точной, имеющей отношение к делу (следств.);

- прийти из компетентного источника.

Как только любому из нас попадается на глаза информационный вброс, к нему сразу возникает несколько вопросов:

- можно ли этой информации доверять?

- можно ли доверять источнику, откуда пришла информация?

- можно ли доверять ее природе происхождения и истории попадания в публичное информационное пространство?

- насколько эта информация точно и полно описывает события, о которых в ней идет речь?

Для получения ответов на эти вопросы для любого информационного вброса разрабатывается легенда, объясняющая происхождение содержащейся в нем информации, и эта легенда придается публичности одновременно с самим информационным вбросом. Делается это следующим образом.

Для того чтобы содержащейся в вбросе информации поверили, она должна быть достоверной, или хотя бы выглядеть таковой. В информационных операциях для наполнения информационных вбросов часто используют не факты, которые легко проверить, а сфальсифицированные данные, вокруг которых создается иллюзия достоверности. Эта иллюзия возникает в тех случаях, если:

- информация, до того, как она попала в открытый доступ (в публичное пространство), была секретной, имела гриф и защищалась спецслужбами разливных стран;

- если для того, чтобы эту секретную информацию добыть, потребовалось выкрасть ее из-под надежной защиты, внедрив для этого (с колоссальным риском) опытных агентов спецслужб в кадровый состав организации, хранившей и защищавшей эти секреты;

- если в публичный доступ эту информацию, украденную то ли у международных криминальных структур, то ли у влиятельных, высокопоставленных, коррумпированных чиновников-спецслужбистов, выложили люди, обладающие безупречной репутацией6 настоящие рыцари-идеалисты, без страха и упрека, поставившие себе цель очищения мира от грязных политиков и коррупционеров, ради этого ежедневно рискующие жизнью, которые по определению не могут врать и подсовывать фальсификат.

Другими словами, если нас удается убедить в том, что содержащаяся в вбросе информация прежде была секретной и тщательно оберегаемой, но затем была украдена агентами спецслужб и передана людям безупречной честности – идеалистам, которые затем и выложили ее в общий доступ, то этой информации можно доверять.

Действительно, рассуждаем мы:

- информацию долго от нас скрывали – значит, она принадлежит к инсайду, «нет дыма без огня»;

- недостоверную и малоценную информацию секретной не назовут и защищать не будут;

- агенты специальных служб действительно могут выкрасть ценную информацию, преодолев любые степени защиты; кроме того, за информацией, не представляющей особого интереса, спецслужбы своих агентов просто так не пошлют;

- благородные рыцари-идеалисты, предавшие публичности эту информацию ради разоблачения коррупционеров, «жуликов и воров», никогда не предадут огласке фальсификат: это невозможно, поскольку противоречит их принципам, ценностям и убеждениям. Таким образом, информации, полученной из «чистых рук», переданной из благородных побуждений, из желания сделать мир чище, невозможно не верить.

И мы довольно часто воспринимаем такую информацию на веру, доверяя предлагаемой нам легенде ее происхождения, дающей, на первый взгляд, исчерпывающие ответы на все возникающие у нас вопросы. Между тем, мало кто при этом задумывается, что верить и доверять предлагаемой информации – это далеко не одно и то же. Особенно, если информация носит ярко выраженный эмоционально окрашенный, вирусный, резонансный характер, и все «факты» и детали, содержащиеся в ней, подобраны именно для усиления резонансного эффекта.

Следующий вопрос, ответ на который всегда содержится в легенде происхождения вбрасываемой информации, касается компетентности ее предполагаемого источника происхождения. Для того чтобы информации можно было доверять, источник ее происхождения обязательно должен быть компетентным:

- иметь доступ к сведениям такого уровня секретности, представленным в вбросе;

- иметь прямое отношение к той сфере деятельности, к которой относятся сведения, содержащиеся в информационном вбросе;

- обладать, по роду служебной деятельности, эксклюзивом, способным, в случае утечки в публичное пространство (случайной или преднамеренной), вызвать грандиозный резонанс с далеко идущими последствиями (вплоть до политических кризисов и отставок).

Очевидно, что информация о новых секретных разработках Минобороны США в области высокоточных вооружений может выглядеть достоверной, но если она придет из источника, не обладающего должным уровнем компетенции (например, из Конституционного суда), никто ей не поверит. Точно также никто не будет верить словам рядового сотрудника ЦРУ, разоблачающего глобальные планы своего высшего руководства: он просто не может их знать, его реальная степень осведомленности ограничивается узким набором частных тем. Для того чтобы вбрасываемой информации действительно поверили, причем сразу и безоговорочно, источником происхождения вбрасываемой информации обычно назначают органы государственной власти высшего эшелона, такие как:

- Администрация Президента США;

- Государственный департамент США;

- Разведывательное сообщество США в целом, возглавляющий его Совет национальной безопасности, ЦРУ или ФБР, в частности;

- Конгресс (Сенат или Палата представителей) США.

Действительно, сомнения в реальной компетенции любого из перечисленных выше ведомств, как правило, не возникают. Для того, чтобы окончательно закрепить эффект сформировавшегося доверия к источнику происхождения информации, довольно часто прямо заявляют, что те или иные «секретные сведения» были переданы журналистам «высокопоставленными сотрудниками Госдепа» или спецслужб, в силу известных причин «пожелавших остаться неизвестными».

В тех случаях, когда содержащаяся во вбросе информация касается нелегальной коммерческой деятельности высокопоставленных зарубежных чиновников, например, их счетов в швейцарских банках или в офшорах, в качестве компетентного источника происхождения информации указывают крупную международную частную структуру (компанию, корпорацию), предоставляющую своим влиятельным клиентам эксклюзивные услуги особой степени деликатности. Именно в такой роли в операции, получившей название «Дело о панамских офшорах» («Панамское досье»), выступила крупная непубличная панамская юридическая компания «Mossack Fontesa», обслуживавшая офшорные операции, услугами которой, как выяснилось, пользовались высокопоставленные чиновники со всего мира, в том числе главы некоторых государств и их особо доверенные лица. Эта компания действительно могла иметь детальные досье на множество мировых политиков, пользовавшихся в разное время ее услугами для вывода или легализации собственных капиталов.

И хотя «Mossack Fontesa» так и не признала факт кражи у нее части особо охраняемых материалов, связанных с офшорными счетами влиятельных политиков и бизнесменов, вряд ли кто-нибудь хоть раз усомнился в том, что она действительно может обладать подобного рода досье. А раз может обладать, то может и утратить - при определенных обстоятельствах, конечно.

Легенда о происхождении вбрасываемой информации всегда включает в себя объяснение того, как именно защищаемая государственными спецслужбами (типа ЦРУ, ФБР, АНБ, БНД, МИ5, СИС) или службами безопасности и разведки частных корпораций (таких как «Mossack Fontesa») информация попала в публичное информационное пространство, оказалась в открытом доступе. Следуя законам формальной логики, произойти это могло только в результате кражи. Именно этот механизм транзита секретной информации от ее первоначальных владельцев к идеалистам-правозащитникам, предающим информацию огласке, присутствует во всех без исключения легендах, объясняющих происхождение сведений, содержащихся в вбросе. В истории с вбросом все оказывается предельно просто: секретную информацию выкрали и затем передали правозащитникам для ее публичной огласки, что здесь непонятного? Все ясно как день. Именно поэтому легенде о том, что секретная информация была украдена, как

правило, хочется верить, не вдаваясь в подробности. Ведь кража – это вполне естественно. При этом в роли вора и взломщика, как правило, выступают либо сотрудник спецслужбы другого государства, внедрившийся в кадровый состав соответствующего разведывательного ведомства (всем известно, что спецслужбы воруют друг у друга секреты – в этом и заключается основная часть их работы), либо предатель, крот, перебежчик, передающий секретную информацию в целях ее публичной огласки ради мести, из чувства обиды или за денежное вознаграждение.

Типичным примером первого случая является агент германской разведки БНД, внедрившийся в панамскую юридическую компанию «Mossack Fontesa» и выкравший большой объем документов, касающихся офшорных операций ее клиентов; примером второй ситуации является перебежчик Эдвард Сноуден, бывший сотрудник американской АНБ.

Последний вопрос, которым задаются обыкновенные граждане, обратившие внимание на информационный вброс, это - насколько содержащаяся в вбросе информация полно и точно описывает те или иные события и характеризует участвовавших в них официальных лиц. Как правило, этим вопросом в обычной ситуации вообще не задаются – вброс по своей структуре наполнен вирусным или клиповым контентом, который воздействует на эмоциональную сферу, фокусируя внимание на испытываемых человеком чувствах и переживаниях, но не на деталях, фактах, подробностях. Подсознательное стремление многих людей обладать «тайными знаниями», инсайдом, обнажающемся при «срывании покровов» с тайной жизни объекта атаки, формирует у внешнего наблюдателя настоятельную потребность верить в достоверность инсайда, отметая рациональные доводы и аргументы. Эту особенность восприятия информации и используют в своих оперативных комбинациях организаторы и технологи операций информационной войны.

При этом подачу информации делают максимально эмоциональной (переводят в эмоциональную плоскость), поскольку для эмоционального восприятия рациональные доказательства не нужны – важен порыв, его наличие; только в этом случае информация воспринимается как априорно достоверная. Если эмоциональный порыв отсутствует – информация, содержащаяся в вбросе, не будет воспринята вообще.

Операции по легализации вбрасываемой информации

Для придания достоверности вбрасываемой информации в современных операциях информационной войны используются так называемые «операции по легализации вбрасываемой информации». По своей природе и функциям это - операции прикрытия (так они называются на языке разведки), придающие вбрасываемой информации вид достоверности, объясняющие ее происхождение (где она хранилась, как попала в руки ее теперешних владельцев) и отвечающие на вопрос о том, из какого источника она пришла – компетентного или сомнительного.

В современных операциях информационной войны вбросы компрометирующей информации никогда не попадают в информационное пространство без сопровождения – только в рамках проводимой одновременно с вбросом операции прикрытия (операции по легализации вбрасываемой информации). Операция по легализации вбрасываемой информации сопровождает информационный вброс всегда.

В современных операциях информационной войны используется три основных вида операций легализации вбрасываемой информации:

- операции «контролируемой утечки» секретной информации;
- публичные заявления, сделанные от имени пожелавших остаться неназванными официальных лиц;
- публичные заявления уполномоченных официальных лиц (президентов, премьеров, глав национальной разведки и др.).

Среди названных выше операций легализации вбрасываемой информации **операции «контролируемой утечки»** являются наиболее распространенным видом операций прикрытия. Сам же термин «контролируемая утечка» в информационные войны пришел из разведки.

> **Определение: «Контролируемая утечка» – это специальная разведывательная операция,** цель которой – дезинформация противника путем передачи ему под видом достоверной информации заведомо ложных или специально сфабрикованных под конкретную задачу сведений секретного характера, путем создания иллюзии случайной утраты этих сведений секретоносителями из-за проявленных ими халатности или неосторожности.
>
> Примеры: 1) История о том, как Хиллари Клинтон оставила в гостинице папку с документами[2] 2) «Панамское досье»[3] 3) ЦРУ прослушивает журналистов (скандал)[4].

---

[2]24 сентября 2016 года американский телеканал ABC, сославшись на итоги расследования ФБР, заявил, что во время визита в Россию в качестве госсекретаря Х. Клинтон оставила папку с секретными документами в своем гостиничном номере. «Когда именно это случилось и что лежало в папке, не сообщается. При этом в ФБР отмечают — папка с государственными тайнами вообще не должна была появляться в гостинице». См.: Хиллари Клинтон забыла секретные документы в московском отеле, передает ABC. [Электронный документ] / 1 канал, 2016, 24 сент. URL: https://www.1tv.ru/news/2016-09-24/310612-hillari_klinton_zabyla_sekretnye_dokumenty_v_moskovskom_otele_peredaet_abc (Дата обращения: 31 марта 2018).

[3] Как сообщает BBC, «в 2016 году в распоряжении крупнейших мировых СМИ оказались миллионы документов панамской офшорной компании «Mossack Fonseca», которые свидетельствуют, что компания помогала клиентам отмывать деньги, избегать санкций и уходить от налогов. В расследовании, проведенном «Международным консорциумом журналистских расследований» (ICIJ) и «Центром по исследованию коррупции и организованной преступности» (OCCRP), упоминаются 72 бывших и нынешних главы различных государств, содержатся данные о секретных офшорных компаниях, связанных

В разведывательных операциях такого типа секретные сведения умышленно теряются секретоносителем (забываются в гостиничных номерах, теряются по пути следования и т.д.), либо остаются на некоторое время без присмотра и в этот самый момент становятся достоянием третьих лиц (журналистов, аккредитивных на секретном объекте, установленных разведчиков противника или их агентуры, и др.), которые затем и придают их огласке, организовав вброс в информационное пространство. Реже сфабрикованными сведениями секретного характера «накачивают» кадрового сотрудник спецслужб, уже совершившего акт предательства или только еще собирающегося стать перебежчиком (пример – Эдвард Сноуден) и затем дают ему уйти за рубеж, предварительно слегка спугнув.

З**аявления от имени псевдоофициальных лиц** (анонимов, выдающих себя за высокопоставленных чиновников Государственного департамента США или ЦРУ, пожелавших остаться неизвестными) также широко используются в целях легализации содержимого информационных вбросов.

Схема этой операции предельно проста: журналисты одного из рейтинговых телевизионных каналов (такого, например, как CNN или Sky News) выпускают в эфир сюжет, связанный с резонансными расследованиями и разоблачениями, в котором они выдвигают обвинения против объекта информационной атаки, ссылаясь на секретные сведения, переданные им неназванными высокопоставленными сотрудниками Госдепа или Разведывательного сообщества США, пожелавшими при этом (в силу вполне известных причин) остаться неизвестными.

с семьями и сподвижниками Х. Мубарака, М. Каддафи, Б. Асада, Т. Блэра» и др. Упоминается там и С. Ролдугин – друг детства В.В. Путина, известный музыкант-виолончелист, которого Запад обвинил в хранении офшорных счетов президента РФ. См.: "Панамское досье": основателей Mossack Fonseca освобождают под залог. [Электронный документ] / BBC, 2017, 22 апр. URL: https://www.bbc.com/russian/news-39677199 (Дата обращения: 31 марта 2018).

[4] Так, 14 мая 2013 года информационное агентство «Associated Press» (AP) «предъявило обвинение властям Америки в незаконном прослушивании телефонных разговоров своих сотрудников. Агентство отправило жалобу генеральному прокурору США Эрику Холдеру. По версии пострадавших, прослушивались несколько десятков телефонных линий агентства. Якобы делал это Минюст США. Агентство называет произошедшее "масштабным и беспрецедентным вмешательством" в работу журналистов по сбору информации. "Телефоны агентства и личные номера репортеров прослушивались. Я узнал об этом в прошлую пятницу. Этому не может быть никакого оправдания", – заявил исполнительный директор Associated Press Гэри Пруитт. По одной из версий, прослушка объясняется работой агентства над историей о предотвращении теракта агентами ЦРУ. В мае 2012 года стало известно, что спецслужбы США не дали преступникам из "Аль-Каиды" взорвать самолет. Выяснилось, что телефонные номера журналистов и редакторов, которые писали на эту тему, прослушивались» См.: Associated Press: Власти США незаконно прослушивают журналистов. [Электронный документ] / Metro, 2013, 14 мая. URL: https://www.metronews.ru/novosti/world/reviews/associated-press-vlasti-ssha-nezakonno-proslushivayut-zhurnalistov-1120727/ (Дата обращения: 31 марта 2018).

Внешне в этих операциях все выглядит логично и заслуживающим доверия:

- журналисты публикуют сведения, полученные от собственных компетентных источников, личные данные которых они имеют полное право не раскрывать (особенно, в том случае, если речь идет о передаче этими источниками журналистам секретной информации, за которой охотятся спецслужбы);

- в компетентности и осведомленности высокопоставленных сотрудников Государственного департамента США или разведки никто не станет сомневаться, с этим обычно соглашаются по умолчанию;

- нежелание конфиденциальных источников раскрывать себя также представляется понятным и обоснованным, так как их раскрытие может привести к немедленному аресту по обвинению в госизмене: передав журналистам секретную информацию, охраняемую государством, они совершили, как минимум, серьезное должностное преступление. Кроме того, если конфиденциальным источником является оперативный сотрудник разведки, то его публичное выступление неминуемо приведет к «засветке» как его самого, так и его агентуры, и такого человека надо будет срочно удалять с оперативной работы, а агентуру, находящуюся у него на связи, спасать всеми доступными способами.

Вместе с тем, в том случае, если зритель по каким-то причинам не поверит предлагаемой ему легенде и захочет убедиться в правдивости сообщаемой телеканалом информации лично, пожелав увидеть самих источников (для того, чтобы убедиться хотя бы в том, что они реально существуют и не выдуманы журналистами телеканала), то его ждет большое разочарование: выясняется, что увидеть персоналии, на показания которых опираются журналисты, нельзя – доступ к ним запрещен. В результате получается, что нас убеждают в том, что эти личности реально существуют и дают разоблачительные показания; но проверить сам факт их существования нет никакой возможности. В этой ситуации становится понятно, что журналисты фактически выступают от имени анонимов, которых, возможно, не существует вовсе, а информацию, вбрасываемую в публичное пространство от их имени, на самом деле никто не крал: ее подготовили сотрудники специальных служб, заинтересованных в организации «контролируемой утечки».

> **Примеры:** 1) «Дело Литвиненко» – заявления, сделанные журналистами британского телеканала Sky News от имени пожелавших остаться неизвестными высокопоставленных сотрудников американской разведки
> .

В отдельных случаях для легализации вбрасываемой информации используются официальные з**аявления уполномоченных официальных**

лиц (президентов США Д. Трампа, Б. Обамы, госсекретаря Д. Керри, официального представителя Администрации Президента США Д. Кёрби и других лиц, облеченных властью).

Принцип действия этой операции предельно прост: официальное лицо уровня президента страны или его заместитель от своего лица заявляют, что та или иная вброшенная в публичное пространство информация – правдива, достоверна и получена от компетентного источника. При этом они как бы ручаются своим весом, авторитетом и репутацией за достоверность сведений, содержащихся в вбросе, и призывают поверить им на слово. И очень многие им сразу же верят, считая, что:

- столь высокие чиновники, облеченные колоссальной властью и не менее колоссальным доверием избирателей, просто в принципе не могут публично говорить неправду;

- президенту виднее, что происходит в стране и в мире на самом деле («жираф большой – ему видней»).

> **Примеры:** 1) Заявление Б. Обамы о том, что Россия, Эбола и ИГ – это одно и тоже[5] 2) Заявление Дж. Керри о том, что Б. Асад сотрудничает с ИГ[6]; 3) Заявление Т. Мэй по делу об отравлении С. Скрипаля[7].

---

[5] 24 сентября 2014 г. Президент США Барак Обама, выступая на 69-й сессии Генеральной ассамблеи ООН, назвал основными мировыми угрозами на сегодня вирус Эболы, действия России в Европе и террористов в Сирии и Ираке. "В то время как мы собрались здесь, вспышка Эболы поражает системы здравоохранения в Западной Африке и угрожает быстро распространиться за ее пределы. Агрессия России в Европе напоминает о днях, когда большие нации угрожали малым, преследуя собственные территориальные амбиции. Жестокость террористов в Сирии и Ираке заставляет нас смотреть в сердце тьмы", - заявил Б. Обама. См.: Обама назвал мировыми угрозами Эболу, действия России и террористов ИГ. [Электронный документ] / РИА Новости, 2014, 24 сен. URL: https://ria.ru/world/20140924/1025469848.html (Дата обращения: 31 марта 2018).

[6] 14 ноября 2015 г. На переговорах в Вене госсекретарь США Дж. Керри назвал президента Сирии Башара Асада "магнитом для террористических группировок". "Асад продает нефть, покупает нефть у ИГИЛ", — сказал Дж. Керри. См.: Керри обвинил Асада в том, что он покупает нефть у ИГ. [Электронный документ] / РИА Новости, 2015, 14 сен. URL: https://ria.ru/syria_chronicle/20151114/1320615451.html (Дата обращения: 31 марта 2018).

[7] 12 марта 2018 г. Премьер-министр ВБ Тереза Мэй, выступая в Парламенте, заявила, что за отравлением С. Скрипаля с высокой вероятностью стоит Россия. «Принимая во внимание то, что …, по нашей оценке, Россия считает некоторых перебежчиков легитимными целями для убийства, правительство пришло к выводу, что Россия с большой вероятностью ответственна за действия, направленные против Сергея Скрипаля и его дочери», - заявила Мэй. См.: Тереза Мэй: за отравлением Скрипаля с высокой вероятностью стоит Россия. [Электронный документ] / BBC, 2018, 12 мар. URL: https://www.bbc.com/russian/news-43378001 (Дата обращения: 31 марта 2018).

Делая с высоты своего официального положения публичные заявления о правдивости того или иного вброса, такие фигуры, как президент или госсекретарь США, выглядят чрезвычайно убедительно; их вес передается той информации, правдивость которой они отстаивают. Между тем, высокое положение вовсе не гарантирует безупречности: даже президенты такой великой державы как США могут сознательно идти на подлог, обманывая свой народ. Таких примеров немало: президент У. Клинтон и госсекретарь Х. Клинтон врали Конгрессу США, находясь под присягой; госсекретарь К. Пауэл сознательно ввел в заблуждение Совет Безопасности ООН, выдав за химическое оружие продемонстрированную им пробирку с обычным белым порошком (мукой или моющим средством); и т.д.

В этом плане, когда президент США Б. Обама, выступая 24 сентября на Генеральной ассамблее ООН, публично заявил, что Россия, вирус Эбола и ИГИЛ представляют собой равные угрозы «свободному миру», а госсекретарь Д. Керри сделал заявление о том, что Б. Асад и ИГИЛ – союзники, очень многие сразу верят заявлениям этих высокопоставленных политиков, не вдаваясь в содержание и детали, не включая критическое мышление и не пытаясь проверить сказанное высокими государственными чиновниками на элементарное соответствие здравому смыслу.

Виды операций «контролируемой утечки»

В свою очередь, операции «контролируемой утечки» информации делятся на четыре вида:

- операция утечки, реализованной путем провоцирования журналистов на кражу секретных материалов, с которых в этот момент снимается защита «от взлома» и они на время становятся доступными для потенциальных похитителей;
- технологии класса «WikiLeaks», предусматривающие маскировку заведомо ложных (сфабрикованных) сведений в большом потоке подлинных, но малоценных документов;
- операции типа «перебежчик» (типичный пример такой операции – побег Э. Сноудена и история с его преследованием);
- операции легализации вбросов через механизм публичных дебатов (технологии класса «Псаки-Метью Ли»).

На каждой из трех указанных выше видов операций «контролируемой утечки» стоит остановиться отдельно.

Провокация кражи секретных сведений

Операции «контролируемой утечки», организуемые путем провоцирования журналистов на кражу секретных сведений и материалов, свидетельствующих о той или иной стороне деятельности высших органов власти или спецслужб – одни из самых распространенных инструментов дезинформации и манипулирования общественным мнением. В основе

операции лежит довольно простая исходная схема: заранее заготовленные «секретные» материалы (папки или файлы), перемешанные – для создания иллюзии достоверности – с другими (подлинными, но малоценными) материалами, вводят в поле зрения журналистов, которых эти материалы не могут не притягивать из-за содержащейся в них эксклюзивной информации о деятельности высших органов власти или спецслужб, инсайда, компромата на лиц, стоящих у власти, сведений разоблачительного характера, которыми всегда располагает разведка.

Статус особой важности и высокой степени секретности придает этим материалам еще большую притягательность. Для того, чтобы журналисты смогли этими материалами негласно воспользоваться, им на время облегчают доступ на секретные объекты, где журналисты случайно могут наткнуться на кем-то забытую секретную папку или включенный компьютер с секретными файлами; легендой для такого проникновения в особо охраняемую зону могут служить различные программы государственно-частного партнерства, предусматривающие временную аккредитацию журналистов при главных офисах спецслужб для «более объективного и всестороннего освещения деятельности органов безопасности, формирования позитивного имиджа разведки» и т.д. Одновременно с этим и с документов, подставляемых под кражу, временно снимается защита «от взлома»; в результате они на время становятся доступными для потенциальных похитителей. Затем остается только создать ситуацию, при которой журналист, пребывающий на охраняемом объекте (например, в штаб-квартире АНБ) на законных основаниях (имея аккредитацию и необходимые формы допуска), физически состыковывается с секретными папками, случайно забытыми на рабочем столе нерасторопным сотрудником спецслужб, забывшем, к тому же, уходя. Запереть свой кабинет на ключ.

В результате секретные папки или файлы оказываются в руках любопытных журналистов, которые, ознакомившись с их содержанием, тут же открывают для себя много нового. После чего у журналиста возникает непреодолимое желание и даже жизненно важная потребность придать эти материалы публичной огласке, причем как можно скорее. Причина этой спешки понятна: надо опередить конкурентов, которые тоже могут узнать о том, как на самом деле эффективно спецслужбы борются с терроризмом, сколько терактов предотвратили и куда идут огромные деньги, ассигнованные Конгрессом, бесследно растворившиеся в тайных операциях разведки за рубежом.

Так журналисты, как правило, и поступают. Разведка, у которой эти сведения украли, тут же заявляет о том, что утечка секретных сведений поставила под угрозу национальную безопасность, а журналисты, выкравшие эти сведения из-по бдительного ока спецслужб, совершили особо тяжкое государственное преступление. Спецслужбы, в свою очередь, «узнав» из газет о краже, приходят в ярость и начинают журналистов преследовать: ставят их телефоны на прослушивание (скрытое документирование), засыпают угрозами и т.д. Мало того, штатные костоломы особо

отталкивающей наружности устремляются в погоню за удачливыми журналистами и так их пугают своим появлением, что журналисты всерьез начинают верить в то, что их жизни угрожает смертельная опасность: спецслужбы решили их «убрать», разумеется, во внесудебном порядке. Это еще больше убеждает журналистов и общество, в которое они выстреливают разоблачительные статьи, обличающие спецслужбы, в том, что сведения, попавшие в руки журналистов – действительно особо важные, достоверные и секретные, раз спецслужбы так взбесились и готовы пойти на все, в том числе на уголовное преступление. Ради того, чтобы эти секретные папки вернуть. Значит, этим сведениям можно верить, причем – сразу и безоговорочно. Тем самым обеспечивается прикрытие и легализация вбрасываемой по указанному каналу информации. Типичным примером такого рода операции является разразившийся в 2013 году в США скандал, связанный с американскими журналистами, аккредитованными при ЦРУ и укравшими документы о проведенных этим ведомством успешных тайных антитеррористических операциях, в том числе, по устранению лидеров террористических ячеек ИГИЛ, Талибана и Аль-Кайды. Вся украденная журналистами информация, оказавшаяся при ближайшем рассмотрении свидетельством высокой эффективности работы ЦРУ, была вброшена в публичное пространство накануне слушаний в Конгрессе, посвященных увеличению ассигнований ЦРУ на антитеррористическую деятельность. Сами же журналисты, обвиненные в государственной измене, едва не получили реальные тюремные сроки; некоторых из них (по их собственным заявлениям) в горячке преследования и травли спецслужбы едва не ликвидировали (опираясь на советующие нормы «Патриотического акта»).

> **Пример:** Скандал с американскими журналистами, аккредитованными при ЦРУ и укравшими документы о проведенных ЦРУ успешных тайных антитеррористических операциях[8].

[8] Агентство «Associated Press» (АР) обвинило власти США в прослушивании телефонов своих журналистов. В своем заявлении АР назвало действия правоохранительных органов Соединенных Штатов «масштабным и беспрецедентным вмешательством» в работу информационного агентства. По заявлению АР, сотрудники правоохранительных органов США в апреле-мае 2012 года отслеживали и записывали исходящие звонки с личных и рабочих телефонов сотрудников агентства, с телефонов корпунктов АР в Нью-Йорке, Вашингтоне и Хартфорде, штат Коннектикут, а также из корпункта в Палате представителей Конгресса США. В общей сложности велась прослушка 20 телефонных линий, используемых агентством и его журналистами. Американские СМИ связывают прослушку телефонов АР с тем, расследованием ФБР, связанным с публикацией АР от 7 мая 2012 года. Тогда «Associated Press» сообщило о предотвращенном теракте, который «Аль-Каида» планировала устроить на борту одного из самолетов, летевших в США. В своем сообщении агентство также раскрывало некоторые подробности спецоперации, проведенной ЦРУ в Йемене. Глава ЦРУ Джон Бреннан назвал публикацию журналистами подробностей этой операции «несанкционированным и опасным раскрытием засекреченной информации». Расследованием этой темы занимались шестеро

Технологии класса «WikiLeaks»

Технологии класса «WikiLeaks» также являются широко используемыми в настоящее время инструментами сокрытия, маскировки и легализации вбрасываемой информации. Их действие основано на факторах, ограничивающих способность человеческого сознания критически воспринимать, усваивать и анализировать поступающую ему извне информацию, если поток падающей на человека информации - избыточен.

Любой человек способен воспринимать и усваивать информацию, содержащуюся в потоке, если интенсивность потока не превышает предельных значений, определяемых индивидуальными способностями индивидуума; при превышении же порогового значения человек уже не будет контролировать весь поток, а лишь ту часть информации, которую он в спешке из этого потока извлек. Если при этом он еще будет пытаться проверить каждое выхваченное им из потока сведение на достоверность, то его мозг очень скоро перегреется и вообще потеряет на время свободность что-либо анализировать. В этом случае природа человека подсказывает ему рациональный выход из ситуации: не зачем проверять весь поток, достаточно выбрать в случайном порядке несколько документов, проверить их на подлинность и результат проверки распространить на все оставшиеся в потоке документы, сведения, справки и сводки. В математике такой метод называется методом экстраполяции – достраивания кривой по нескольким значениям, в отношении которых допускается их корректность (подлинность). То есть, если в массе документов, возникших однажды на сайте типа «WikiLeaks», есть несколько, достоверность которых легко проверяется, то у человека, лично извлекших эти документы и убедившегося в их подлинности, возникает настоятельное желание воспринимать и остальные документы в этом массиве как подлинные, потому что они – такие же, как и те, прошедшие проверку. Поэтому любой, даже очень критически настроенный человек, зашедший на подобного рода сайт, всегда ограничится выборочной проверкой всего лишь нескольких документов, а подлинность других будет уже воспринимать на веру, по умолчанию, – в том, конечно, случае, если выбранные им для проверки документы его не разочаруют.

Технологии класса «WikiLeaks» осуществляют маскировку заведомо ложных (сфабрикованных) сведений, помещая их в избыточно большой поток подлинных, но малоценных документов. Как правило, это – сведения о переписке какого-нибудь американского дипломата и высокопоставленного военного накануне очередной войны в Заливе. В этой переписке адресаты

журналистов из тех, чьи звонки могли прослушиваться. В феврале 2013 года в рамках этого расследования директор ЦРУ Джон Бреннан был допрошен уже в качестве подозреваемого в соучастии. ФБР подозревало его в передаче информации о спецоперации агентству АР. Бреннан все предположения и подозрения категорически опроверг. См.: Власти США прослушивали журналистов Associated Press. [Электронный документ] / МП, 2013, 14 мая. URL: http://mir-politika.ru/4772-vlasti-ssha-proslushivali-zhurnalistov-associated-press.html (Дата обращения: 31 марта 2018).

могут разрывать страшные планы готовящейся агрессии против Саддама Хусейна, ругать правительство США, раскрывать интригующие детали специальных операций ЦРУ, в том числе по подкупу и ликвидации лидеров Аль-Кайды, и т.д. Эти сведения могут выглядеть чрезвычайно интересно, возбуждать любопытство, но оперативной ценности при этом совершенно не представлять: дело было давно, дипломат и генерал, участвовавшие в переписке, давно уже отошли от дел и тихо мирно живут на пенсии, Ирак взяли, Саддама казнили. Никого в реальности по этим сведениям ни привлечь к ответственности, ни зацепить, ни, тем более, завербовать не удастся. При этом несложно убедиться, что они – подлинные, и когда-то видимо представляли часть государственной тайны.

Именно такие документы и попадаются на глаза в первую очередь. Они легко проверяются, и каждый результат проверки формирует чувство все большего доверия к той информации, которая содержится в оставшемся массиве. В какой-то момент критическое отношение исчезает совсем и уступает априорной вере в то, что все документы – подлинные. И вот тогда-то на глаза попадаются документы, имеющие прямое отношение к событиям сегодняшнего дня. Они, в отличие от «давно протухших» переписок военных и дипломатов, остры и актуальны, в некоторой степени даже сенсационны; они содержат разоблачения тайных операций, махинаций и афер, проворачиваемых политиками, все еще находящимися у власти. И поэтому в их подлинность очень хочется верить. Но именно эти документы как раз и могут оказаться подделкой, искусно вброшенной в массив подлинны документов, чтобы там на время затеряться.

В этом плане сайт сенсационных разоблачений противоправной деятельности американских властей и спецслужб «WikiLeaks» действует как ресурс, используемый ЦРУ «втемную» (манипулируя идеалистом Ассанжем). Не случайно на определенной фазе разразившегося в 2016 году скандала с панамскими офшорами («The Panama Papiers») именно на сайте «WikiLeaks» появился массив документов, из которых следовало, что главной целью панамского досье было скомпрометировать именно Президента Российской Федерации – при всем при том, что о В.В. Путине в документах «панамского досье» не было сказано ни слова[9]. «WikiLeaks» в этом плане использовался организаторами скандала как страховочный канал информационного воздействия, задача которого – довести мысль о причастности российского руководства к панамским офшорным операциям даже для самых непонятливых. Это такая типичная для информационных операций «повторная подсветка» исходного события с «правильной» (корректирующей) его интерпретацией: тем, кто сразу не понял, с помощью

[9] 6 апреля 2016 года «Wikileaks» написала в своем твиттере, что «Атака на Путина была осуществлена OCCRP, она была нацелена на Россию и страны бывшего СССР и была профинансирована USAID и Соросом». См.: Wikileaks обвинила в утечке «панамских бумаг» USAID и Сороса [Электронный документ] / Forbes, 2016, 6 апр. URL: http://www.forbes.ru/news/317323-wikileaks-obvinila-v-utechke-panamskikh-bumag-usaid-i-sorosa (Дата обращения: 31 марта 2018).

WikiLeaks доходчиво объяснили, что связь «панамского досье» с первыми лицами российского государства существует, эта связь прямая и явная.

Операции типа «перебежчик»

Операции «перебежчик» - одни из самых известных в истории специальных служб. Это операции по дезинформации противника путем засылки к нему агента-перебежчика. Перебежчик переходит на сторону противника, принося с собой особо ценные, охраняемые, секретные сведения. Если перебежчик является агентом спецслужб и специально засылается к врагу, то сведения, передаваемые им противнику, могут носить ложный характер, способный ввести руководство противника в заблуждение и тем самым повлиять на принятие им управленческих решений. Не менее часто встречается схема, в которой сотрудника спецслужб, склоняющегося к измене Родине (переходу на сторону противника), специально накачивают сведениями секретного характера, часть которых ловко подделана самими спецслужбами, а затем дают ему возможность перебежать к противнику, имитируя в некоторых случаях для правдоподобности погоню.

История Эдварда Сноудена очень хорошо вписывается в эту схему. Э. Сноуден, сотрудник АНБ, 1983 года рождения, в 2013 году бежал из США, похитив и унеся с собой секретные документы и файлы этой специальной службы, составляющие гостайну. Предварительно в начале июня 2013 года Сноуден передал газетам The Guardian и The Washington Post секретную информацию АНБ, касающуюся тотальной слежки американских спецслужб за переговорами между гражданами различных государств. Свои действия идеалист Э. Сноуден объяснял как борьбу за свободу и права человека против преступного разведывательного сообщества США, грубо эти права нарушающие. Однако есть основания полагать, что причиной побега Сноудена стало не стремление его к восстановлению справедливости, а затяжной конфликт с сослуживцами, вызванный сложным характером американца, в ходе которого Сноудена внутри АНБ просто начали травить. В результате его побег стал, скорее всего, не актом борьбы, а актом мести, которую затем сам Сноуден облек в форму самопожертвования ради «выведения на чистую воду» преступников, свивших гнездо в спецслужбах США.

Существует версия о том, что, увидев девиантное поведение Сноудена и постоянные конфликтов с коллегами, сопровождаемое все большим замыканием Сноудена в себе, его руководство решило не увольнять его по статье, а дать возможность набрать побольше секретной информации и затем с этой информацией сбежать в РФ. Увидев, что Сноуден, пользуясь служебным доступам к архивам секретных документов, начинает собирать досье на тайные операции АНБ, ему дали возможность собрать довольно большой объем секретных файлов, большая часть из которых была подлинной (но малоценной), а затем чем-то напугали и побудили его экстренно сорваться с места, прихватив эти сведения с собой. Сноуден так и

сделал. При этом за Сноуденом была организована погоня из лучших агентов-ликвидаторов ЦРУ, которые гнались за ним вплоть до посадки в самолет, следующий в Гонконг, но, по неизвестным причинам, так и не догнали.

Организованная по всем правилам детективного жанра погоня, упустившая, впрочем, Сноудена на финишной прямой, и грозные обвинения в измене и шпионаже преследовали цель убедить мировое сообщество и руководство той страны. Которое в итоге Сноудена приютило, в том, что он действительно украл у АНБ и ЦРУ сведения чрезвычайной ценности и важности, и при этом серьезно рисковал жизнью, вывозя их за рубеж. Между тем, агентов ЦРУ, перехватывавших в прошлом подобного рода же перебежчиков десятками, сложно обвинить в потере профессионализма: Сноудена при желании могли вообще не выпустить из США живым. Именно поэтому реальной представляется версия об инсценировке его побега, о чем Сноуден, разумеется, даже не догадывался. При этом среди секретных материалов, вывезенных им за рубеж и попавших в руки РФ, наверняка присутствовали и документы, специально сфабрикованные ЦРУ с целью дезинформирования Москвы по целому ряду ключевых вопросов международной политической повестки. Сноуден же доставил эти фальсификаты адресно, прямо в руки «русских», - как первоклассный курьер.

Примечательно, что США лишили Сноудена гражданства, когда он следовал на борту самолета в Москву – для того, чтобы из Москвы он никуда дальше не полетел и все сведения, которые он увез с собой, попали бы в руки именно русским (для которых они, видимо, и предназначались).

Технологии вброса управляющей информации через механизм публичных дебатов (технологии класса «Псаки-Метью Ли»)

Технологии вброса управляющей информации через механизм публичных дебатов в американской политике известны давно, но в качестве рабочего механизма операций легализации вбрасываемой информации их стали использовать только с появлением на посту официального представителя Администрации Президента США сотрудника госаппарата Джен Псаки. Тогда же в паре с Псаки стал выступать «независимо мыслящий» американский журналист Метью Ли, смело вступавший в дебаты и столкновения с Псаки по любым, в том числе принципиальным, вопросам. В этой паре Ли всегда наступал, поражая аудитории уровнем своей принципиальности и профессионализма, а Псаки всегда оборонялась, делая это очень неумело и демонстрируя эмоциональную неустойчивость, отсутствие владения информацией, неграмотность. В целом дебаты между Ли и Псаки выглядели как развлекательное шоу, в котором «правдоруб» Ли, выступающий всегда за справедливость, превращал любой брифинг Псаки в ее форменное «избиение». При этом большинство зрительской аудитории всегда принимало сторону «борца за справедливость» Ли, а Псаки сочувствовали единицы. Не меньшее число зрителей, насмотревшись дебатов

между Ли и Псаки, впоследствии искренне считало, что, окажись они на месте Метью Ли, они вели себя по отношению к Джен Псаки точно также, как этот известный американский журналист.

В основе данного вида технологий легализации лежит два предельно простых, но при этом исключительно эффективных базовым психологических эффекта: эффект присоединения и эффект (психологического) слияния. Последовательное использование этих эффектов при организации информационного воздействия на зрительскую аудиторию и дали технологию, получившую название по именам двум главным действующих лиц – технологию класса «Псаки-Метью Ли».

Наблюдая за тем, как «правдоруб» Метью Ли смело набрасывается на Псаки и начинает уличать ее во лжи, некомпетентности, отсутствии внятных объяснений, попытках скрыть от американского народа правду, обыкновенный среднестатистический зритель проникается к Ли безграничной симпатией, а затем и доверием. Причина этого проста: Ли – за правду и справедливость, он «на светлой стороне силы». Кроме того, из каждой схватки с Псаки Метью Ли неизменно выходит победителем, и это важно: кто хочет поддерживать поигравшего? Все всегда стремятся оказаться на победившей стороне, присоединиться к победителю. Именно поэтому с любым зрителем, наблюдавшим дебаты Ли и Псаки, начинали происходить изменения, связанные с «эффектом присоединения»: через некоторое время он начинал считать, что Ли – такой же, как и он, простой парень, выступающий за правду; ценности Ли – это «мои ценности». И, если бы этот зритель оказался бы в тот самый момент в зале, где проходил брифинг, он сразу и не колеблясь встал бы рядом с Метью Ли, плечом к плечу, и лично атаковал бы Псаки так, как это делает Ли, и теми же словами и аргументами, которые он использует.

Еще через некоторого время эффект присоединения обязательно породил бы другой известный психологический эффект – «психоэмоционального слияния»: этот эффект срабатывает тогда, когда зритель, наблюдая за поведением его героя (в данном случае, Ли) на экране телевизора, начинает считать, что Метью Ли – это и есть он сам, только по ту сторону экрана: «Ли – это я, я – это Ли». В результате любые действия Ли на экране телевизора зритель начинает воспринимать как свои собственные: это он сам в образе ли треплет Псаки, наносит ей удары, уличает во лжи; это он сам говорит устами Ли правильные слова собравшимся на брифинге журналистам.

Но это слияние имеет и свои особые последствия. Дело в том, что зритель, слившись с образом героя с экрана телевизора, перестает критически относиться к тому, что произноси его герой, что бы он при этом не сказал. Любые слова, заявления Метью Ли с этого момента воспринимаются на веру и не проверяются, не оспариваются, критически не оцениваются. И в это момент устами «правдоруба» Ли и осуществляется вброс информации, которая сразу же воспринимается как истина в последней инстанции. И

направсно, потому что при ближайшем рассмотрении речь Метью Ли в дебатах обращает на себя внимание своей особой структурированностью.

Любое своей выступление Ли начинает с критических замечаний в адрес Псаки: он цепляет ее за любую опущенную ею неточность и затем выводит Псаки из себя. В ответ Псаки начинает отбиваться, объясняя, что Белоруссии есть море, а в Ростове - горы, и своими новыми ошибками еще сильнее дает себя зацепить. К этому моменту зрители уже практически все на стороне Метью Ли, Псаки при этом даже не сочувствуют – все предвкушают шоу, в которое должно перейти публичное избиение официального представителя Белого Дома. «Присоединение к победителю» уже произошло, еще немного – и наступит слияние.

В этот момент Ли меняет тактику - он произносит вводную фразу: «На самом деле, в мире все обстоит совсем по-другому». И после этого Ли начинает излагать в повествовательном ключе свою позицию, содержащую характеристику той или иной проблемы мирового уровня, с цифрами, оценками, аналитикой. Это и есть информационный вброс, содержание которого под воздействием эффекта слияния сразу попадает в мозг «присоединившейся» к Ли массовой аудитории – быстро, мгновенно и без искажения. Аудитория к этому моменту Ли доверяет абсолютно и проверять его высказывания не будет. Между тем, в этих оценках, выдаваемых Ли, может содержаться и откровенная дезинформация, необходимая для проведения очередной оперативной комбинации курирующими Ли спецслужбами. И, как правило, это так и есть.

В том момент, когда Ли заканчивает свой монолог, «раскладывающий по полочкам» очередную мировую проблему, он мастерски выводит зрителей из состояния транса, в которое их погрузил эффект слияния, путем возвращения к тактике агрессивных нападок на Псаки: он снова налетает на Псаки, дожидается любой ответной ее реакции и затем триумфатором выходит «из игры». Дело сделано.

Технологии легализации класса «Псаки-Метью Ли» — это сверхтонкие технологии, обладающие высшей степенью организации и требующие идеальной синхронизации игры двух дебатеров – Ли, с одной стороны, и Псаки, с другой. Причем от Ли требуется умение и особое чутье, а от Псаки, тщательно подобранной специально на эту роль, - просто быть самой собой. Именно поэтому этот тип технологий чрезвычайно трудно воспроизвести на другой платформе, подобрав других кандидатов на роль официального представителя и независимого журналиста: необходима еще особого рода слаженность их взаимных действий. Когда эффективность этого вида технологий стала очевидной, в России попытались повторить эту схему, выдвинув на роль «псаки» Марию Захарову (ставшую «нашим ответом Псаки»). Однако найти ей партнера класса Метью Ли так и не удалось, и в целом этот весьма прогрессивный американский опыт так и оказался невоспроизведенным на российской земле.

Признаки операций легализации вбрасываемой информации

Любая операция по легализации вбрасываемой информации имеет свои признаки-маркеры, указывающие на использование в данных операциях стандартных и повторяющихся приемов легендирования информационных вбросов. Все они укладываются в следующую простейшую схему легендирования:

1. Источник происхождения вбрасываемой информации – всегда **ЦРУ, Госдеп**, **Администрация Президента** (ведомство или организация, обладающая высшим уровенем компетентности, в идеале – являющееся **хранилищем гос. секретов**).

2. Механизм попадания информации в публичное пространство: **кража** (всегда один и тот же).

3. Кто выкрал информацию? – сотрудник разведки, госдепа, агенты спецслужб, имена которых нельзя разглашать.

4. Физическое лицо, через которого инф. легализовалась в публичном пространстве: **романтик-идеалист, борец за справедливость** (Ассанж, Сноуден, независимые журналисты – реальные люди)

5. Почему не публикует все материалы сразу, а **вбрасывает их частями**? Ответ: большой объем, долго анализировать.