Информационно-психологическая безопасность в интернет-коммуникации: как тобой манипулируют? : информационно-аналитическая справка / Д.Е. Гуляев, Ю.В. Чалышева. — Москва, 2023. — 14 с.

Чалышева Юлия Владимировна,

Инспектор Центра по обеспечению прав молодежи в цифровом пространстве Университета имени О.Е. Кутафина (МГЮА)

Гуляев Дмитрий Евгеньевич,

Директор Центра по обеспечению прав молодежи в цифровом пространстве Университета имени О.Е. Кутафина (МГЮА)

Информационно-аналитическая справка «Информационно-психологическая безопасность в интернет-коммуникации: как тобой манипулируют?»

1. ВВЕДЕНИЕ:

На сегодняшний день не сложилось единого понятия информационно-психологической безопасности. Проблема исследования информационно-психологической безопасности в научной среде представлена через призму междисциплинарного подхода и обеспечивает практическую

востребованность в отношении вопросов национальной безопасности. Попробуем разобраться с понятием, исследуя разные точки зрения ученых.

А.В. Манойло выделяет понятие «информационно-психологическая безопасность личности». Это состояние психического сознания человека, которое ресурсно позволяет ему развиваться, удовлетворяет все его потребности, обеспечивает адаптацию в условиях социальной турбулентности и неустойчивости, конструктивно позволяет выстроить социально одобряемые и эффективные стратегии поведения в условиях социальной среды. К основным компонентам, сферам, которые позволяют сопротивляться информационно-психологическому воздействию, он относит систему ценностей и личностных установок, показатели психического здоровья, свободу воли[1].

А.Н. Лунев и Н.Б. Пугачева в контексте философского знания трактуют информационнопсихологическую безопасность в терминах защищенности личности от негативного воздействия средствами осознания механизмов, средств воздействия и развития способов совладания со стрессом и противодействия ему[2].

Важно заметить, что С.М. Ненашев в терминологическом и понятийном пространстве разграничивает вопрос понятия «информационно-техническая безопасность» и «информационно-психологическая безопасность». Он фиксирует факт о смежности и взаимозависимости данных понятий, поскольку угрозы, которые представлены техническими воздействиями, опосредованно влияют на психическое состояние личности и способность принимать адекватные решения в условиях агрессивной риторики[3].

---

[1] Манойло А.В. Государственная информационная политика в особых условиях: монография. М., 2003. 388 с. (из статьи «Проблема информационно-психологической безопасности в психологии» А.В. Бырканова - аспиранта Саратовского научно-исследовательского университета имени Н.Г. Чернышевского.

[2] Лунев А.Н., Пугачева Н.Б. Информационно-психологическая безопасность личности: философский аспект // Общество: философия, история, культура. 2014. № 1. С. 11–16.

[3] Ненашев С.М. Информационно-технологическая и информационно-психологическая безопасность пользователей социальных сетей // Вопросы кибербезопасности

Опираясь на Доктрину информационной безопасности Российской Федерации, исследователи устанавливают, что информационно-психологическая безопасность – это «защищенность граждан, отдельных групп и социальных слоев, массовых объединений людей и населения страны в целом от негативных информационно-психологических воздействий». Выделяют сознательный и бессознательный уровень воздействия на личность в информационно-психологическом плане. В результате происходит деформация установок и системы отношений, что негативно сказывается на деятельности и поведении в целом[4].

Информационно-психологическое воздействие, которое оказывается в контексте информационного влияния, имеет разные уровни: изменяя состояние сознания, влияя на убеждения, ценностные ориентации, познавательную сферу личности, трансформируя картину мира личности. Источниками угроз становятся как социально-психологические факторы, так и личностные, внутренние.

Отдельные исследователи считают, что информационно-психологическое воздействие наносит ущерб на разных структурных уровнях сознания человека. А именно на уровне:

– личностном – затрагивает самооценку, уверенность в себе, Я-концепцию, образ Я, индивидуальность;

– мотивационном – изменяет желания, побуждения, вкусы личности;

– когнитивных структур – трансформирует мировоззрение, ценности, знания;

– поведенческом – воздействует на привычки, способности, установки, стратегии поведения[5].

Установлено терминологическое многообразие, которое позволяет выделить информационно-психологическую безопасность как совокупность

[4] Балахтар В.В. Манипуляция и манипулятивное воздействие // Национальная ассоциация ученых. 2015. № 4-3. С. 57–60.
[5] Biyimbetov J.K. Philosophical Analysis of the Problem of Information Psychological Security // Adam alemi. 2021. №. 2 (88). P. 3–9.

системных субъектных характеристик, обеспечивающих стабильность состояний, переживаний человека, связанных с его положением в настоящем, перспективами на будущее и чувством защищенности от разного рода опасностей[6].

Таким образом, можно сделать вывод, что главным признаком информационно-психологической безопасности является защищенность и способность защищаться от информационно-психологического воздействия, которое может проявляться в различных формах с множеством признаков - угрозы информационно-психологической безопасности.

Где же чаще всего на человека оказывают информационно-психологическое воздействие? Конечно, же в интернет-коммуникация - сейчас это место, где человек проводит большое количество времени. Само сочетание этих двух терминов - «интернет» и «коммуникация» вызывает огромный интерес. Ведь Интернет представляет собой среду, а коммуникация является сутью этой среды. Однако сочетание такого использования этих терминов оправдывается тем, что до недавнего времени основная функция Интернета была связана лишь с получением и хранением информации, но на сегодняшний день она перестает быть ведущей. Все больше Интернет берет на себя роль канала коммуникации, стимулируя «новые социокультурные процессы».

И сегодня в рамках темы мы рассмотрим такой аспект информационно-психологического воздействия как манипуляция.

Манипуляция - это скрытое психологическое воздействие со стороны манипулятора, с целью изменения в своих интересах поведения манипулируемого объекта.

[6] А.В. Бырканов. Проблема информационно-психологической безопасности в психологии. Саратовский научно-исследовательский университет имени Н.Г. Чернышевского.

2. КАК ПОНЯТЬ, ЧТО ТОБОЙ МАНИПУЛИРУЮТ[7]:

Логично предположить, что интернеткоммуникация, вышедшая из классической массовой коммуникации, получила свои отличия от последней вследствие постоянного развития и внедрения новых сред и технологических новаций. По мнению С.В. Володенкова в настоящее время интернеткоммуникации присущи некоторые содержательные, структурные и технологические особенности[8], которые приобретают важные функции в контексте манипулятивного процесса, то есть данные характеристики выступают в качестве «уязвимостей» интернет-коммуникации:

1. **Структурированность аудитории.** Вытекает из важных функций Интернета (нахождение необходимой информации и связь людей по интересам на больших расстояниях). С помощью манипуляций возможно воздействие на конкретные аудитории, группы людей, к примеру: с помощью частых напоминаний СМИ в соц. сетях о новости о создании Стратегии развития в Нижегородской области и ее общественном обсуждении происходит объединение разбросанных по всему субъекту предпринимателей и объединение их для нахождения экономического консенсуса. Данная характеристика подразумевает, что манипулятор может составить так называемый портрет аудитории и осуществить воздействие.

2. **«Горизонтальность» коммуникации.** Любой человек в Интернете является полноправным субъектом коммуникации с большой свободой самовыражения. В итоге информация не только достигает конкретного адресата, но и распространяется дальше, к другим пользователям, что часто используется в технологиях эмоционального «заражения» масс. Наглядным примером здесь выступает ведение Дональдом Трампом аккаунта в Твиттере *(заблокирован на территории Российской Федерации)*, это дает возможность напрямую и более прямо, без посредников говорить с аудиторией в данном примере избирателей, своевременно заявляя свою точку зрения. Эта

[7] https://elar.urfu.ru/bitstream/10995/83894/1/978-5-321-02538-3_2017_074.pdf?ysclid=lfgotsbxfi985976753

[8] Володенков С.В. Интернеткоммуникации в глобальном пространстве современного политического управления. – М.: Издательство Московского университета; Проспект, 2015.

стратегия позволила ему избавиться от журналистов и достичь большей популярности за счет «неофициальных» диалогов с аудиторией.

3. **Пользовательская генерация контента.** Сами участники интернеткоммуникации привносят в ходе общения новый контент на свои площадки, чем запускают дальнейшую реакцию в виде загрузки «ответного» контента другими пользователями. И иногда то, что загрузил один человек может вызвать бурю эмоций у другого, и не всегда положительных.

4. Высокий мобилизационный потенциал. За счет сильно развитых сообществ, «горизонтальности» и скорости распространения информации ответная реакция пользователей поступает в короткие сроки. В таких условиях трудно быстро реагировать на проблему и противостоять ей.

5. **Влияние Интернета на традиционное политическое, социальное коммуникационное пространство.** Заметна тенденция к тому, что самой активной частью населения, способствующей возникновению и развитию политических, социальных событий становятся именно пользователи интернета. Одним из отражений этого явления стало появление Совета блогеров при Госдуме - лидеров общественного мнения, воздействующих на массы и оказывающих сильное влияние на обстановку в стране.

6. **Нелимитированность.** Количество информации в Интернете ограничивается лишь емкостью накопителей на серверах. Таким образом, поток манипуляции может быть практически неограниченным по объёму.

7.**Таргетированность.** С помощью имеющихся сервисов метрики, трекеров, рекламных идентификаторов и др. создается профиль пользователя у различных компаний, что способствует предоставлению информации, связанной с его интересами, запросами, но также опосредованно манипулирует его мнением - ведет к «навязыванию» определенных взглядов.

8. **Мультимедийностъ.** Основой нынешнего Интернета является наглядность и привлекательность информации (иногда самая привлекательноизложенная информация бывает самой неправдивой).

Поддержка всех известных форматов данных для удовлетворения потребностей пользователя способствует этому.

9. **Экстемпоральностъ.** Наличие таких сервисов как веб-архивы, кэш поисковых систем, копии страниц, а также различных средств для противодействия блокировкам позволяют в любой момент получить доступ к большинству необходимой информации.

10. **Оперативность.** В Интернете временные ограничения по работе с информацией лишь связаны с работой техники, предоставляющей эти услуги, в связи с чем также имеется возможность к быстрой редактуре/изменению любой выгруженной в общественный доступ информации.

11. **Интерактивность.** На различных ресурсах пользователи могут взаимодействовать друг с другом с помощью встроенных инструментов и функций. Также данная возможность может быть использована для создания рекламы, основанной на взаимодействии с пользователем. К примеру, в игровой форме, ведь как известно, информация хорошо усваивается при подаче ее в понятном и доходчивом виде, который заинтересует реципиента.

Таким образом, манипуляцию в Интернете можно определить по нескольким признакам. В первую очередь пользователю необходимо обращать внимание на **то, как представлена интересующая информация.**

Вероятность использования манипуляции существенно увеличивается, в случае если в процессе работы с каким-либо информационным объектом, например, с текстом:

1) отсутствуют ссылки на источник информации;

2) в качестве источника информации представлен неизвестный эксперт;

3) в тексте используются многократные повторы одной и тоиˊ же информации;

4) информация носит ярко выражено оценочный характер;

5) при подаче информации приоритет отдается визуальным компонентам (мемам, демотиваторам, таблицам, диаграммам, схемам и др.).

В процессе осуществления общения в Интернете **необходимо проявлять осторожность, если отмечается:**

1) стремление коммуникатора быстрее «перейти на ты»;

2) отсутствие информации о коммуникаторе;

3) высмеивание, оскорбление;

4) использование системы рейтинга, при ее наличии;

5) апелляция к эмоциям во время беседы.

Также можно выявить наиболее частые приемы манупуляций в интернете:

1) **дробление информации**: заключается в выдаче информации обществу «маленькими порциями». Такая подача информации затрудняет концептуальное восприятие процесса или явления в целом, что приводит к их непониманию и, как следствие, к снижению интереса к ним. Разновидностью дробления может быть чрезмерное обилие информации, в неадекватных реалиям пропорциях, когда несущественные сведения маскируют нежелательную для манипулятора истинную картину. Такой способ коммуникации подавляет индивидуальный выбор и дезориентирует человека; Главная отличительная особенность данного метода заключается в том, что манипулятор, вместо акцентирования внимания на каком-то событии действительности, наоборот уменьшает значимость и актуальность происходящего.

Пример: Предположим, произошло яркое событие в общественно-политической жизни страны. Но, например, СМИ по каким-то причинам не хочет, чтобы произошедшее вызвало широкий общественный резонанс. Тогда новость дробится на небольшие «подновости», которые доходят до читателя в разных номерах газеты и на разных её полосах. Лжи тут нет, но нужный эффект достигается: читателю сложно выловить все части головоломки из потока информационных сообщений и «склеить» их воедино; он рассматривает их как несвязанные между собой факты.

2) **замалчивание.** Умалчивать можно не всю информацию, а лишь существенные детали, не выгодные манипулятору. Использование приема «умолчания» дает возможность программировать поведение больших масс людей;

3) **прием «прямого комментирования»** результатов исследования. Комментарий обязательно опирается на логические и оценочные основания, уже имеющиеся в сознании людей. Манипулятор, комментируя собранные факты, находит эти опоры, преобразуя их во мнения, взгляды на обсуждаемую проблему. Логические структуры, используемые для этого, чаще всего предельно просты и квалифицируют события с позиций «черное – белое», «добро – зло», что соответствует довольно низкому культурному уровню манипулируемых. Но они могут быть и более сложными и приближаться к адекватной оценке проблемы;

4) **прием «игра цифрами и фактами»** для создания видимости объективности и точности;

5) **дезинформация** используется в качестве искусственно распускаемого слуха, соответствующего подсознательному желанию общества. Специалисты в области PR-технологий доказали, что влияние популярного дезинформационного сообщения не способно уменьшить даже объективная информация;

6) приемы, основанные на нарушении **законов формальной логики**:

-ложная аналогия - это сравнение двух терминов, которое ошибочно, потому что это рассуждение кажется верным, но на самом деле не так.

Примеры: Моего соседа зовут Мария, соседа Хуана зовут Мария, у моего соседа есть собака; следовательно, у соседа Хуана тоже есть собака. (Однако тот факт, что этих двоих зовут Мария и они чьи-то соседи, не является достаточным основанием для вывода о том, что у них обоих есть собака.)

У Земли есть атмосфера, у Венеры есть атмосфера, на Земле люди могут дышать; следовательно, на Венере люди могут дышать. (Однако

атмосфера Венеры отличается от атмосферы Земли, поэтому люди не могут дышать воздухом Венеры.)

- **подмена причины следствием** - речь идет о случаях, когда результат принимается за причину: «Если пожарники тушат дом, то в доме пожар». Пожар вызван тем, что дом тушат пожарники, или наоборот, пожарники тушат дом, потому что он горит? Случаи такой перестановки не очень распространены, но все же время от времени встречаются. И все это направлено на то, чтобы запутать пользователя.

И еще: вывод без достаточного основания, подмена тезиса, тавтология, диффамация, демагогия, ссылка на «заслуживающий доверие источник», ссылка на авторитеты;

7) **двойной стандарт.** Используя этот прием, манипулятор применяет различные критерии при оценке явлений, событий и позиций, участвующих или заинтересованных в них лиц[9].

3. ОСНОВНЫЕ УГРОЗЫ ИНТЕРНЕТ-КОММУНИКАЦИИ.

Цифровая среда - пространство постоянных перемен, в данной среде находят проявления следующие отрицательные явления:

- открытая либо закамуфлированная **вербовка** (онлайн-рекрутинг) в радикально настроенные группы и деструктивные сообщества через социальные сети с использованием таких манипулятивных приемов, как мифотворчество (романтизация, героизация), элитарность («не такой как все»); геймификация (игровые механизмы), челленджи («беги или умри»), «запретный» контент, конфликт поколений («взрослый мир - плохой мир»), аккумулирование негативизма («весь мир против тебя», «государство - зло» и т.п.), закрытая общность («брат за брата») и др.;

- осуществление незаконной миссионерской деятельности;

[9] Сладкова О. Б. Манипулирование общественным сознанием в информационном обществе // Обсерватория культуры. 2006. № 6. С. 4–12.

- **киберсуицид** (согласованные сумоубийства), включая онлайн кибербуллицид (самоубийство в режиме реального времени перед веб-камерой), флешмоб-киберсуицид, аддиктивный киберсуицид.

- **пропаганда** (героизация, романтизация) **аутодеструктивного** (анорексия, булимия, селф-харм) и суицидального поведения онлайн (в том числе так называемые «группы смерти»; «суицидальные квесты» с использованием сигнов; мистические группы, использующие кодирование информации; форумные ролевые игры и т.д.);

-**кибертроллинг** (включая флейм (флейминг)) - форма социальной провокации в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации;

-**кибербуллин**г (кибермоббинг) травля, вербальное издевательство, в том числе угрозы, вызывание чувства стыда, враждебного отношения; дискриминационные высказывания, связанные с внешним видом, умственными способностями, умениями и т.д.: харассмент, имперсонация, эксклюзия (остракизм), стигматизация, кибersталкинг, угрозы, хейтинг, стигматизация, хеппислепинг («радостное избиение) и др.

- **кибергруминг** - установление «дружеских отношений и эмоциональной связи с ребенком или подростком для завоевания его доверия с целью сексуальной эксплуатации».

- **секстинг** - «вид виртуальной коммуникации, включающий отправку, получение или пересылку текстовых сообщений, изображений фотографий, аудио- и видеозаписей с сексуальным содержанием».

-**секс-шантаж** - «угроза публикации интимных фото жертвы с целью вымогательства дополнительных фотографий, видео или сексуальных действий»

-**доксинг** - «объявление о том, что жертва предлагает сексуальные услуги.

4. ЧТО ДЕЛАТЬ, ЕСЛИ ТОБОЙ МАНИПУЛИРУЮТ?

Методы противодействия манипуляции в Интернете можно разделить на **три основные группы:**

- В первой группе методов акцентируется внимание на устойчивости психики человека к воздействию манипуляции.
- Вторая группа методов основана на развитии и использовании критического мышления при работе с информацией.
- В третьей группе методов даются рекомендации по использованию инструментария Интернета.
- Правовые механизмы защиты от манипуляций в сети.

В **первой группе** можно выделить следующие методы противодействия, которые основаны на умении человека контролировать и анализировать свои действия.

- Прежде всего, пользователю необходимо уметь отстаивать свою точку зрения, свои взгляды и убеждения в дискуссиях или спорах.
- Пользователю необходимо подтверждать свою позицию фактами.
- Вступив в дискуссию агрессивного характера, не стоит пытаться оправдываться или защищаться. Оправдываясь или защищаясь, человек резко теряет инициативу в дискуссии, оставаясь беззащитным перед манипулятором.
- Важно, чтобы пользователь знал свои слабые места и старался обходить стороной беседы, которые так или иначе могут вызвать у него негативные эмоции.
- Пользователю необходимо доверять своей интуиции, если он сомневается в намерениях собеседника, а также в правдивости изучаемой им информации.

- Во время дискуссии или поиска информации не позволять отвлекать себя от изначально интересующей темы.
- Контролируйте процесс информационного воздействия, а также контролируйте свои реакции на внешнее информационное воздействие.

Вторая группа методов направлена на развитие критического мышления. Критическое мышление позволяет избегать одномерного восприятия информации, людей, событий. Методика развития критического мышления чаще всего бывает представлена в нескольких постулатах.

- Необходимо проверять поступающую информацию, искать ее источники, а также альтернативные позиции, которые могут подтвердить или опровергнуть информацию, представленную в оригинале.
- Если имеет место активное влияние субъекта, то необходим поиск информации об этом субъекте, его профиль в Интернете, просмотр его круга общения, возможно и общение с самим кругом.
- Ключевым элементом критического мышления являются ответы на вопросы: «Зачем мне нужно общаться с этим человеком?», «Почему я должен читать этот блог или прислушиваться к мнению этого человека»? и др. Вопросы подобного рода позволяют создать первичный блок к восприятию информации манипулятивного характера.
- Выставляйте психологические барьеры и старайтесь оградить психику от внешнего ненужного, негативного и непроверенного информационного потока.

Третья группа методов направлена на рациональное и эффективное использование доступного инструментария интернет-ресурсов. Для защиты от манипулирования пользователю необходимо.

- Использовать систему черных списков.

- Использовать систему фильтрации нецензурных слов, которая позволяет испытывать меньший эмоциональный дискомфорт в общении с другими пользователями.
- Обратиться в центры безопасности или к администраторам интернет-ресурсов с просьбой заблокировать агрессивного пользователя в случае столкновения с кибер-запугиванием
- Не оставлять в Интернете слишком много информации о себе. Эти сведения манипулятор сможет использовать для того, чтобы войти в круг общения пользователя (прикрывшись общими интересами), либо выступить в роли интернет-тролля и подвергнуть критике вас и ваши интересы с целью «наклеивания» на вас ярлыков.
- Периодически меняйте пароли. Чтобы минимизировать риск кражи личных данных, регулярно обновляйте свои пароли во всех информационных ресурсах. Также никому не сообщайте свои пароли.
- Нормируйте использование компьютерных и мобильных устройств. Создайте режим пользования цифровыми технологиями, не проводите в Интернет-пространстве слишком много времени.