Социальная физика Девида Пентланда и поведенческие войны

Е.С.Ларина, ООО «Персоналинвест»

Что такое Надж и какое отношение он имеет к социальной физике

В XXI веке произошло стирание границ между войной и миром. Появились различного рода теневые, гибридные, асимметричные войны, скрытые конфликты и т.п. Все чаще используют термин «мировойна».

Поскольку границы между войной и миром стерлись, то сегодня национальную безопасность рассматривают с точки зрения семи сфер противоборств и пяти полей боя. Так, в Стратегии национальной безопасности США 2015 г. выделяются именно такие поля и сферы (они будут рассмотрены в докладе). Соответственно именно по этим направлениям США и их союзники навязывают жесткое противоборство своим конкурентам и противникам.

Если мы внимательно рассмотрим семь сфер противоборств и пять полей боя, везде можно увидеть информационную составляющую. Информация есть везде, поэтому каждый под термином «информационная безопасность» понимает свое. Существуют, однако, три различные сферы, в которых информация играет определяющую роль.

Первая сфера – это сфера телекоммуникаций, где информация выступает как сигнал. Главные процессы здесь – передача, обработка и хранение данных. Сигналы могут передавать и принимать как различного рода устройства, так и люди. Это мир хакеров, мир баз данных, провайдеров и т.д. Этот аспект информационной безопасности мы будем называть *сетевой безопасностью*.

Вторая сфера – это информация как контент. Здесь отправителями и получателями информации являются люди. Информация имеет вид текстов, видео, аудио-сообщений и т.д. Это та информация, с которой мы встречаемся каждый день как пользователи или авторы интернета. Это сфера информационных войн, рекламных и пропагандистских кампаний. Данный аспект информационной безопасности будем называть *контентной безопасностью*.

Третья сфера, которую в популярной литературе почти не обсуждают – это сфера человеческого поведения. Здесь информация важна не как сигнал и не как смысл сообщения, а как причина для каких-либо практических действий человека. Это мир поступков, тех или иных действий. Мир Надж (англ. nudge – толкнуть локтем, подтолкнуть, тж. навести на мысль)**.** Этот аспект

информационной безопасности мы будем называть *поведенческой безопасностью*.

Мы затронем только вторую и третью сферы – контентную и поведенческую. Первая сфера – сетевая безопасность – вотчина специалистов по информационной безопасности, как ее понимают в IT-индустрии программисты, разработчики, хакеры и т.д. Если говорить кратко, эта сфера, где противоборствующие стороны стараются технически нарушить каналы передачи информации, затруднить или изменить алгоритмы ее обработки, украсть, повредить либо изменить информацию в местах ее хранения.

Рассмотрим контентную безопасность и меры по ее защите. Важно понимать, что суверенитет в электромагнитной среде поддерживать труднее, чем привычный (географический) суверенитет. В электромагнитной среде нет границ как таковых, поэтому трудно обеспечить их физическую охрану.

Обеспечение контентной безопасности является важнейшей задачей государственной политики и патриотических сил любой страны. Решение этой ключевой задачи достигается за счет задействования совокупности факторов и инструментов, из которых важнейшими являются следующие

1. Принадлежность поисковых инструментов и социальных сетей. Подавляющее большинство интернет-пользователей продолжают заходить на сайты при помощи поисковиков. Поисковик – своего рода трасса: пользователи попадают именно туда, куда хотят их направить владельцы поисковика. Поэтому первый важнейший пункт контентной безопасности – принадлежность поисковиков. В этом смысле Россия и Китай находятся в уникальном положении: только в этих двух странах Google не является главным поисковым инструментом.

Такая же ситуация и с социальными сетями. Здесь у России есть собственные мощные социальные сети, прежде всего ВКонтакте и Одноклассники, которые по количеству пользователей и по их активности превышают масштаб соответствующих американских сетей.

2. Еще один элемент информационного суверенитета – это компьютерные игры. Во всем мире происходит процесс «геймификации». Уже многие люди учатся, познают реальность, развлекаются и даже формируют жизненные установки и ценности через компьютерные онлайн-игры. Соответственно, кто их производит – тот и хозяин аудитории. В мировой табели о рангах игровые российские компании занимают очень приличные места.

Все, что было сказано об играх, целиком относится и к телевидению. Помимо производителей сериалов, хотелось бы отметить телеканал Russia Today. Известно, что он вошел в число пяти наиболее активно просматриваемых видео-новостных каналов американского интернета и видеонета многих европейских стран.

Почему это важно? Широкополосный дешевый интернет изменил правила игры в глобальной паутине. Если вообще информация в интернете удваивается каждый 2,5 года, то объем видеофайлов удваивается каждые шесть месяцев.

Информационная безопасность в текстовой сфере предполагает соблюдение нескольких обязательных требований:

Во-первых, всегда надо помнить, что интернет отличается от физического мира тем, что информационные следы остаются в нем навсегда.

Во-вторых, всегда надо помнить о том, что пользователи интернета крайне неоднородны. Нет потребителя контента вообще, так же как нет и обобщенного человека. Поэтому каждый текст и каждый электронный ресурс должен быть ориентирован на конкретную аудиторию.

В-третьих, надо иметь в виду, что в интернете даже больше, чем в реальной жизни, важно доверие аудитории. Доверие трудно завоевать, но легко потерять. Сильная информационная политика всегда базируется на доверии. В этой связи в информационном потоке надо четко разделять факты и их интерпретацию.

Что такое поведенческое противоборство? Классические информационные противоборства в виде информационных войн или психологических войн предполагают, прежде всего, убеждение аудитории. В конечном счете, именно в этом состоит задача агитации, пропаганды, PR и т.п.

Однако человек – сложная система. Как установили психологи, социологи, специалисты нейронаук, в различных ситуациях от 50 до 90% своих действий люди осуществляют «автоматически». Это открытие и положено в основу поведенческих противоборств. Не надо людям ничего объяснять, убеждать, изменять ценности: необходимо просто воспользоваться имеющимися у них привычками, стереотипами, склонностью выбирать наименее энергозатратный и простой путь достижения целей – в собственных интересах тех, кто ведет противоборство.

Поведенческие варианты противоборства базируются на трех китах.

Первый – Большие Данные (Big Data, БД) и методы их обработки. Поскольку у разных групп людей разные привычки и стереотипы, обработка БД позволяет узнать привычки, стереотипы, склонности конкретных групп и даже отдельных людей как представителей этих групп. Откуда черпаются эти БД? Опять-таки из интернета. Это огромный поведенческий архив, где хранится информация не просто о мыслях, но и о реальных действиях всех относительно всего. К тому же в дополнение к поведенческим архивам есть огромные базы данных. Например, в массиве данных компании (дата-брокера) AXIOM насчитывается 700 млн. аккаунтов, или профилей конкретных людей, классифицированных по 150 параметрам. В результате БД позволяют не только разделять всех пользователей на конкретные группы с общими привычками, стереотипами и особенностями автоматизма, но и предсказывать их поведение.

Второй кит – это так называемые поведенческие технологии. Самая известная из них – «мягкое подталкивание», или Надж. Эту технологию разработали один из ближайших сотрудников и даже друзей Б.Обамы, его «информационный царь» Касс Санстейн и советник премьер-министра Великобритании Д.Камерона Ричард Талер. Суть технологии Надж заключена в названии: подталкивание. Надж старается поставить человека в такую ситуацию, когда самое легкое решение оказывается таким, какое нужно тому, кто эту ситуацию создает, т.е. «подталкивателю».

Третий кит – это платформы, при помощи которых происходит подталкивание. Поскольку в ходе поведенческих противоборств собранная информация используется путем применения определенных технологий (прежде всего Наджа), необходимо еще и место, где осуществлять подталкивание. Поскольку сегодня активность переносится в цифровую среду, а между реальностью и виртуальностью в этой единой цифровой среде практически нет разницы (они соединились) – в ней и происходит подталкивание. Оно осуществляется через различного рода электронные выборы, платформы интернет-магазинов и т.п.

И еще один, очень характерный факт. Руководителем рабочей группы по реформе АНБ (NSA, National Security Agency), самой мощной организации США по собиранию, хранению и обработке данных со всех цифровых платформ, был уже упомянутый Касс Санстейн, который к этому времени уже ушел с государственной службы.

Кто предупрежден – тот вооружен.