УДК 004

**Психосоматика кибербытия:**

**постановка проблемы и аспекты безопасности**

А.И. Терентьев

*Центральный банк Российской Федерации*

*107016, Москва, ул. Неглинная, 12, Российская Федерация*

В современном высокотехнологичном обществе и сложившемся цифровом миропорядке гуманитарные, социальные и психологические аспекты информационной безопасности все больше вызывают интерес различных групп влияния и приобретают особую значимость, что обуславливает актуальность и необходимость соответствующих научно-практических исследований.

Карл Маркс, В.И. Ульянов (Ленин) и многие другие великие мыслители и ученые установили, что общественное бытие людей определяет их сознание. В общем понимании «бытие» это синоним понятия «существование», некая окружающая нас действительность или реальность, наличие явлений и предметов самих по себе или как данности. Сознание – способность человека мыслить, рассуждать и определять свое отношение к этой действительности, восприятие и понимание окружающей его действительности, психическая деятельность как отражение действительности. Сознание есть функция мозга. Сознание – субъективный образ объективного мира. Сознание так или иначе определяет поведение человека и порождает действия.

Таким образом, очевидно непосредственное и неотвратимое влияние окружающего нас материального мира, одним из элементов которого, наряду с другим многообразием, является какая-либо киберсистема, киберпространство или любое иное киберпроявление, поглощаемое единым понятием, определенным автором как «кибербытие», на физическое и душевное состояние человеке, а следовательно на его поведение и поступки.

В медицинской психологии существует специальное направление, называемое [психосоматик](https://dic.academic.ru/dic.nsf/psihologic/1499)ой (от греч. *psyche* душа и *soma* тело), связанное с изучением влияния психических факторов на развитие функциональных и органических расстройств человека, т.е. по сути в более широком толковании – влияния психических факторов на тело (телесное состояние человека). Аналогичным образом, если речь о психических факторах, порождаемых кибербытием человека, можно выделить новую, своего рода «психобиотехническую» проблему, названную автором как психосоматика кибербытия.

Таким образом, манипулируя посредством современных информационных технологий сознанием или подсознанием человека, можно управлять его телесным состоянием и инициировать нужные манипулятору действия или поведение, и как следствие, влиять, при необходимости, на целевые группы людей.

Проведенные автором исследования показывают, что условно можно выделить следующие виды психосоматической реакции:

1. Объектно-ориентированная (целенаправленная) реакция. Возникает в случае самостоятельной или наведенной возможности идентифицировать источник осознанной или неосознанной проблемы (т.е. раздражитель). Такую реакцию можно также условно разделить на негативную или позитивную по отношения к источнику осознанной или неосознанной проблемы (раздражителю).

2. Рассеянная (дезориентированная, не целенаправленная) реакция. Возникает в случае невозможности идентифицировать источник проблемы (раздражитель). Такую реакцию можно условно разделить на негативную или позитивную по отношения к внешнему материальному миру.

Указанные виды реакции по характеру предполагаемых последствий можно условно разделить на:

1. Конструктивную (продуктивную, созидательную, эволюционную и т.п.) реакцию.

2. Деструктивную (контрпродуктивную, разрушительную, революционную и т.п.) реакцию.

По характеру влияния (воздействия) на состояние конкретного человека можно выделить:

1. Мотивирующую (укрепляющую, жизнеутверждающую и т.п.) реакцию.

2. Травматическую реакцию, негативно влияющую на физическое и психическое состояние и здоровье человека.

Условно можно выделить 3 типа ответной реакции (последующих действий или состояний) человека:

1. Возбуждение, гнев, месть.

2. Депрессия, бессилие, отрешение.

3. Самоанализ (психоанализ, психосинтез) с последующими коррекцией и восстановлением (выздоровлением), в следствие компенсации или существенного снижения значимости и влияния ключевых раздражающих факторов.

Не углубляясь далее в условную классификацию возможных психосоматических реакций, нетрудно понять, какие могут быть возможные последствия, если кто-либо научится (или уже научился) тем или иным образом ими управлять. Очевидной становится лежащая на поверхности очень актуальная и соблазнительная в настоящее время для различных групп влияния (бенефициаров) задача, заключающаяся в прогнозировании, инициировании и управлении состоянием и поведением человека (индивидуума) посредством формирования специальной, т.е. соответствующей заранее поставленной цели, доступной или навязанной человеку информационной или цифровой среды (киберпространства). Соответственно, научившись управлять таким образом поведением одного человека, можно управлять поведением группы людей, т.е. массами.

В рассматриваем случае под целевой воздействующей киберсредой понимается совокупность доступных или навязанных человеку различных технических средств и специальных возможностей (сервисов), согласованных в пространстве и во времени. При этом манипуляция осуществляется всегда с умыслом. В противном случае речь может идти о некой естественной эволюции, т.е. не направленной трансформации, возникающей вследствие формирования и действия исторически складывающихся внешних факторов.

Следует отметить, что результативность любой манипуляции многократно возрастает, если налажена какая-либо (постоянная или периодическая, устойчивая или не устойчивая, непосредственная или опосредованная и т.п.) обратная связь манипулятора или бенефициара с манипулируемым объектом. Обратная связь позволяет манипулятору или бенефициару оценивать текущее состояние объекта и своевременно корректировать (актуализировать) в своих интересах целевую воздействующую киберсреду.

Бенефициарами в каждом конкретном случае могут являться:

1. Человек.

2. Бизнес.

3. Криминал.

4. Государство.

При этом отчетливо можно выделить следующие, вытекающие в первую очередь из целей манипуляции, производные проблемы комплексной безопасности:

1. Государственной безопасности.

2. Производственной (коммерческой) безопасности.

3. Личной безопасности и здоровья.

В настоящем материале не рассматриваются конкретные законы и инструменты манипуляции, которые безусловно есть, поскольку исследованием этой проблемы не могут не заниматься компетентные органы индустриально развитых стран и международный криминал. Кроме этого, определенные исследования идут и в научном сообществе, о чем можно с уверенностью судить из открытых источников информации. При этом вполне очевидно, что эффективное решение указанных проблем требует существенных финансовых, временных и других ресурсных затрат, что возможно в большей степени на крупном корпоративном или государственном уровне и предполагает создание и постоянное совершенствование адекватных угрозам высокотехнологичных инструментов и систем противодействия, обеспечивающих необходимые функции защиты, включая обнаружение, изучение и устранение возникших или потенциальных проблем. При этом следует признать, что активная или проактивная защита невозможны без использования определенных средств нападения, которые безусловно должны быть в арсенале современного независимого государства или самодостаточной крупной корпорации.

Таким образом, постигая и впоследствии применяя в конструктивных или, к сожалению, в деструктивных целях законы и инструменты формирования и влияния кибербытия на поведение человека можно натворить как очень много плохого, так и очень много хорошего. По какому пути в конечном итоге пойдет человечество зависит каждого из нас.