**Как защитить себя и наших детей в киберсреде**



**Киберугрозы современности: суть и пути решения**

Анализируя причины негативных социальных явлений в российском обществе и пути их преодоления, крайне важно учитывать исторически сформировавшийся культурный код русского человека.  
  
По природе своей русский человек – это добрый человек, остро и чутко воспринимающий зло, негативные проявления и вызовы, в первую очередь, на интуитивном уровне. Автоматически естественная реакция для нас – это попытка отстраниться, дистанцироваться от подобного явления и его источника.  
  
В первую очередь, потому что это абсолютно чуждо, неприемлемо и непонятно нам. Выход для нас – это позвать особого знающего специалиста (волхва, знахаря, врача и др.), чтобы он описал «болезнь», поставил «диагноз» и нашёл решение.  
  
В этом кроется одна из ключевых особенностей российского общества, а в настоящее время, и внутренних угроз. Русский человек в массе своей при столкновении с негативными явлениями не знает, как им противостоять, он не привык решать эти вопросы самостоятельно.  
  
В условиях резко агрессивной социальной среды, характерной для нашего социума последние 30 лет, естественная защитная реакция психики ввиду непонимания – шок, паралич.

**В условиях развязанной против России широкомасштабной «гибридной войны» каждый должен уметь самостоятельно** описать «симптомы» и источник болезни, поставить «диагноз», **найти решение.** Дистанцироваться, закрыть глаза на проблему не удастся. «Оппонентами» России, в том числе мировыми преступными группировками, используются передовые, отточенные годами технологии последовательного, многократного воздействия на психику человека с использованием современных информационных средств.  
  
[](https://ss69100.livejournal.com/attachment/vstavka2/)Теория и практика информационно-психологического воздействия на людей совершенствовались со времён двух мировых войн XX века и во время многочисленных вооруженных конфликтов регионального масштаба. Появление радио, телевидения и, наконец, сети Интернет позволило проводить психологические операции как в адресном, так и в массовом порядке.  
  
На настоящий момент в мире признается сам факт, что идёт война или противоборство, которое называют по-разному: холодная война, мягкая сила, информационная война, гибридная война, контентная война.

На сегодняшний день лидирующей страной в наступательном ведении «гибридных войн» являются США. Ещё в 1985 г. в них было основано объединенное командование гражданской администрации и психологических операций сухопутных войск (United StatesArmy Civil Affairs and Psychological Operations Command (Airborne)).

В июне 2010 г. директива министра обороны США переименовала «психологические операции» (Psychological Operations, или PSYOP) в «военные операции по информационному обеспечению» (Military Information Support Operation (MISO)), с целью специально сокрыть открыто враждебный характер данной деятельности.  
  
В 2009 г. США создали отдельную структуру «Киберкомандование» (Cyber Command) для проведения наступательных операций в сети Интернет. Единое киберкомандование по сути выполняет управление над всеми специальными структурами США. Сделано это неслучайно: мир стал информационным, соответственно, формирование и управление киберпространством стало **задачей стратегической важности**.  
  
Следует обратить внимание, что расход бюджета США на кибербезопасность в 2016 г. составил почти 14 млрд долларов. (Для сравнения суммарный бюджет Российской Федерации на информационную безопасность составил порядка 250 млн в 2016 г.)[](https://ss69100.livejournal.com/attachment/fg/)

Подготовка кадров для создания и обеспечения данного процесса в США является системой и ведется достаточно давно. Более того, ежегодно США привлекает более 100 тыс. несовершеннолетних на работу по информационно-наступательным действиям в сети Интернет (комментирование новостей, троллинг, рассылка и др.) в отношении других стран и народов. Причём никого не волнует, что «детские умы» в руках военных – это предсказуемая мина агрессии для будущего всего человечества в непредсказуемых масштабах.

Понятие **кибербезопасность** как инструмент защиты и наступления в данном противоборстве было сформулировано мировой общественностью относительно недавно. Кибербезопасность включает в себя набор средств, стратегий, принципов обеспечения безопасности, подходов к управлению рисками, действий, профессиональной подготовки и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

Сегодня к киберугрозам относится не только незаконное вредоносное проникновение в информационные технические системы, но, в первую очередь, наполнение смыслами, идеями, стандартами информационного пространства и всех вовлечённых в него пользователей.  
  
Соотношение важности действий по обеспечению кибербезопасности в технологической и социальной сферах оценивается как 10% к 90%. Наибольшая угроза идет со стороны внедрения информационных «вирусов» в сознание людей, культивирующих деградационные процессы. Сложность в том, что **сам механизм формирования общественного мнения и методов работы с социумом в информационной среде не виден.**Это позволяет сегодня беспрепятственно осуществлять психологические операции при помощи создания контента и управления им в социальных сетях.  
  
[](https://ss69100.livejournal.com/attachment/vstavka5/)Контент формирует общественное мнение, оказывает информационно-алгоритмическое воздействие на человека, побуждая его к определенным действиям, будь то выбор одежды, еды, места учёбы, времяпрепровождения, работы, страны для жизни, кандидата на выборах. Медиапродукты становятся инструментом для формирования стандартов мышления, ценностей, алгоритмов поведения человека.  
  
Для этого используются следующие приемы: *во-первых, психологическое давление; во-вторых, незаметное проникновение в сознание; в-третьих, скрытое нарушение и искажение законов логики*. Сюда относятся подмена тезиса, ложная аналогия, вывод без достаточного основания, подмена причины следствием, подмена понятий. В результате проведения подобных операций снижается интеллектуальный потенциал человека. Интеллект становится заточенным на потребление, разрушение и уже не способен самостоятельно приподняться над установленными алгоритмами.

Сегодня обработкой и анализом информации, формированием и распространением контента в режиме «онлайн» занимаются специальные **киберцентры**. Формирование общественного мнения происходит за счет массированной подачи информации и бессознательного доверия пользователя к полученным данным.  
  
Для этого используются киберботы – компьютерные программы, автоматически совершающие набор определённых действий на основе модуля искусственного интеллекта. Боты ведут пропаганду с помощью всевозможных методов вброса информации.  
  
Они способны вбрасывать и распространять контент с огромной скоростью, одновременно воздействуя на миллионы людей. Их действия сложно отличить от действий обычных людей в Интернете. Например, только под руководством Киберкомандования США работаeт не менее 7 киберцентров (а есть ещё Великобритания, Германия, Франция, Китай, Израиль). В совокупности 500 операторов, работающих в одном таком центре, управляют 50 000 киберботами. На практике это означает, что на одного оператора приходится 100 ботов.  
  
Именно из таких киберцентров массово осуществляется комментирование новостей, троллинг, рассылка информации и прочее. При этом следует понимать, что воздействие возможно из любой точки киберпространства: в виртуальной среде отсутствует привязка к конкретной территории.

[](https://ss69100.livejournal.com/attachment/awesomecyberpicture/)

Так, многолетняя агрессивно направленная пропаганда против русских на Украине неизбежно привела к вооруженному конфликту внутри страны, к непрекращающемуся военному столкновению России и Украины.

Ещё 15 лет назад жители самой Украины представить не могли, что будут открыто воевать против России. Но сегодня население, подвергшееся влиянию информационной войны, в изменённом состоянии психики, массово зарабатывает на горе жителей собственной страны.  
  
Более того, Украина используется как передовой пункт ведения информационной войны против России. По официальным данным ООН, на Донбассе в боевых действиях погибло порядка 10 тыс. жителей Украины, по неофициальной статистике зарегистрировано более 50 тыс. погибших с украинской стороны.  
  
И та же неофициальная статистика говорит о более 50 тыс. граждан Украины, кто в режиме онлайн работает на зарубежные киберцентры – посредством троллинга и спама в сети Интернет ведёт агрессивную пропаганду против России, дискредитируя её имидж, культивируя порочный образ жизни.

Инструкция США по ведению «гибридной войны» включает следующие последовательные шаги по её проведению: 1) **информационное противостояние: подготовка территории к восприятию и навязыванию чуждых ценностей, интересов**; 2) подрыв экономики с использованием политических, технических, информационных средств (Россия до сих пор не пережила своеобразный экономический переворот 2014 г. с многоаспектной девальвацией российского рубля); 3) подрыв политического статуса вплоть до цветных революций, смены политического руководства; 4) зачистка политнекорректных, кто не приемлет навязываемые перемены.

**[](https://ss69100.livejournal.com/attachment/bez-imeni/)**

**Именно целенаправленное нагнетание негатива в масс-медиа неизбежно приводит к проявлению негатива в жизни.** В том числе формирует преступления в молодёжной среде (правонарушения, наркомания, девиантное поведение, экстремизм). В основном преступления совершаются молодёжью под воздействием порочной агрессивной информационной среды. Это напрямую сказывается не только на статистике и качестве общественных явлений, но и усложняет ведение профилактической работы.

**На сегодняшний день в мире и в нашей стране ещё не созданы институты, способные остановить эти деструктивные процессы. Более того, нет даже понимания происходящего и всей его пагубности у профессионалов и обычного населения нашей страны и других стран мира.**

История со студенткой отделения культурологии философского факультета МГУ, дочерью интеллигентной семьи Варварой Карауловой, ставшей активисткой ИГИЛ, может и должна служить ярким и наглядным примером для нашего общества. Несмотря на широкую огласку в СМИ, суть этого «феномена» понимают немногие. Судебно-медицинская экспертиза признала студентку МГУ вменяемой, однако это далеко от реальности.  
  
Дело, в первую очередь, в том, что **критерии оценки состояния личности критически устарели**.  
  
Обследование на методах восприятия информации, не оценивает состояние алгоритмов восприятия и обработки человеком информации об окружающем мире. Они не учитывают, что это личность глубоко «поражённая», её психика не способна адекватно воспринимать происходящее и принимать правильные решения. **Подобное состояние сравнимо с контузией на поле боя**.  
  
Внешне человек сохраняет способность воспроизводить привычные ритуалы и стереотипы поведения, обладает отличной фактологией. Однако под массивным потоком информационного воздействия произошло критическое смещение в сторону неадекватной трактовки фактов, событий, явлений, полнейшая ценностная дезориентация. В этом контексте постановка вопроса «Понимала она или не понимала что делает» совершенно не уместна.  
  
Однозначный ответ – нет. Контуженных уносят с поля боя и проводят долгую реабилитацию. «Пустота в душе», о которой говорит Варвара, − следствие детской психики, неспособной самостоятельно взаимодействовать с миром реальным, и характерно оно, к сожалению, для всего молодого поколения, ежедневно выхолащиваемого технологиями масс-медиа.  
  
Этот «вакуум» у молодёжи не заполняется сегодня должным образом государственными, общественными институтами, семьёй. Речь вести нужно об *ответственности*, в первую очередь, государства и всего общества в целом.[](https://ss69100.livejournal.com/attachment/vstavka3/)

Этот и другие примеры свидетельствуют о том, что в таких условиях невозможно ориентироваться на устоявшиеся подходы (медицинские, педагогические, юридические и др.), привычные профессиональные критерии. А соответственно, как минимум ошибочно и даже преступно вести речь о введении стандартизации в работе с детьми и молодёжью в сфере воспитания и профилактики негативных социальных явлений. По крайней мере, на сегодняшний день, пока не выработаны здравые критерии и система адекватных действий.

На данный момент Россия находится на этапе выработки решений по формированию системы обеспечения информационной безопасности общества. Мы постепенно оцениваем специфику времени, перестраиваемся на новые подходы и методы работы в информационном пространстве.

Руководство нашего государства акцентирует внимание на вопросах кибербезопасности и оглашает их как на внутриполитическом, так и на внешнеполитическом контуре. На VII Международном Форуме безопасного Интернета, который состоялся в апреле 2016 г. в Москве, помощник президента И.О. Щеголев отметил необходимость выработки глобального консенсуса и определения ответственных сил в связи с нарастанием напряженностей в мире, новых угроз, связанных с киберпространством, и важность отведения государствам больших полномочий в регулировании интернет-пространства.

В этом направлении принимаются государственные нормативные документы, носящие принципиальный и рамочный характер. В декабре 2015 г. была утверждена «Концепция информационной безопасности детей», направленная на обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России.  
  
5 декабря 2016 г. Указом Президента РФ **утверждена новая «Доктрина информационной безопасности Российской Федерации»**. Доктрину приравнивают по значимости к мероприятиям по защите границ нашего государства. Защита границ относится к компетенции органов государственной безопасности, имеет большую инфраструктуру, сформированную годами, и соответствующее финансирование.  
  
Вывод мероприятий по информационной безопасности на подобный системный уровень работы, полноценное формирование кибервойск в России будут осуществляться на протяжении порядка 15 лет.

Речь идёт не только об оперативном противоборстве и отражении кибераттак в технической сфере, где российские войска и сегодня показывают себя достойно. Самая сложная и **основная задача − выявление скрытой социально-культурной угрозы**, ведущей к разрушению культурного кода России, и, соответственно, **выработка оперативных и стратегических контрмер для предотвращения** запуска негативных сценариев через информационную сеть.

**Анатолий Валерьевич Рудаков,**

**эксперт Фонда национальной и международной безопасности:**

«Современные средства массовой коммуникации формируют особый вид идентичности за счёт ментальных вирусов. Они разрабатываются как в коммерческих целях, так и в боевых геополитических, когда ставится задача манипулирования конкретными целевыми группами.  
  
Этому можно противостоять и рецепт здесь один – это защита тех форм идентичности, которые у нас исторически сложились. Существующей сети различного рода информационных ресурсов, через которые транслируются разрушительные смыслы, противостоять может только контрсеть, развиваемая людьми, кто отстаивает свои ценности и смыслы.»

Информационная война уже сегодня глубоко поразила наше общество. Поэтому адекватный ответ и решение современных вызовов возможны лишь при условии масштабного включения населения во взаимодействие с властью и содействие правоохранительным органам.

На данный момент, пока ещё, субъектами управления в киберсреде остаются разные правительства, корпорации, гражданское общество. И гражданскому обществу принадлежит особая роль − пользователи, создающие и распространяющие контент, формирующие адекватный взгляд на мир приравниваются сегодня к солдатам «народного ополчения» на поле противоборства за умы наших детей и здоровое безопасное будущее.

**В России необходимо формировать** такое **гражданское общество**, в полноценном смысле, **способное осуществлять самостоятельно мероприятия по самообороне**. Начинать необходимо с просветительской разъяснительной работы с населением.  
  
В противном случае тематика дня и призыв о помощи не будет воспринят обществом, не удастся сформировать **«дивизии народного ополчения»**.  
  
[](https://ss69100.livejournal.com/attachment/vstavka4/)При всём этом надеяться лишь на «народное ополчение» глупо и бесполезно. Общественные силы самоорганизации смогут лишь временно приостановить разрушительные явления. Подобно действиям во время Великой Отечественной войны 1941–1945 гг. населению для защиты своей земли необходима поддержка профессиональной армии – артиллерии, танков, авиации.  
  
Это, в свою очередь, требует организации специального обучения. Также как невозможно заочно присвоить квалификацию летчика без должной подготовки, при столкновении с реальной киберугрозой «заочные ордена и степени» на деле никому не помогут.

В современном контексте речь идёт о специалистах, способных:

— описывать происходящие на уровне страны и мира явления и процессы;

— произвести оценку происходящих событий с позиции: хорошо-плохо, приемлемо-неприемлемо, целесообразно-нецелесообразно;

— вести самостоятельную разъяснительную работу на местах относительно современных угроз и вызовов, путей их решения;

— организовывать общественные группы, в т.ч. из числа молодёжи, ведущие активную контр и упреждающую работу по созидательной пропаганде, разъяснению в социальных сетях.

Основным препятствием на пути выстраивания системы современной защиты может стать «псевдопатриотизм» с постановкой заведомо «ложных целей», навязыванием борьбы с «мифическим врагом» и «мнимыми победами» в интересах заочно заработать политические бонусы на патриотизме, войне и горе. В этих условиях может сложиться ситуация, когда активно обсуждается проблематика, все громко порицают и борются с явлением – но дальше слов дело не идёт.  
  
В таком случае (по аналогии с историей) поднятые на защиту Родины «народные дружины» не дождутся подхода основных сил и просто погибнут.

**Владимир Владимирович Путин,**

**президент Российской Федерации:**

«Эта работа непростая, и самая главная «засада», самая главная опасность этой работы – если она будет формальной. Она тогда убьёт нашу конечную цель на корню, с первых шагов. Ведь люди настолько устали от прямой и тупой пропаганды, что они перестали ей доверять. А в этом деле очень важны честность, открытость и, в конечном счёте, эффективность. Чрезвычайно важные вещи.  
  
Если мы не добьёмся этого состояния работы по этому направлению, результат будет нулевой либо отрицательный. Шаблон в этой работе абсолютно недопустим, он контрпродуктивен.»

Встреча с представителями общественности по вопросам духовного состояния молодежи и ключевым аспектам нравственного и патриотического воспитания.

Таким образом, необходимы:

— осуществление широкой просветительской работы с населением по вопросам кибербезопасности и разъяснению методов противодействия современным угрозам, обучение сохранению своего культурного кода;

— формирование групп населения («дивизий народного ополчения») по созданию и распространению созидательного контента, ведения разъяснительной работы;

— подготовка специалистов по превентивной работе с детьми и молодёжью на специальной ценностной основе и критериях;

— формирование системы специальной подготовки кадров в области информационной безопасности;

— создание отечественных экспертных информационно-аналитических центров, которые в состоянии решать вопросы кибербезопасности во всех направлениях;

— разработка и внедрение теоретико-методологического и аналитического материала для обеспечения данной деятельности (в т.ч. выработка новых критериев оценки негативных социальных явлений, степени их воздействия на личность и последствия).

Этот материал подготовило экспертное сообщество Центра СИ. С одной стороны, мы разрабатываем научно-аналитические подходы по обеспечению кибербезопасности общества, с другой стороны, на практике отрабатываем методы работы с молодым поколением, с населением на основе современных информационных подходов.[[1]](https://ss69100.livejournal.com/3505073.html#1) Особое внимание нами уделяется выработке у человека алгоритма различения разнокачественных информационных потоков – основного защитного механизма от киберугроз.

Осуществляя эту работу, мы на своём примере сталкиваемся со всеми негативными проявлениями информационной среды, в том числе со всевозможными противодействиями разных групп. Кто-то из них действует бессознательно, являясь носителем прошитых деструктивных ценностей, кто-то – намеренно в целях наживы.

И, тем не менее, мы знаем, что, если этими вопросами не заниматься, шанса нет ни у кого – ни у нас с вами, ни у наших детей. В этих условиях не удастся ни переждать, ни отмахнуться, речь идёт о выживании и сохранении человека как вида на планете Земля.

От каждого жителя, нашей осознанности зависит – будет ли у нас будущее и каким оно будет. Каждый из нас в состоянии своими конструктивными действиями давать отпор самым негативным сценариям.

В свою очередь, призываем все здоровые силы не сдаваться под гнётом агрессивных факторов, активно разбираться с вопросами кибербезопасности и помогать в этом другим, день за днём формировать силы гражданской обороны для защиты от информационной агрессии и создавать условия для подготовки в России профессиональных специалистов в этом направлении.

Основные принципы воздействия на человека виртуального пространства и информационных технологий, входящих в категорию кибероружие, освещает аналитический фильм [«Территория БезОпасности»](https://www.youtube.com/watch?v=xAf246oXDis).

Он будет полезен всем, кто заинтересован в устойчивом развитии нашей страны, в мирном будущем наших детей.

Материал подготовлен экспертным сообществом [**Центра СИ**](http://center-si.com/analitics/kak-zashhitit-sebya-i-nashix-detej-v-kibersrede/)