Андрей Афанасьев

Методическое пособие. Основы выживания в сети. Краткий курс для детей и родителей

Москва 2022

Оглавление

1. Вступление…….5

2. Поисковики……7

О проблеме поиска информации……...7
Википедия……..10
Перевернутый алгоритм восприятия информации…… ……14

3. Мошенники. …… ……17

Телефонные мошенники……..17
Интернет-мошенники……... 23
Поддельные интеренет-магазины……30
Фишинговые ссылки Опасные приложения …….…… 33
Сайты-казино, ставки на спорт, букмекерские конторы……. .35

4. Компьютерные игры……..37

Сайты-казино в игровой индустрии. Мошенники. ……...…46

5. Шантаж, вымогательство…… ….48

Шантаж интим-контентом…….… …..48
Псевдошантажисты…… …..49
Откуда шантажисты берут материалы…….. ….51
Что делать, если вы подверглись шантажу?..... .52
Как быть, если компрометирующие вас данные уже попали в сеть?..... .53

6. Манипуляторы…….…….. 54

7. Опасные группы…… …60

Деструктивные группы…….. 60
Причины интереса деструктивных групп к детской аудитории..62
Семантические капсулы. Эхо-камеры социальных сетей……66
Радикализация. Переход обычных групп в разряд деструктивных……..68
Околосектантские группы…….…..70
Пропаганда насилия……71
Экстремистские группы……...72
Почему люди так доверяют всему прочитанному в сети?.....74
Политические манипуляторы. Использование детей в качестве

протестной силы…….…….….75
Как не попасть в обработку таких групп?.....78
Темные места Интернета……..……80

8. Ответственность за распространение информации…...…..81

Самые распространенные заблуждения……..….81
Экстремизм……85
Что будет, если вы по незнанию опубликуете какой-то материал из списка запрещенных?.....90
Травля, буллинг…….……92
Клевета…….…..94
Конфликты, ссоры, оскорбления…….……94
Взлом аккаунта……..……95

9. Фейки……..……..95

Ответственность за фейки…….…..98
Ответственность за ложные сообщения об актах терроризма…100
Дипфейки…….102

10. Наркотики……102

Распространение…….104
Вовлечение……..105
Ответственность за распространение. …….107

11. Снюсы, вейпы, электронные средства

доставки никотина……..108

12. Рекомендации по безопасности аккаунта в сети……..…112

13. Новая цифровая реальность……...118

14. Есть ли у вас интернет-зависимость? Тест…….…….123

15. Заключение……..……124

16. Рекомендации для органов государственной власти….126

1. ВСТУПЛЕНИЕ

Данное пособие предназначено как для родителей, так и для детей, начинающих самостоятельное использование сети Интернет.

Что же такое Интернет – добро или зло? На этот вопрос не будет прямых ответов, но по нашим наблюдениям можем сказать, что он ни то, ни другое. Первое слово, которое более всего подходит для описания большинства процессов, происходящих в Интернете – это манипуляция.

Под манипулированием обычно понимают систему способов идеологического и социально-психологического воздействия с целью изменения мышления и поведения людей вопреки их интересам. Подобные приёмы используют в своей работе не только обычные мошенники, о которых мы поговорим в начале, но и более крупные игроки, на которых мы подробнее остановимся в главе «Опасные группы».

По своей сути Интернет является инструментом по распространению информации, но, как и любой другой инструмент, он может служить как во благо, так и во вред.

При помощи топора можно сделать из бревна произведение искусства, а можно нечаянно отрубить себе ногу – всё зависит от знания и умения человека, взявшего его в руки. Аналогичная ситуация с Интернетом: данный инструмент, попадая в плохие руки, может нести хаос и разруху, а, попав в хорошие, принесёт пользу и знания. Все зависит от конкретного человека, использующего этот достаточно сложный инструмент.

Ещё Интернет уместно сравнить с дорожным движением, ведь все действия, производимые пользователями в сети, – это движение информации. Как в автомобильной, так и в интернет-среде это движение подчиняется определенным правилам, незнание которых может привести к серьёзным и достаточно печальным последствиям.

Основной продукт, производимый в Интернете, – информация. Она создаётся в сети в таком объёме, который сложно вообразить. Однако качество производимой в Интернете информации зачастую весьма сомнительное, поскольку основной её массив никем

не проверяется и не контролируется, что создает большие проблемы у пользователей.

К сожалению, мы вынуждены признать, что на данный момент интернет-среда функционирует по принципу диких джунглей, и при внешней иллюзии удобства, простоты и безопасности в сети сегодня орудует огромное количество людей-манипуляторов, несущих деструктивные идеи, пытающихся либо подчинить других людей своей воле, либо желающих заработать на них денег. Несмотря на вполне очевидные цели манипуляторов, их не так просто распознать, а борьба с ними, равно как и борьба с создаваемыми ими сообществами, у нас в стране ведется, к сожалению, крайне неэффективно. По отдельным направлениям она полностью отсутствует, что порождает еще большие проблемы.

Причины такого положения дел разбирать не будем, поскольку цели нашего пособия другие – научить вас выживать в современных интернет-джунглях, а также научить вас тому, как не стать лёгкой добычей для интернет-хищников разных направлений. Для этого разберём основные манипуляции и приёмы, используемые мошенниками и манипуляторами, пытающимися на вас заработать, а также уделим особое внимание тем, кто занимается этим официально.

Заметим, что далеко не все мошенники и манипуляторы в Интернете выглядят как люди с плаката «их разыскивает полиция». Часто они могут быть известными, цитируемыми и раскручиваемыми в СМИ людьми, быть рукопожатными и даже служить для многих образцами и моделями поведения, что на самом деле не меняет их сути. Такие примеры мы тоже рассмотрим.

Кроме вопросов, касающихся вашей личной безопасности в Интернете, мы также поговорим и про ответственность. Как вам самим не попасть в неприятные ситуации, связанные с нарушением закона в сети? Какие законы работают в Интернете? Что вам можно, а что ни при каких обстоятельствах нельзя публиковать, и какая за это будет ответственность? Про это поговорим в главе «Ответственность за распространение информации».

2. ПОИСКОВИКИ

О проблеме поиска информации

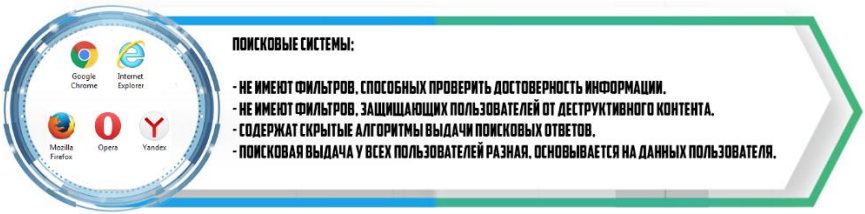
Первое, с чем сталкивается человек, вошедший в Интернет, – это поисковик. Поисковых систем существует достаточно много, и мы не будем разбирать каждую из них отдельно, потому что те отличия, которые между ними существуют, крайне незначительны и не имеют отношения к основной теме пособия. Нам важно понять другое: насколько та информация, которую выдают эти поисковики, является правдивой, как её отличить от ложной, и можно ли в принципе доверять поисковым системам?

Сразу начнём с вывода и прямого ответа – **полностью доверять им нельзя!** Да, поисковые системы несут безусловную пользу в тех случаях, когда нам надо найти какой-то конкретный сайт или адрес. Они очень удобны для поиска товаров, фильмов, музыки, и т.д., но при этом они же служат и навигатором по морю фейков, вбросов, ложной и заведомо недостоверной информации, причём поисковики освобождены от какой-либо ответственности за выдачу в топ недостоверной, опасной и ложной информации, что порождает многие неочевидные для пользователей проблемы, о которых поговорим далее.

Как большинство родителей, да и учителей сейчас учат ребенка пользоваться поисковиком? – «Набираешь запрос, и первые строчки выдачи – это и есть нужная и достоверная информация». Для того, чтобы понять, почему так делать категорически нельзя, разберём на примере, как работает поисковая машина Яндекса или Гугла. Не будем вдаваться в сложные термины и алгоритмы, а попробуем объяснить простым языком общий принцип.

Есть такое понятие, как релевантность поискового запроса. Оно означает соответствие интента (поискового намерения), заложенного в запросе, и выдачи в поисковой системе, полученной в результате этого запроса. Когда вы задаете поисковый запрос Яндексу или Гуглу, то в первых строчках он выдает ссылки не на те сайты, которые наиболее достоверные и безопасные, а на те,

которые наиболее посещаемые, популярные и цитируемые в поставленном вами вопросе. Так работают все поисковые машины, и они не оперируют такими понятиями, как честность, правдивость или безопасность.



Все популярные поисковые системы изначально не имеют никаких фильтров и ограничений выдаваемой информации, а это очень важно, потому что компании и продавцы всякой всячины круглосуточно ведут жёсткую борьбу за право оказаться в первых страницах выдачи информации по определённым поисковым запросам.

Многие из них тратят огромные деньги на то, чтобы оказаться в верхних строках выдачи. Так что по популярным поисковым запросам в первых строчках выдачи результатов поиска всегда будут хорошо раскрученные и проплаченные ресурсы, владельцы которых часто тратят немалые средства на то, чтобы оказаться в топе.

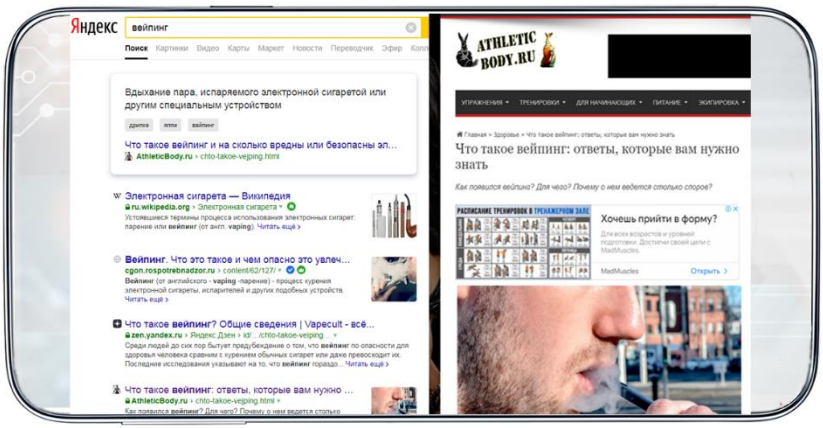
На практике это приводит к тому, что если вы спрашиваете, например, о вреде чего-то, то попадаете в первых строках поисковой выдачи на сайты тех, кто это «что-то» и продаёт. Как вы думаете, какой направленности там будут статьи? Они расскажут вам правду о товаре? Конечно, нет!

А ведь товаром может быть не только вещь. Точно таким же образом продаются и навязываются политические и социальные взгляды, убеждения и идеи – всё, что угодно. Технологически это уже давно стало возможным, и вы должны понимать: всё, что вы видите в поисковой выдаче в первых строках, могло там оказаться не просто так.

Приведем конкретный пример. Сейчас актуальна проблема подсадки детей табачными компаниями на свою продукцию. Подробно мы это разберем в отдельной главе, сейчас же рассмотрим

один из методов продвижения табачниками этой опасной продукции среди детей – как они это делают через распространение ложной информации о якобы «безопасности» и даже «пользе» всех электронных систем доставки никотина.

Ещё относительно недавно, если вы вводили в поисковой строке Яндекса слово «вейпинг», то первой в выдаче была статья, в которой оказались собраны все ложные аргументы о якобы «безопасности» этих систем. По факту это была рекламная статья, практически гарантированно написанная по заказу продавцов всей этой отравы.



Но это не единственная манипуляция, используемая в данном примере: статья была размещена на сайте https://athleticbody.ru, название которого переводится как «атлетическое тело». Таким образом, у пользователей возникала ассоциация со спортом и со здоровьем, – и это ещё одна манипуляция, призванная убедить читателя в якобы безопасности всех этих систем.

Любопытно, что долгое время именно эта статья и именно с этого сайта выдавалась в первой строке при поисковом запросе «вейпинг», и не исключено, что именно продавцы вейп-продукции приложили к этому руку. За деньги, которые у них есть, вполне возможно создать качественную поисковую оптимизацию, продвижение и, тем самым, вывести нужную им ложную информацию

в топ. Существуют даже специальные сервисы, занимающиеся именно таким продвижением.

Поисковые системы никогда не проверяли, не проверяют и не будут проверять свои результаты выдачи на предмет честности и безопасности как сайтов, так и отдельных статей, и про это важно всегда помнить.

Кроме того, что поисковая выдача в принципе не может быть абсолютно достоверной, она ещё и у всех разная. Вы можете это легко проверить. Попробуйте, находясь в компании друзей, вбить один и тот же поисковый запрос на разных телефонах. У каждого из вас, скорее всего, будут разные ответы, в которых поисковик будет учитывать ваши предыдущие запросы, предпочтения и прочие факторы, известные только ему. Имея такие возможности, будет ли Гугл или Яндекс манипулировать людьми в своих интересах, давая им «правильные» ответы на их поисковые запросы? Мы не знаем точно, но это информация для размышления, и об этом стоит задуматься.

Так что ни о какой объективности в работе поисковиков уже давно речи не идёт, и это даже не столько техническая, сколько гуманитарная проблема, которая, скорее, никогда не будет решена. Никакой искусственный интеллект никогда не сможет отличить добро от зла, также как и правдивую информацию от ложной – это технически невыполнимая задача.

Википедия

Удивительно, но многие люди по всему миру, включая Россию, до сих пор считают Википедию чуть ли не истиной в последней инстанции, хотя это сосем не так. Названный ресурс не имеет никакого отношения ни к науке, ни к медицине, ни вообще к чему-либо серьёзному. Это хорошо раскрученный бренд, но не более того.

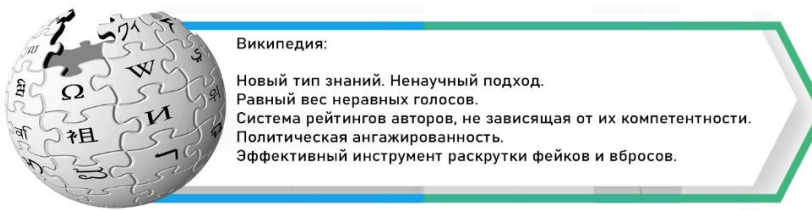
Далее приведём цитаты из книги Игоря Ашманова и Натальи Касперской «Цифровая гигиена». Всем рекомендуем её к прочтению, поскольку она является на сегодняшний день лучшим сборником

материалов по теме Интернета, составленным профессионалами, работающими в этой сфере.

«Википедия действительно представляет собой новый тип знаний. Он именно новый. Это знание не доказанное, подтвержденное экспертами, известными специалистами и учеными (как в обычных энциклопедиях и учебниках), а знание консенсуса, согласие между собой авторов и администрации интернет-энциклопедии, подтверждаемое ссылками на «авторитетные источники».

По сути, это бытовое знание вида: «да все в городе знают, что…» со всеми его рисками и недостатками. Да, быстро понять, что означает новое слово или понятие, проверить дату или имя-отчество в Википедии можно. Полагаться на достоверность – нельзя. Составлять себе базовое представление о мире, обществе, истории, личностях, по статьям Википедии категорически нельзя и даже очень вредно. Не говоря уж о подготовке к экзаменам или самолечении.

Условно говоря, распространенный миф, о котором много написано в СМИ, имеет все шансы стать «знанием» в Википедии».



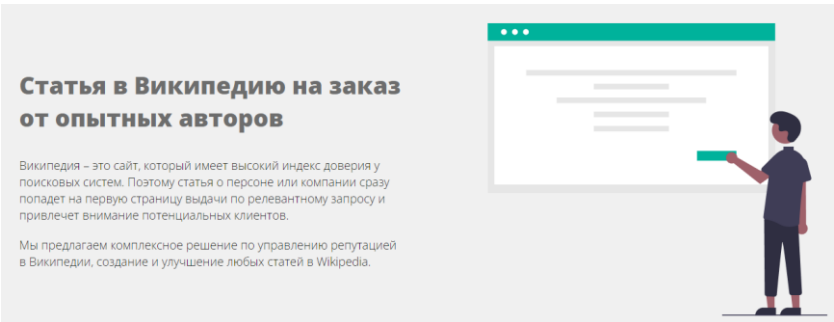
Отдельно важно сказать про авторов статей Википедии. Практически в 100% случаев это люди, не имеющие образования и реального в тех темах, по которым они пишут, или, что ещё хуже – правят статьи. Обычно это энтузиасты, обладающие большим запасом свободного времени, которого нет у профессионалов ввиду их постоянной занятости. В итоге Википедия – это продукт, созданный не экспертами и не профессионалами, в отличие от настоящих энциклопедий или научных книг.

Хотя некоторые из профессионалов своего дела всё же иногда пытаются исправлять неточные и откровенно недостоверные данные. Но это не так просто и, как они пишут, «*единожды исправив ошибку, или написав статью в Википедии, ты до конца жизни*

вынужден стоять возле неё с палкой и отмахиваться от толпы невежд, имеющих другое, более ценное мнение о данной проблеме, и более высокий рейтинг в Википедии, который на самом деле ни о чём не говорит».

Если мы посмотрим рейтинг авторов текстов Википедии, то увидим, что все верхние позиции там занимают боты – программы, которые пишут эти статьи. Как вы понимаете, качество у них соответствующее…

Кроме того, коммерческую составляющую никто не отменял. Поскольку этот ресурс крайне раскручен, любая относительно грамотно и околонаучно написанная статья вполне может оказаться в топе выдачи, чем умело пользуются и люди, желающие вывести свою не совсем безопасную продукцию в топ, как в случае с вейпами, о которых мы писали выше. Для них есть даже специальные сервисы (скрин) сайты, открыто предлагающие подобные услуги. За деньги заказчика они делают любую информацию «знанием, закрепленным в Википедии».



Более того, ввиду своей крайней популярности Википедия давно стала политическим инструментом по продвижению в массы нужных заказчикам мнений. Происходит это всегда по одной схеме: создание (редактирование) статьи в нужном русле и тут же, пока не исправили, ссылка на неё в крупных СМИ как на «проверенный и надёжный источник». Это же сама Википедия, как можно ей не верить? Картину дополняют и вышеупомянутые боты, которые также включаются в процесс и следят за «правильной» повесткой.

Основываясь на личных наблюдениях, можем сказать, что если в Википедии даётся статья о каком-нибудь хорошем и достойном человеке, но при этом не следующем «правильной» повестке, то все его положительные качества будут принижены, а незначительные ошибки или неудачные высказывания сильно преувеличены и заявлены как его главные достижения, хотя они такими не являются.

Кроме того, простой интернет-вандализм в Википедии – дело достаточно привычное. Причин тому множество: чья-то личная неприязнь к субъекту статьи, желание повеселиться, искренняя убеждённость в верности позиции, отличной от той, что приведена в текущей версии материала и т.д.

Конкретный пример: в 2009 году второкурсница колледжа вместе со своим приятелем решила внести в ряд Вики-статей невинные и на первый взгляд достоверные правки. Просто так, ради смеха. Они всласть потрудились над несколькими заметками об американских детских писателях – не огульно добавляя туда откровенную ложь, а приписывая из головы какие-то «факты», им самим показавшиеся на тот момент достаточно оригинальными и правдоподобными. Последствия того вечера за компьютером нежданным бумерангом вернулись к ней. Онлайновая журналистка, уже успевшая доучиться в колледже, вдруг обнаружила, что её невинная правка в статье об Амалии Беделии живёт и здравствует. Да ещё как живёт! Её цитируют, на неё ссылаются, а исследователи детской литературы на её основе даже делают далеко идущие выводы!

Еще один пример. Уиллиам Конноли – один из ведущих учёных в мире, занимающийся моделированием климатических изменений на Земле, как-то на досуге редактировал Википедию строго по своему вопросу. Само собой, он ввязался в войну правок, обвинив других редакторов в полной некомпетенции в вопросе, за что и был забанен, получив ограничение вносить одну правку в неделю. Администрация обвинила Коннели в том, что страницы Википедии должны представлять несколько точек зрения на проблему. Поэтому его научная репутация в данном вопросе роли не играет.

В Википедии действует принцип «**равный вес неравных голосов**», и этот пример очень показателен в плане «научности» Википедии.

Итак, если человек не подготовлен в каком-то вопросе или не имеет в нём своего жизненного опыта, то практически на 100% он столкнется в сети с дезинформацией. Вы сами можете в этом легко убедиться, воспользовавшись поисковиком и начав искать информацию, в которой лично хорошо разбираетесь. Проверьте ради интереса, сколько дезинформации и глупости вы прочтёте, а ведь это происходит во всех сферах.

Перевернутый алготритм восприятия информации

Чем больше вы включены в реальность, тем более адекватно вы можете реагировать на меняющуюся обстановку, и тем правильнее и полезнее в первую очередь для себя самого решения вы можете принимать. Если же вы воспринимаете реальность через медиасреду и Интернет, то вы контактируете уже не с настоящей реальностью, а с реальностью искусственно для вас созданной, которая может кардинально отличаться от истинного положения вещей. В таком случае, все принятые вами решения уже будут выгодны и полезны не вам, а создателям той самой параллельной реальности, которую предлагает медиасреда.

Получается, чем больше человек проводит времени в Интернете, тем больше он оторван от реальности, и тем более он зависим от чужих манипуляций, навязываемых извне, – неважно, какой контент он потребляет – хороший или плохой.

В одном исследовании изучалось, каким образом количество времени, которое молодёжь проводит в виртуальной среде, менялось в сторону увеличения: приблизительно в 2014 году произошёл переворот – теперь молодёжь часто проводит более 7 часов в день. Такому массовому уходу в виртуальную среду во многом поспособствовал технологический переход на переносную электронику, то есть на смартфоны.

В результате такого перехода у многих подростков неизбежно поменялись ориентиры, и для них виртуальные люди и виртуальные герои стали более значимы, чем реальные люди, учителя и родители. Вы, наверное, замечали, как некоторые ваши друзья начинают перепроверять всё услышанное от вас в Интернете, т.е. они стали доверять сети больше, чем вам, живым людям. И чем больше человек проводит времени в Интернете, тем эта взаимосвязь сильнее, и тем более мнение, написанное там непонятно кем и зачем, становится для них важнее и авторитетнее. О достоверности информации в сети мы уже говорили выше.

Соответственно, чем дальше, тем человек становится менее способным объективно воспринимать реальность, и тем проще становится манипуляторам внушать ему альтернативную реальность, нарисованную кем-то для того, чтобы его использовать.

Таким образом, у людей переворачивается сам алгоритм анализа информации. Если мы прочитанное в Интернете сразу подвергаем внутреннему сомнению и сверяем с тем, что знаем из своего жизненного опыта, то у них всё происходит наоборот. Если они что-то слышат от взрослых или учителей, то сразу подвергают

сомнению и сверяют с тем, что им напишут в Интернете в первых строках поисковых запросов.

Вот и получается, что они становятся напрямую управляемыми теми, кто формирует и оплачивает вывод в топ определённых ссылок по поисковым запросам. Достаточно за деньги вывести какие-то сайты и статьи в верхние строчки, как всё, что там написано по просьбе заказчика, и будет для таких людей истиной в последней инстанции, а не ваши слова и жизненный опыт. При этом у внушаемых людей не происходит разрыва реальностей. Если информация в Интернете не соответствует и не совпадает с тем, что они видят в настоящей жизни, то они всё равно выбирают информацию в Интернете и верят именно ей, несмотря даже на полное несоответствие. Это страшно, поскольку людей, предпочитающих виртуальную информацию реальной, с каждым годом становится всё больше.

Поэтому всегда сверяйте то, что читаете в Интернете, с реальной жизнью, а не наоборот. Доверяйте в первую очередь живым людям, а не говорящим головам с экрана. Эта привычка поможет вам более объективно воспринимать реальность, а, значит, и принимать для себя правильные и независимые решения.

Но даже если вы используете проверенную и объективную информацию, помните – Интернет предлагает информацию, но не знания: это совершенно разные понятия. Информация – это сырые данные, не позволяющие делать какие-либо выводы или служить поводом для принятия важных для вас решений. Информация ценна только в том случае, если вам известен контекст, а также глубина темы, по которой вы нашли нужную информацию. Только в таком случае она закрепляется и переходит в категорию знаний.

Интернет нас приучает к быстрому получению информации, но не знаний; к тому же то, что легко достаётся, также легко и быстро забывается. Это можно сравнить с ездой по навигатору: когда вы едете по нему, вы не запоминаете дорогу, но стоит вам найти адрес

самостоятельно или по карте, – вы его навсегда запомните, потому что приложили к этому усилия.

Именно поэтому, найдя какую-либо информацию по поисковому запросу, вы быстро её забываете – так устроен ваш мозг. К тому же сама привычка быстрого получения информации приучает ваш мозг не запоминать её, он как бы вам говорит: а зачем запоминать, если можно загуглить? В итоге мы уже сейчас можем видеть людей, похожих на киборгов, постоянно гуглящих, у которых часть мозга и памяти находится в телефоне. Эксперименты показывают, что привычка всё время обращаться к смартфону отупляет на физическом уровне, потому что она постоянно прерывает течение мысли, отучает от построения мыслительных цепочек и рассуждений.

Таким образом, в современных реалиях ваши настоящие знания – это то, что вы можете сказать людям без подключения к Интернету, и чем больше у вас будет таких реальных «оффлайн» знаний, тем будет лучше, прежде всего, для вас.

3. МОШЕННИКИ

Мошенничество сейчас, пожалуй, – самый быстро растущий по количеству вид преступлений, особенно когда речь идет об Интернете. К сожалению, рано или поздно с ними сталкивается каждый пользователь, и вы тоже обязательно с этим столкнётесь, и не раз, поэтому разберём основные виды мошенничества, чтобы знать, как их избежать.

Телефонные мошенники

Это необязательно звонки со службы безопасности банка, хотя они пока что безусловные лидеры. Звонить вам может кто угодно, причём по любому поводу. Вас могут просить помочь в расследовании, говорить о том, что на вас оформлен кредит, что нужно

срочно перевести деньги на другой счет и т.п., – каждый день придумываются новые более изощрённые схемы.

Все схемы разбирать не будем, но остановимся на главных и общих принципах, на которые следует в первую очередь обращать внимание. Недаром говорится, что «знание нескольких принципов освобождает от знания многих фактов». Вам нужно просто запомнить некоторые базовые моменты, которые необходимо всегда держать в голове.

Никогда и ни при каких обстоятельствах никому нельзя называть: **задние три цифры на карте и коды из СМС!** Про эти два пункта вы должны всегда помнить, потому что они – основа всех схем.

Разговор с мошенником может быть о чём угодно, но в конечном счёте ему всегда от вас нужны только три цифры на обороте и код СМС. Номер вашей карты он, скорее всего, уже знает – это не такая уж и тайна, а вот информацией о трех цифрах он владеть не может: они являются ключом от вашей карты и, сообщив их, неважно кому и как, вы сразу же отдаете все свои деньги.

Помните, что сообщая мошеннику код из СМС, вы тем самым как бы ставите свою электронную подпись под согласием передать ему свои деньги, после чего банк их вам уже не вернёт. Никогда и ни при каких обстоятельствах сотрудники банка, полиции, ФСБ и прочих ведомств не будут спрашивать у вас эти три цифры с оборота карты или код из СМС, поэтому если в любом диалоге вы слышите просьбу сообщить такую информацию – сразу вешайте трубку. В 100% случаев – это мошенники.

Никогда не перезванивать на незнакомые номера.

Если вам позвонили с незнакомого номера, а вы не успели взять трубку, – никогда не перезванивайте. Есть у мошенников одна простая схема, на которую попадаются очень многие. Они оформляют себе платный номер, при звонке на который у любого абонента за каждую минуту разговора снимается определенная сумма на их счёт. После этого они начинают звонить всем подряд, и сразу же сбрасывать для того, чтобы человек им перезвонил и «подарил» немного денег. Сотовые операторы, несмотря на всю очевидность такого мошенничества, до сих пор не пресекают подобные схемы

и продолжают на них зарабатывать вместе с телефонными аферистами.
Завершая тему телефонного мошенничества, разберем основные приёмы, используемые мошенниками при разговоре – запомните, и если услышите их в телефонном диалоге с неизвестными людьми, – вешайте трубку.

Приемы телефонных мошенников:

1). Срочность! Главная цель мошенника – сбить вас с толку, и заставить принять вас срочное, но очень нужное для него решение. Он прекрасно понимает, что любой, даже самый короткий обрыв диалога приведет к тому, что вы начнёте сомневаться, вспомните правила действий в подобных ситуациях, и сойдёте с его крючка. Поэтому всегда помните, что срочность в диалоге – явный маркер манипуляции.
2). Действия под диктовку. Как только вам начинают диктовать, что нужно делать (скачать приложение, ввести код, перейти на сайт, набрать комбинацию цифр и т.д.), сразу же вешайте трубку – вы в руках мошенников.
3). Помощь в поимке преступника. Вам звонит якобы представитель полиции (ФСБ, Росгвардии, Налоговой, ССП, т.д.) и просит вас помочь поймать преступника, пытающегося прямо сейчас украсть деньги с вашей карты. Еще вам могут сказать, что прямо сейчас на вас оформляется кредит, или что они ловят сотрудника Сбербанка, совершающего махинации с вашим счётом – версии могут быть какие угодно, но цель мошенника всегда одна – получить от вас нужные для него данные. Бывают схемы, когда вас самих ставят в роль подозреваемых, когда предполагаемый преступник – это вы. Тут используется та же самая манипуляция на страхе, только страх уже не за своё имущество, а за свою свободу.
Запомните главное: если вам кто-то звонит и представляется сотрудником правоохранительных органов, то это уже практически 100% обман. Сотрудники полиции и прочих силовых ведомств никогда не решают такие вопросы по телефону, и если им на самом

деле нужно будет с вами связаться, то они обязательно нанесут вам визит. По телефону вы не можете удостовериться в личности собеседника, соответственно, все представления по телефону ничего не стоят и не имеют никакой юридической силы. Поэтому кто бы вам ни звонил, и кем бы ни представлялся, вы можете совершенно спокойно, не опасаясь никаких последствий, положить трубку – имеете на это полное право, даже если это окажется на самом деле сотрудник полиции.

4). Выгодное предложение! Если предыдущие схемы работали на эксплуатацию человеческого страха, то данная схема работает на эксплуатацию человеческой жадности. Вам звонит представитель крупной фирмы (популярного интернет-магазина, игры, в которой вы делали покупки, и т.д.) и сообщает вам о выигрыше в конкурсе, лотерее или чём-то подобном. Либо вам делают «уникальное предложение» о покупке чего-то очень ценного за сущие копейки. Если вы клюнули, то дальше уже дело техники.

Мошенники часто пользуются той информацией и теми цифровыми следами, которые мы сами оставляем в Интернете, когда посещаем определенные сайты или пишем комментарии. Данная информация собирается, обрабатывается и перепродается, в том числе и легально.

Подобные базы покупают мошенники, и тогда они уже звонят вам не как рядовому абоненту, а именно вам как конкретному человеку. Поэтому когда вы слышите в трубке приятный голос, который обращается к вам по имени отчеству и говорит от имени какого-либо крупного интернет-магазина, вы не должны расслабляться: с большой степенью вероятности вы общаетесь с мошенником, и ваша «выгодная покупка» будет сделана в его пользу.

То же самое касается сообщений в мессенджерах. Такие сообщения очень часто приходят с контактов, на аватаре у которых стоит логотип какого-нибудь популярного интернет-магазина. Вроде бы, мелочь, но многие люди верят в подлинность таких сообщений, следуют инструкциям мошенников, и в итоге лишаются своих денег.

5). Спишемся в мессенджере! Большинство пользователей не видят особой разницы между звонками по телефону и общением в

мессенджерах, хотя в плане безопасности разница есть, и она более чем существенная.

Дело в том, что все наши телефонные звонки фиксируются, записываются и, согласно закону Яровой, хранятся по полгода, представляя из себя в случае чего доказательную базу, что для мошенников не очень хорошо. С мессенджерами ситуация иная. Все сервера самых популярных у нас мессенджеров находятся за границей, в связи с чем часто возникают проблемы с получением переписки в случае возбуждения уголовных дел. Кроме того, в мессенджерах используется шифрованное соединение, которое не позволяет получить данные о переписке и разговоре вне сервера мессенджера. Эти технические нюансы хорошо знают мошенники, и именно поэтому мессенджеры – их главный инструмент.

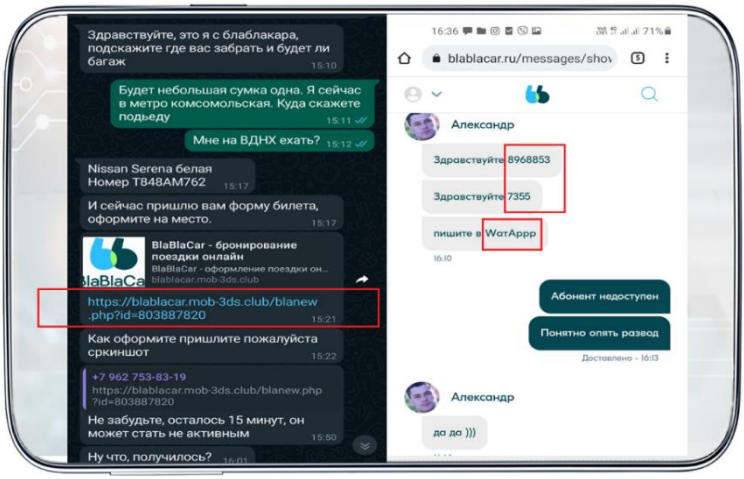
При этом всё сказанное выше вовсе не означает, что ваша переписка в мессенджере абсолютно защищена – вовсе нет, просто эти возможности мессенджеров в сочетании со специальным ПО, которое используют мошенники, и которого нет в свободном доступе, позволяют им работать более эффективно.

Это всегда необходимо иметь ввиду, и если вы видите, что незнакомый человек вдруг предлагает перевести общение в мессенджер и начинает вам писать уже там, то с большой степенью вероятности можно предположить, что это мошенник.

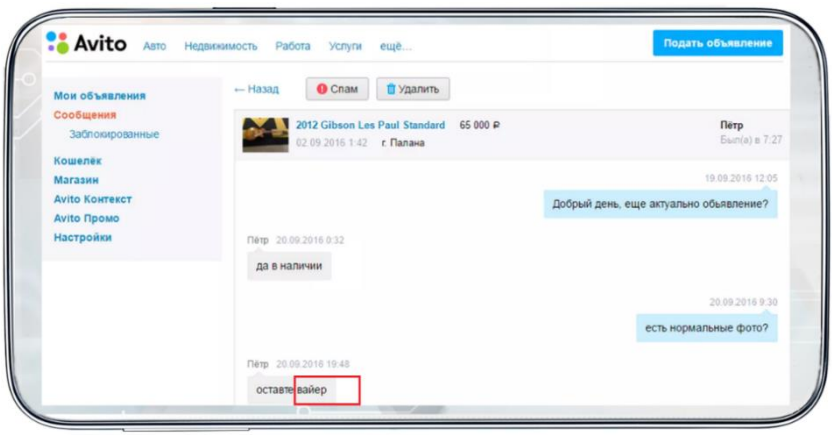
Особенно это актуально на таких сервисах как «Авито» или «БлаБлаКар». Запомните, что любые платформы, где имеются в открытом доступе какие-либо номера телефонов или какие-либо объявления, всегда становятся благодатным полем для действий мошенников.

На скрине пример того, как это происходит на сервисе БлаБлаКар, на котором каждый день создаётся огромное количество аккаунтов мошенников, предлагающих поездки в разные города. Как только клиент выбирает поездку, мошенник тут же предлагает продолжить общение в мессенджере (первый скрин), где он уже действует по отработанной схеме, давая ссылку на мошеннический сайт, в названии которого вначале написано blablacar. Но если

посмотреть внимательно, то ссылка всё же имеет другой вид, и после «blablacar» идет не «.ru», а «.mob-3ds.clu…».



На первом скрине есть ещё один немаловажый нюанс: обратите внимание на то, как мошенник пишет свой номер телефона. Он разделяет его на 2 части для того, чтобы система сайта по защите от подобных мошеннических сообщений его не заблокировала. Заметьте, как в его сообщении написано слово WhatsApp. Это сделано по тем же соображениям, так что всегда заостряйте внимание и на такие существенные мелочи. Аналогичный пример приведён на следующем скрине: обратите внимание, как мошенник пишет слово «Вайбер».



Что касается сервиса БлаБлаКар, то он с таким беспределом борется крайне неэффективно, если вообще борется, и вы можете в любой момент в этом убедиться, пытаясь найти поездку. Почти половина аккаунтов будут без истории поездок, и это на 90% и есть те самые мошенники.

6). Запись голоса, сбор биометрии. К сожалению, в последнее время кроме сбора ваших обычных персональных данных мошенники собирают и биометрические, – например, голос. Он им нужен для того, чтобы потом попытаться от вашего лица пройти процедуру идентификации в банке. Для этого им нужен образец вашего голоса, особенно ключевые слова, произнесенные вами. Например, такие, как фамилия, имя, отчество и слово «да». Звонившие могут представляться кем угодно, поэтому старайтесь не вступать с неизвестными людьми в ненужные разговоры, и если по телефону просят произнести ваши фамилию, имя и отчество, то это практически наверняка мошенники.

Интернет-мошенники.

У них очень много схожих черт с мошенниками телефонными, но имеется и ряд отличий. Все виды интернет-мошенничества мы разобрать не сможем, поскольку их очень много, к тому же каждый день появляется что-то новое, – поэтому рассмотрим общие принципы.

Основные моменты совпадают с теми, которые мы разбирали в прошлой главе. В Интернете происходит всё то же самое, только вместо звонков вам приходят сообщения, которые вы получаете не только в соцсетях, но и на всех ресурсах, где есть возможность общения. Особенно это касается компьютерных игр. По аналогии с предыдущим разделом разберем **основные приёмы интернет-мошенников.**

1). Привет! Hi! Если вам пришло такое сообщение – неважно, где и от кого, – то это практически 100% сообщение-крючок. Его мошенники рассылают всем пользователям и, как бы забрасывая крючок, смотрят, кто и как на него клюнет, а также проверяют,

активен аккаунт или нет (если сообщение прочитано, значит, активен). Если вы ответили, значит, с вами будут работать дальше, т.е. раскручивать вас на нужный им сценарий. Если вы не ответили, то на этом в 99% случаев всё и закончится. Мошенники не будут тратить время на тех, кто не отвечает.

Так что первое правило такое: никогда не отвечайте на те сообщения, которые составлены по формуле – подойдут для каждого. Это почти всегда мошенники или манипуляторы, о которых поговорим в следующей главе.

Сами аккаунты, с которых приходят такие сообщения, могут выглядеть как угодно. Они, как правило, пустые, или полупустые. Их создают специально с целью рассылки спама, и в них чаще всего ничего кроме фотографии нет, хотя имеются нюансы. Например, если вы подросток, то вам, скорее всего, будет писать красивая девушка, а если вы девушка, то вам будет писать мошенник с красивым парнем на аватарке. Для чего это делается, и в чем тут манипуляция, думаю объяснять не надо.

2). Выгодное предложение! Оно не просто выгодное, а очень выгодное! К тому же не абы какое, а полностью совпадающее с вашими интересами. Вам предлагают не какой-нибудь условный Гербалайф, а именно то, что вы давно искали и сильно хотели, да еще и за полцены! Как такое возможно?

В отличие от телефонных мошенников, которые, как правило, работают «по площадям» и шлют всем примерно одно и то же, в Интернете всё гораздо сложнее, и манипуляторы действуют куда изощрённее. Каждую неделю мы в новостях читаем сообщения о том, что в сеть слита очередная база какого-нибудь крупного онлайн-сервиса или интернет-магазина.

Вы когда-нибудь задавались вопросом, кому и зачем нужны эти базы? Они нужны в первую очередь интернет-мошенникам, которые ими активно пользуются. Ведь эти базы содержат уникальные данные о каждом человеке, которые по отдельности, возможно, и не так ценны, но объединенные воедино, вкупе с данными соцсетей, которые мы публикуем о себе сами, позволяют составить на каждого человека его максимально точный психологический портрет. Причем делают это не люди, а программы, которые на основе

таких данных могут слать каждому пользователю индивидуальные сообщения, учитывающие его психотип и потребности, и подходящие именно для него.

Кроме того, бродя по Интернету, мы всегда оставляем за собой цифровые следы, и все наши действия так или иначе фиксируются различными системами, причем чаще всего без нашего на то согласия. Все ваши поисковые запросы, все просмотренные вами товары в интернет-магазинах, товары, добавленные в корзину, но не купленные, – вся эта информация представляет из себя реальную коммерческую ценность, и она, естественно, собирается и перепродается. Все крупные сайты давно собирают о нас всю информацию, и делают они это не просто так.

Информация с данными пользователей подлежит обмену и продаже на специальных биржах, где ее покупают рекламщики, чтобы потом перепродать подороже. Поэтому когда вы поговорили о чём-то с другом, а через час увидели рекламу этого товара у себя в соцсетях – не удивляйтесь, это не чудо и не совпадение. Просто одно из приложений вашего телефона вас в очередной раз монетизировало, продав информацию о вас какой-нибудь рекламной фирме на интернет-аукционе в автоматическом режиме. Это происходит автоматически, через приложения, которым вы разрешили доступ к микрофону вашего телефона, когда их устанавливали. Но даже если и не разрешали, то вы же не можете это никак реально проверить…

Многие приложения при установке требуют дать им разрешение на доступ к вашей телефонной книге, файлам, фотографиям и т. д. Бесплатному приложению они нужны для заработка путём получения и перепродажи ваших персональных данных. Есть классический пример бесплатного приложения «Фонарик», которому, вполне очевидно, для функционирования никаких разрешений не требуется, но, тем не менее, для установки оно требует разрешение на доступ к звонкам и адресной книге.

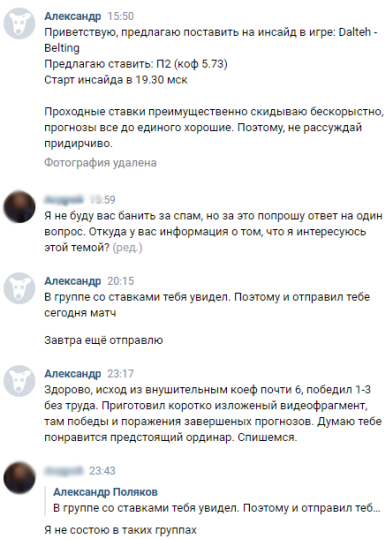
Кроме того, на основании списка контактов, беспроводных сетей, Bluetooth-устройств в зоне видимости пользователя можно делать выводы о его ближайшем окружении, примерном уровне дохода,

семейном положении. Проще говоря, чем более интенсивно используется устройство, тем больше данных о своём владельце оно накапливает.

Человек в Интернете давно стал товаром, вернее, даже не он сам, а его потребности и желания, чаще всего сформированные там же и этими же платформами совершенно сознательно. Как говорят знающие люди: «***Если вы в Интернете пользуетесь чем-то бесплатно, значит товар – это вы***».

Но вернемся к нашим мошенникам. Теперь вы понимаете, откуда у них могут быть такие точные данные о ваших желаниях и потребностях? Им даже необязательно их воровать – они могут их приобрести за копейки вполне легально под видом рекламщиков, чтобы потом использовать эту информацию против вас. Такую информацию открыто продают даже сотовые операторы и социальные сети, предлагая заказчикам (которыми могут быть мошенники) рекламные кампании, нацеленные на узкие группы пользователей.

Конкретный пример: такие сообщения от мошенников стали мне приходить сразу же после того, как я начал собирать в соцсетях информацию на тему нелегальных букмекерских контор, зарабатывающих на ставках. Эту тему мы более подробно разберем в главе о компьютерных играх.


Александр 15:50
Приветствую, предлагаю поставить на инсайд в игре: Dalteh - Belting
Предлагаю ставить: П2 (коф 5.73)
Старт инсайда в 19.30 мск

Проходные ставки преимущественно скидываю бескорыстно, прогнозы все до единого хорошие. Поэтому, не рассуждай придирчиво.
Фотография удалена

59
Я не буду вас банить за спам, но за это попрошу ответ на один вопрос. Откуда у вас информация о том, что я интересуюсь этой темой? (ред.)

Александр 20:15
В группе со ставками тебя увидел. Поэтому и отправил тебе сегодня матч

Завтра ещё отправлю

Александр 23:17
Здорово, исход из внушительным коеф почти 6, победил 1-3 без труда. Приготовил коротко изложеный видеофрагмент, там победы и поражения завершеных прогнозов. Думаю тебе понравится предстоящий ординар. Спишемся.

23:43
Александр Поляков
В группе со ставками тебя увидел. Поэтому и отправил теб...

Я не состою в таких группах

Поэтому любое сверхвыгодное коммерческое предложение вас должно как минимум насторожить. Если вы видите, что в Интернете кто-то предлагает вам именно то, что нужно вам, да еще и с хорошей скидкой – это серьёзный повод насторожиться!

3). Мы – суперкрутая фирма, и предлагаем персонально вам сверхвыгодную работу! (бизнес, товар, услугу). Вам надо только немного вложиться и заплатить нам за наши мелкие расходы…

Это, можно сказать, «классика» интернет-мошенников. Схема строится в первую очередь на алчности жертвы и её желании заработать быстро и много, по возможности при этом ничего не делая (а именно это, как правило, и предлагают).

Подобных продавцов вашего светлого будущего обычно называют «инфоцыгане». Схем «быстрого заработка» они предлагают великое множество, это может быть перепродажа криптовалюты, биржевые торги, инвестиции и прочие мутные схемы, которые обычному человеку без специальных знаний невозможно перепроверить.

Тут важно понять и запомнить простой принцип: любое предложение заработать что-то, сначала «немного» в это вложившись, – это даже не 100%, а 1000% мошенничество. Здесь в принципе не может быть других вариантов. Видов такого мошенничества очень

много. Вам, например, обещают оформить какие-то якобы положенные вам гигантские выплаты, компенсации, или еще что-то сверхвыгодное, но за это просят небольшую (или большую) сумму на оплату услуг юриста. Это – 100% развод.

Ещё вариант. Человек, сидя в крутом автомобиле, весь в золоте и с пачками купюр, показывает вам на телефоне свой счет (авто не его, золото не настоящее, купюры распечатаны на принтере, скрины счетов сделаны в фотошопе) и рассказывает, как можно легко и не напрягаясь заработать миллион. Для этого вам надо всего лишь купить его курс….

Поймите простую вещь: если человек на самом деле как-то смог заработать миллион, то первое, что он сделает, – пойдет зарабатывать второй миллион. И он совершенно точно не будет никого этому учить, наоборот, он сделает всё для того, чтобы про это узнало как можно меньше людей.

Это, вроде бы, очевидные вещи, но, тем не менее, довольно много людей ведутся на такую красивую картинку и отдают последнее подобным мошенникам. Так что смело посылайте лесом всех «бизнес-учителей» и «успешных инвесторов»: всё, что им от вас нужно – ваши деньги.

Приведем еще несколько примеров фраз-заманух, используемых мошенниками: «**Заработай от 100.000 не выходя из дома»! «Выйди на доход 200.000 рублей в месяц, не выходя из дома, уделяя работе 3 часа в день»! «Получи пассивный доход от 20.000 в день»! «Начал использовать этот метод и приобрел финансовую независимость за 2 недели»!** – вариаций таких фраз, напоминающих фразы Емели из сказки «По щучьему велению», вы можете встретить очень много. Подобные объявления мошенников играют на человеческой глупости, жадности и извечной верой людей в «халяву», которой, как показывает жизнь, не бывает.

Заметим, что в соцсетях такие объявления будут более адресными. Например, ВК позволяет рекламщикам делать рассылки в ленту пользователям индивидуальной рекламы, в тексте которой будут учитываться ваши интересы, возраст и место жительства.

Например, если вам 22 года, вы студент и живете в Ярославле, то реклама этих манипуляторов у вас в ленте будет выглядеть примерно следующим образом – фотография хорошо одетого парня (или девушки) возле дорогой машины с пачками денег в обеих руках и подпись: «Ищу молодого человека от 22 лет в Ярославле, можно студента на подработку, для совместного бизнеса (пассивного заработка, легкой работы по 3 часа в день, приносящей 200.000 в месяц и т.д.)». Основа соцсетей – таргетинговая реклама, именно для этого они хотят знать о вас всё, чтобы потом продать информацию всем желающим, в том числе таким мошенникам.

Когда же вы поймёте, что отдали им свои деньги безвозвратно и навсегда, вернуть назад вы их уже не сможете. Ведь вы им отдали их добровольно, позарившись на легкий заработок, так что в данном случае закон будет, к сожалению, на стороне мошенников.

Поддельные интернет магазины.

Ещё один крайне распространенный вид мошенничества – это создание поддельных интернет-магазинов, которые выглядят практически один в один как настоящие. Очень часто они мимикрируют под известные бренды, копируя у них не только название, но и дизайн. Хотя это могут быть и отдельные, независимые магазины с собственными названиями.

Объединяет их один нюанс: стоит вам ввести на их сайтах данные своей карты, как вы тут же потеряете все деньги. Как вы понимаете, не случайно, пункт «интернет-магазины» идет сразу же после пункта «выгодное предложение», ведь это практически всегда напрямую связанные вещи, и «уникальное предложение» вам делают именно для того, чтобы потом перевести вас в такой поддельный интернет-магазин.

Рекламу такого поддельного магазина вы можете встретить абсолютно в любом месте Интернета. Ссылки на них распространяются не только в виде личных сообщений, но и в качестве контекстной рекламы, всплывающей в отдельных окнах практически на всех сайтах. Эта реклама, как правило, всегда таргетирована, то есть подстроена под ваш цифровой профиль, так что вероятность увидеть в ней что-то привлекательное именно для вас крайне велика.

Как отличить мошеннический «интернет-магазин» от настоящего? Есть несколько способов, и все они довольно просты.

Цены. Скидка до 90% – это повод насторожиться. Сравните, сколько аналогичный товар стоит в других магазинах. Сегодня цены в разных магазинах не сильно отличаются, и если вы видите безумно большую скидку на товар, который есть во всех других магазинах, то, скорее всего, это сайт-подделка. Настоящие магазины не занимаются благотворительностью, и никогда не будут продавать вам свой товар с такой безумной скидкой.

Не реагируйте на такие фразы, как «**срочная распродажа остатков»! «таможенный конфискат»! «срочно освобождаем склад»!** Подобные обращения всегда нацелены на то, чтобы оправдать нереально заниженные цены в поддельном интернет-магазине, чтобы вы клюнули на их приманку, воспользовались «выгодным предложением» и ввели на их сайте реквизиты своей карты.

Сайт не имеет протокол HTTPS. Все серьёзные сайты продаж работают только через протокол HTTPS (адрес сайта имеет вид **https**://САЙТ). Если интернет-магазин работает через HTTP, лучше пройти мимо него. Хотя наличие «https» в адресной строке на самом деле не гарантирует безопасность сайта. Это просто протокол шифрования, который можно свободно купить и подключить к любому сайту, что и делают многие мошенники. Так что данный признак не является определяющим. Нельзя сказать, что все интернет-магазины, содержащие https, – настоящие, зато

сказать, что все интернет-магазины, не содержащие https – мошеннические, – можно почти уверенно.

Малоизвестный сайт. Если вы нашли нужный товар на малоизвестном сайте, то в первую очередь постарайтесь поискать его же на большом и известном сайте. В небольших интернет-магазинах цены иногда могут быть немного ниже, но если разница в цене составляет несколько сот рублей, то лучше приобрести товар в более надежном месте. Особенно это касается тех случаев, когда магазин требует предоплату. Требование предоплаты не является признаком мошеннического сайта, но, тем не менее, лучше всегда покупки оплачивать только при получении.

Если же вы столкнулись с малоизвестным интернет-магазином и уже решили в нём что-то приобрести, то обязательно проверьте его перед этим. В сети полно сервисов, которые бесплатно выдадут подробный отчет о сайте. Например, тут: https://pr-cy.ru/. У нормального сайта, как правило, имеются страницы в социальных сетях, присутствует индексация в Яндексе и Гугле и т.д.
Заодно проверьте, на кого сайт зарегистрирован и, самое важное, – давно ли он существует в Интернете. Подойдет любой Whois-сервис (https://www.nic.ru/whois/). Если сайт зарегистрирован недавно (тем более несколько дней назад), лучше ему не доверять.
Адресная строка сайта. Чаще всего «выгодное предложение» от мошенников содержит ссылку, похожую на ссылку известного интернет-магазина. Выше был приведён конкретный пример.
Большинство пользователей не обращают на это внимание, а очень зря. Если вы получили предложение от крупного интернет-магазина, то скопируйте название предлагаемого товара и вбейте его в поиск, например, Яндекса, поставив впереди него название магазина, как в приведенном скрине: «озон Xiaomi Redmi Note 9». Поисковик вам в первой строке выдаст легальный интернет-магазин и, увидев там цену, вы скорее всего убедитесь в том, что вас только что хотели обмануть.

Фишинговые ссылки. Опасные приложения.

Еще один крайне распространенный вид мошенничества – фишинг (от английского fishing – «рыбная ловля»). Это кража данных вашей карты, паролей и всего прочего, что может представлять интерес для мошенников путём установки на ваше устройство вредоносных фишинговых программ. Установка такой программы происходит, как правило, в фоновом режиме и незаметно для вас.

Вирус, содержащий такую скрытую программу-установщика, может быть в письме, пришедшем вам по почте, в ссылке по которой вам предложил пройти анонимный «друг» в чате, в скачанном «полезном приложении», в присланном архиве с чем-то полезным и даже в официальном приложении, – например, в какой-нибудь сомнительной игре с Гугл плей маркета.

Существует бесчисленное количество способов доставить вам на компьютер или смартфон такую вредоносную программу, которая может не только красть нужные ей данные, но и собирать о вас всю информацию. Поэтому никогда не переходите ни по каким ссылкам, присланным вам по СМС, и никогда не устанавливайте никаких приложений, предлагаемых неизвестными людьми. Имейте в виду, что «друзья» в чате или игре тоже к ним относятся. Если вы в сети с кем-то очень давно общаетесь, то это вовсе не значит, что вы его знаете и что вы можете ему доверять. Подробно эту проблему мы разберем в главе «Манипуляторы».

Но даже если вам присылает какой-то файл друг, которого вы знаете, всё равно не стоит его открывать, потому что ваш знакомый человек может сам не знать о существовании таких угроз и по незнанию начать распространять подобный вирус.

Приложения

Всем пользователям смартфонов системы Андройд хорошо знаком сервис Гугл плей, и все мы знаем, насколько много там интересных приложений, вот только мало кто задумывается над их безопасностью. Важно понимать, что сервис Гугл плей сам по себе базово небезопасный. Он служит площадкой для производителей

различных приложений, но при этом он не занимается их анализом и проверкой на безопасность.

Что же касается приложений, устанавливаемых вне этого сервиса с каких-то других сайтов, то здесь риски повышается многократно, и лучше этого вообще никогда не делать. Да, Гугл плей ненадежен, и он не несет ответственности за те приложения, которые на нём есть, но он, по крайней мере, удаляет те приложения, на которые жалуются пользователи.

Хотя, как правило, приложения сделаны так, что пользователи не замечают подвоха. Например экранную клавиатуру для Android Ai.type скачали более 40 миллионов раз, а осенью 2019 года оказалось, что это троян, ворующий деньги владельцев смартфонов.

Периодически проверяйте, какие разрешения требуют ваши приложения. Если, к примеру, установленная вами игра требует доступ к вашей геолокации, телефонной книге и прочим не относящимся к ней функциям, то их следует отключить, а еще лучше – удалить приложение. Многие условно бесплатные игры служат ширмой для сбора и перепродажи ваших данных.

Кроме того, есть категории приложений, которыми лучше в принципе не пользоваться. В первую очередь это приложения «улучшатели», якобы расширяющие функционал популярных программ – «дополнения» (или «аддоны») для WhatsApp, Instagram, Minecraft и т.д.

Все эти приложения для своей работы требуют вход через них в ваш аккаунт, и тем самым вы частично передаёте им его в управление. Можно ли быть уверенным в том, что они этим не воспользуются в корыстных целях? Конечно нет, тем более при установке вы с этим соглашаетесь, давая им разрешения.

Игра Minecraft – общеизвестный чемпион по вирусам среди дополнений в категории «Игры». А многочисленные инструменты для накрутки аккаунтов в Instagram – чемпионы по встроенным вирусам среди мобильных приложений для коммуникаций.

Ну, и если вам предлагают что-то установить для того, чтобы скачать свежий фильм, игру или приложение, то, скорее всего, это вредоносное ПО. Общий принцип такой: если вам предлагают скачать какую-то программу или приложение, которое может делать

что-то запрещённое, даёт накрутку или какие-то другие преимущества вроде игрового читерства, то в большинстве случаев в ней будет вирус, который вы не увидите.

Важно понимать, что само по себе **наличие на компьютере антивируса не дает полной защиты от вирусов**. Антивирус может защитить вас, например, от автоматической установки вируса при переходе на соответствующий сайт, но если вы сами устанавливаете какую-то вредоносную программу (при этом думаете, что полезную) и даёте ей нужные для её работы разрешения, то тут он вам уже не поможет.

Кроме того, никогда не вставляйте в компьютер найденные где-то на улице флешки, – они могли быть «потеряны» специально и на них, как правило, содержится вредоносное ПО. Никогда не запускайте загрузку MMS, присланного с неизвестного номера, и никогда не открывайте вложенные текстовые файлы и файлы архивов, присланные по почте.

Сайты-казино, ставки на спорт, букмекерские конторы.

Всё, что касается любых видов онлайн-казино, букмекерских контор, ставок на спорт и прочих лотерей с обещаниями волшебных выигрышей, не должно вызывать у вас никаких сомнений в «честности» подобных предложений. Сомнений тут быть не может – всё это столетиями известные способы гарантированного избавления вас от ненужных вам денег. Вы однозначно выйдите с этих ресурсов не просто с пустыми карманами, но, скорее всего, ещё и с долгами.

Всё это старо как мир. Наивные и доверчивые люди, желающие заработать много и сразу, при этом ничего не делая, были и будут всегда, и именно на таких людей подобные заведения всегда были и будут рассчитаны. Меняется только форма, но не содержание. То же самое касается всех лотерей, которые совершенно справедливо называют «налогом на дурака».

Все азартные игры, привлекающие наивных граждан ложной иллюзией легких денег, с появлением цифровых технологий сразу же перекочевали в Интернет, и тут они чувствуют себя еще более вольготно. Более того, работа в Интернете для них более привлекательна, чем работа в «оффлайн».

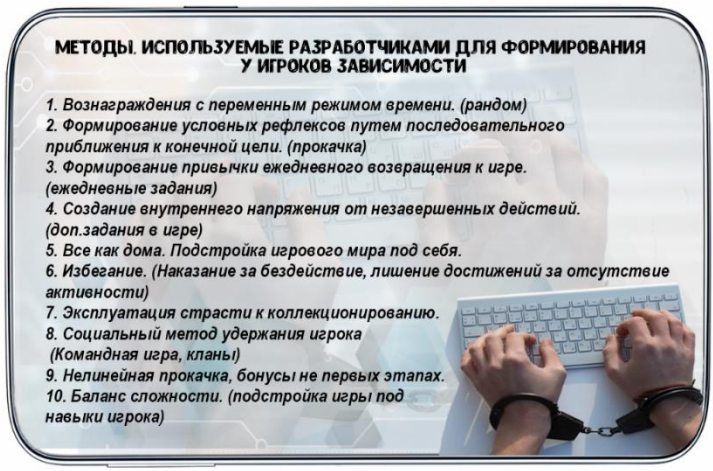
Дело в том, что любая азартная игровая индустрия во всем мире контролируется государствами, над ней стоят множество проверяющих комиссий, и для нее создаются серьёзные ограничения. В Интернете же всего этого нет, и подобные конторы не ограничены фактически ничем, особенно в России. Например, онлайн казино Azino777 является запрещённым, как и все остальные онлайн казино, но при этом его рекламу во всех уголках Интернета мы видим чуть ли не каждый день. Запомните, что легальных онлайн-казино в России нет и не предвидится. Практически все их организаторы находятся в розыске, а, значит ваши финансовые претензии будут адресованы в пустоту, и никто вам их не удовлетворит.

С официальными бухмекерскими конторами ситуация немного иная, некоторые из них легальны (в России их чуть боле десяти), но это не значит, что шанс в них что-то выиграть сильно больше. Все подобные «сервисы» существуют только ради получения

собственной прибыли, а не ради получения выигрыша игроками, и это важно всегда помнить.

4. КОМПЬЮТЕРНЫЕ ИГРЫ

Технологии казино сейчас активно переходят в индустрию компьютерных игр, многие из которых уже давно стали фактически аналогами казино благодаря агрессивным внутриигровым механикам, заставляющим игроков вносить реальные деньги в игру.



Современные игры сильно изменились. И любая современная компьютерная многопользовательская онлайн-игра – это по факту просто инструмент вымогательства с игроков денег, причём инструмент более наглый и эффективный, чем те же самые игровые автоматы. Задача абсолютно всех разработчиков современных игр довольно простая – подсадить человека на игру, сформировать зависимость и потом заставить игрока платить уже настоящие деньги за некоторые преференции в игре, за какие-то дополнительные возможности или даже просто за дизайн. Подробно эта проблема разобрана в передаче, которая называется «Компьютерные игры и дрессировка людей. Ловушка игр», всем любителям компьютерных игр очень рекомендуем. Выше представлен краткий

список тех приёмов, которые используют разработчики. Все разбирать не будем, рассмотрим только некоторые.

Первый пункт – вознаграждение с переменным режимом времени. Эта технология сейчас одна из основных, и она используется в большинстве современных компьютерных и мобильных игр.

Изобретение этой технологии изначально никак не было связано с темой компьютерных игр. Профессор Фредерик Скиннер в 60-х годах прошлого века занимался изучением поведения живых существ. В своей лаборатории он ставил эксперименты на крысах и хомяках, и доказал, как при помощи внешних стимулов можно контролировать и, что самое важное, программировать нужное экспериментатору поведение.

Один из его самых известных экспериментов назывался «ящик Скинера». В ящик сажался хомяк, в ящике была педаль, при нажатии на которую выпадал корм. На первый взгляд всё просто, хомяки довольно быстро соображали, как это работает, и с удовольствием этим пользовались. Но на самом деле задача заключалась в том, чтобы без применения насилия заставить хомяка жать на этот рычаг постоянно и самозабвенно.

Если выдавать хомяку корм после каждого нажатия, он быстро наестся и потеряет к этому интерес, тоже самое будет, если выдавать его через раз. Если вообще не давать корм, то он перестанет жать этот рычаг еще быстрее.

Оказалось, что лучший способ приучить хомячка постоянно жать на кнопку – выдавать ему корм через случайные промежутки времени. Эксперименты показывают, что при таком подходе хомячок очень быстро начинает давить на эту кнопку как одержимый. И ему уже становится важна не столько еда, столько сам процесс, само предчувствие выигрыша. Вам это ничего не напоминает? Всё как в игровых автоматах, это и называется «вознаграждение с переменным режимом времени».

Сначала этот принцип взяли на вооружение хозяева казино, и именно по такому принципу работают все игровые автоматы. Там тот же самый принцип заложен в формирование зависимости, в них человек подсаживается не столько на сам выигрыш, сколько на его предвкушение.

И теперь этот же принцип случайных вознаграждений переняли все производители компьютерных игр. Именно поэтому в играх вам выпадают бонусы и ценные предметы в случайном порядке. Именно поэтому вам выпадает то хорошая команда, то плохая, причём в первом случае вы можете уйти пить чай и всё равно выиграете, а во втором всё равно проиграете независимо от ваших умений.

В играх это называется «Рандом». Игры, использующие этот принцип, вызывают зависимость по такой же схеме, что и автоматы в казино. Вы не можете остановиться прямо сейчас, потому что очень вероятно, что именно следующее нажатие кнопки принесёт вам удачу. Или следующее за следующим. Или то, которое будет после этого. Постоянное чувство приближающейся, но все время ускользающей награды заставляет игрока жать на кнопку снова и снова.

В своей статье разработчик игр из Microsoft Джон Хопсон убедительно доказывает: разработчики прекрасно понимают, что те предметы, которые они заставляют геймеров собирать, – это те самые куски сухого корма, которые получают хомяки в камере Скиннера.

Формирование условных рефлексов путем последовательного приближения к конечной цели. (прокачка)

Главная коммерческая цель долгой прокачки, которая теперь присутствует в каждой игре, заключается в том, чтобы игрок как можно дольше играл, постепенно приближаясь к своей нарисованной разработчиками цели. Для того чтобы разработчикам удержать человека на привязи, ему надо дать долговременную цель, и

специалисты по созданию цепляющих компьютерных игр начали черпать вдохновение у того же Скинера.

Вернёмся к его несчастным зависимым хомячкам. Он экспериментально установил, что приучать нужно постепенно. Сухой корм нужно выдавать хомячкам неравномерно: пусть сначала кусочки сыплются быстро, но с течением времени скорость их подачи нужно уменьшать. От этого хомячок не станет жать рычаг медленнее, скорее, даже наоборот. То есть корма меньше, а результат такой же.

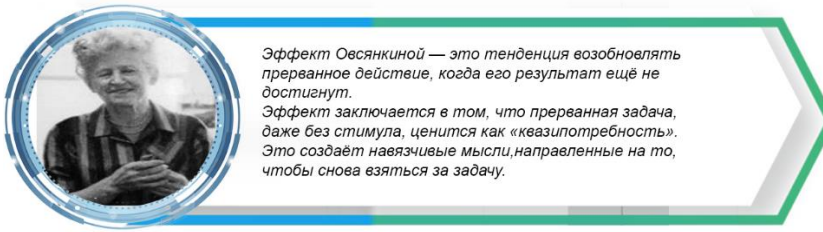
Именно поэтому первые часы любой игры вы прокачиваетесь с чудовищной скоростью, новые уровни достигаются за пару заданий, а предметы сыплются на вас как из рога изобилия. Но с каждым часом, проведённым в игре, количество опыта для следующего уровня требуется всё больше, а, значит нужно тратить больше времени. И это правило работает сейчас во всех играх.

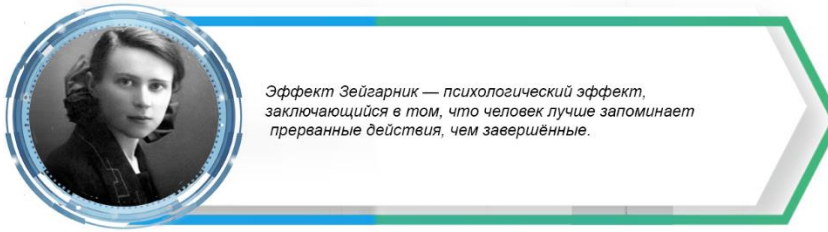
Джон Хопсон, последователь Скинера, выяснил, что человек, подсознательно помня о том, как легко было в начале, получает всё большее удовольствие от достижения новых уровней, и поэтому с каждым новым уровнем геймеры играют всё более фанатично.

Создание внутреннего напряжения от незавершенных действий. Бесполезные задания.

Согласитесь, все, кто играли в современные игры, сталкивались с тем, что в них часто есть масса посторонних заданий, не влияющих на прохождение, второстепенных квестов, каких-то дополнительных миссий или заданий на перепрохождение чего-то.

На самом деле тут разработчики решают сразу 3 задачи. Первая – сделать и без того примитивный сюжет игры немного длиннее, вторая – увеличить время нахождения игрока в игре и третья – создать у игрока внутреннее напряжение от незавершённого действия, чтобы он обязательно вернулся в игру. И тут разработчики снова используют два давно известных психологических эффекта:





На практике оба эти эффекта приводят к тому, что при наличии заряда напряжения от невыполненного задания игрок склонен к нему вернуться. Поэтому в современных играх подобные заряды напряжения не просто умышленно создаются, но и обеспечивается их непрерывная циркуляция. Разработчики ради собственной прибыли эксплуатируют желание игроков выполнить все задания. И ММО-игры разработаны так, что ваш список задач никогда не будет выполнен. Как только вы закончите один квест, вам тут же предложат новый. И так по кругу.
Никакого нового содержания, никакой практической пользы, никаких новых достижений от таких заданий, как правило, нет. Это просто виртуальная беговая дорожка или колесо для хомячка.

Избегание.

Вышеперечисленные методы можно отнести к прянику. Но есть у разработчиков и методы кнута, когда игрока стимулируют выполнять нужные действия не при помощи награды, а за счет избегания наказания, ведь есть ещё один способ заставить хомячка постоянно нажимать на рычаг. Можно за каждое не-нажатие бить его

током, и такие эксперименты тоже ставились Скинером. В ящике Скинера устанавливался такой алгоритм, что если хомячок жмет на рычаг, то его 30 секунд не бьет током. И это тоже работало не хуже, чем метод случайного вознаграждения. Хомяк также не отходил от рычага, и жал на него также самоотверженно.

Как вы думаете, каким образом этот эффект использую разработчики компьютерных игр? Они бы, конечно, с удовольствием сделали так же, как и Скинер, но законодательство пока не позволяет им этого. Хотя с их деньгами не исключено, что когда-нибудь они пролоббируют нужный закон. Но пока им нельзя бить забывших зайти в игру игроков током, они придумали метод немного гуманнее.

Можно забирать у игрока некие его достижения, если он регулярно не посещает игру. Например, в Ultima Online игроки, владеющие замками или домами, должны регулярно посещать их, иначе они начнут разлагаться. А в мобильной ферме грядки зачахнут, если их не поливать. Это относительно дешевая стратегия с точки зрения разработчиков игр, так как им не нужно постоянно предоставлять игроку новые игрушки или награды.

Еще одна тактика, распространённая в ролевых играх: дать пользователю в самом начале почувствовать себя в роли высокоуровневых игроков (чтобы стало понятно, чего здесь можно достичь), а потом все отобрать и вернуть его в самое начало прокачки.

Ежедневные задания.

К методу избегания можно отнести ещё один приём разработчиков, который они используют для того, чтобы игрок заходил в игру каждый день. Это ежедневные задания, за выполнение которых игрок получает бонус, например, двойной опыт за первый бой на каждом танке или что-то подобное. Для разработчиков очень важно, чтобы вы хотя бы один раз в день заходили в игру! Только вы думаете, что на 5 минут выполнить задания. Однако остальное сделают все используемые ими аддитивные технологии, да так, что вы и сами не поймёте, как 5 минут переросли в час ночи.

Эти ежедневные задания можно отнести ещё и к предыдущему пункту, к технологиям избегания, потому что тут они как бы забирают у вас упущенную выгоду. Они как бы говорят: вот тебе ежедневный бонус, но если не зайдёшь в игру, то ты его не получишь.

Кланы, командная игра, социальная составляющая.

Все современные игры крайне активно поощряют создание кланов, команд и прочих объединений игроков, потому что это крайне эффективное для производителей средство удержания игрока. Ведь если игрок состоит в каком-нибудь клане, то он будет входить в игру лишний раз, даже тогда, когда он этого и не хочет, просто чтобы не подвести свою команду и поучаствовать в какой-нибудь бесполезной тренировке. Ещё кланы способствуют тому, чтобы игроки покупали платную экипировку ради соответствия стилю клана.

Надо сказать, что социальный метод удержания игроков – это вообще мощнейший инструмент, который используется сегодня практически во всех играх. Разработчики знают, что выход из среды, в которой люди не просто общаются, а взаимодействуют друг с другом, связан со стрессом.

Мысль о расставании с друзьями-соклановцами в случае ухода из проекта служит тем самым барьером, который мешает перестать играть даже тогда, когда игрок понимает, что игра однообразна, откровенно высасывает деньги и перестала быть интересной. И пока попавшиеся в эти сети геймеры ходят по этому замкнутому кругу, разработчики благодаря только одному социальному элементу повышают средний заработок, который идёт им с каждого пользователя.

Конечно же, мы указали лишь некоторые приемы, используемые разработчиками. Про все игровые механики рассказывать слишком долго, да и книга всё же не про игры. Но в конце этой темы нельзя не сказать о, пожалуй, самой жадной и бесчеловечной игровой механике, используемой производителями.

Лутбоксы.

С 2017 года мировая общественность обсуждает игровую механику, известную как лутбокс. Она представляет собой виртуальный ящик, который игрок покупает за реальные деньги. Лутбокс содержит какой-нибудь игровой предмет, который может быть как чем-то ценным, так и откровенным барахлом. Естественно, узнать наперёд, что именно выпадет, невозможно. По сути, эта игровая механика полностью соответствует механике азартных игр и казино.

— Когда игрок взаимодействует с сундуком, у него в мозгу возникает азартная зависимость, аддикция. Она на физиологическом уровне заставляет игрока тратить реальные средства, чтобы достичь результата.
— В нашем мозгу существует нейромедиаторы, заставляющие нас переживать определённые эмоции. Чем сильнее эмоции, тем больше в нашу кровь выплёскивается нейромедиаторов. Человек запрограммирован так, что не может сопротивляться действию нейромедиаторов.
Есть три нейромедиатора, которые отвечают за получение удовлетворения от достигнутой цели: дофамин, эндорфин, серотонин.
Все три разработчики эксплуатируют в ходе создания лутбоксов.

Алексей Филатов, преподаватель дисциплины "Монетизация игр" в Высшей школе бизнес-информатики

Покупая лутбокс, вы, по сути, покупаете фишку для «однорукого бандита» (популярный игровой автомат в казино) или лотерейный билет, – разницы абсолютно никакой нет, ведь это та же самая игровая механика. В ней жертва подсаживается не столько на сам выигрыш, сколько на всплеск эмоций от предчувствия выигрыша, которого может и не быть.

Приём с сундуками, в которых неизвестно что лежит, сейчас используют практически все производители игр.

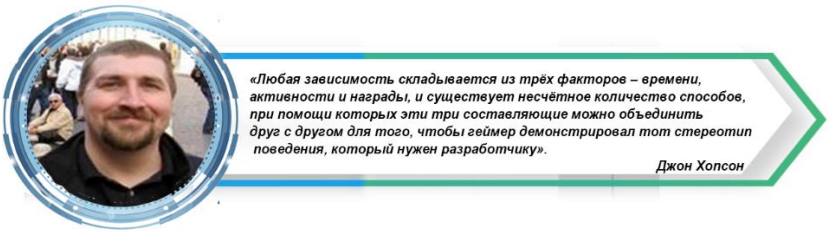
С 2012 года использование лутбоксов ограничено в Японии, с 2017 года они запрещены в Китае – там они совершенно справедливо

приравнены к лотерейным билетам, а в Бельгии и Нидерландах они приравнены к азартным играм.

Мы, к сожалению, в этом плане сильно отстаём, и у нас они до сих пор не запрещены. Более того, как пишет «Форбс», Россия входит в первую пятёрку стран по объёму **потребления** игрового контента. Проще говоря, мы находимся в пятёрке мировых лидеров по количеству обманутых и обобранных подобными азартными игровыми механиками игроков.

Сейчас производители активно внедряют лутбоксы везде, где только можно, многие игры уже делаются так, что без покупки этих лутбоксов на определённом этапе возникают большие проблемы. В некоторых играх, например в таких как «Бравл Старс» лутбоксы даже участвуют непосредственно в процессе прокачки персонажей, и тем самым создают так называемую стену оплаты. Пока не заплатишь – не пройдёшь.
Игра «Бравл Старс» – хороший пример жадности и беспринципности производителей игр. Задумайтесь, это ведь бесплатная игра! Но при этом бесплатная игра зарабатывает каждый год по полмиллиарда долларов. За счёт чего? Как раз за счёт всех этих манипулятивных технологий, и в первую очередь благодаря лутбоксам.

Перечисленные технологии, используемые в играх и вызывающие от них зависимость, – это не какая-то теория заговора, это вполне конкретные вещи, довольно давно известные и подробно описанные. Например, Джон Хопсон много лет работал в Microsoft, и его работа заключалась в том, чтобы заставлять людей как можно больше времени проводить в игре, независимо от того, нравится им это или нет. Делал он это профессионально – он защитил кандидатскую диссертацию по данной теме. Вот цитата из его статьи, которая называется «Поведенческий игровой дизайн», содержащая его знаменитую фразу:



Обратите внимание, что в приведенной цитате ни разу не встретились слова вроде «удовольствие» или «развлечение». Эти понятия не интересуют разработчиков игр. Для них важен только определённый стереотип поведения, который они формируют у игроков.

Сайты-казино в игровой индустрии. Мошенники.

Еще одни акулы, крутящиеся вокруг всей этой сверхденежной игровой индустрии, – это букмекерские конторы, ставки на спорт и онлайн-казино. Но теперь речь пойдёт не про те сайты, о которых мы говорили в прошлой главе. Обращаем ваше внимание на то, что все эти так называемые «сервисы» берут в качестве ставок заработанные или купленные игроками за реальные деньги игровые предметы. Работают они по тому же принципу казино, что мы разбирали чуть выше.

В середине сентября 2018 года 15 ведущих стран, включая Австрию, Чехию и Испанию, создали специальный альянс, который решил привлечь внимание разработчиков к проблеме сайтов-казино, где дети и взрослые ставят на кон игровые предметы.

Следовательно, об этой проблеме знают, и там ею занимаются. Во многих странах те же самые лутбоксы давно запрещены, и игроиндустрия выполняет требования этих стран, удаляя в национальных версиях своих игр такую возможность подзаработать. Россия же, как обычно, находится в числе тех стран, которые вообще не у дел, и подобные «сервисы» у нас работают в больших количествах, постоянно завлекая к себе новых жертв через навязчивую рекламу и недобросовестных блогеров.

Они же часто продвигают различные площадки по продаже и обмену внутриигровых предметов, абсолютное большинство из которых также нелегальны. Нужно чётко понимать, что сам по себе такой формат торговли и обмена вашими игровыми предметами **вне той игры (!)**, в которой они существуют, категорически не приветствуется всеми производителями игр, и в случае выявления ими таких действий ваш аккаунт будет навсегда заблокирован. Данное условие прописано практически во всех пользовательских соглашениях игр. Да, это тот самый текст, который вам показывают при первой установке игры, который вы никогда не читаете, но ставите галочку «согласен».

Кроме того, сами платформы по обмену или осуществлению ставок игровыми предметами всегда требуют ваш логин-пароль от игры, который может быть запросто ими украден, и тогда вы потеряете всё. Если вы во что-то играете, то никогда не вводите пароль от своей игры ни на каких посторонних ресурсах. Ваш игровой аккаунт представляет из себя вполне материальную ценность, которую можно перепродать, а, значит, он всегда будет интересен злоумышленникам. Вы никогда не задумывались над тем, откуда берётся столько объявлений о продаже аккаунтов? Теперь понимаете, откуда эти аккаунты берутся?

И ещё один вид хищников, обитающих вокруг игровой индустрии, – это мошенники. Примерно такие же, какие вам звонят из службы поддержки банка, только происходит это уже не по телефону, а непосредственно в игре. Сейчас практически в каждой игре есть чаты, и именно там они находят своих жертв. Чаще всего их ловят на «выгодное предложение».

Хорошо, если всё заканчивается потерей аккаунта. Хуже то, что существует много схем, когда мошенники начинают учить детей воровать деньги с карточек родителей и толкают их на прочие преступления. Подобный случай очень хорошо описан в статье «Мой малолетний сын украл 200 тысяч на игры и стримеров».

5. Шантаж. Вымогательство.

Один из самых распространенных видов преступлений в интернете – шантаж. Происходит это, прежде всего, потому что большинство интернет-пользователей крайне беспечно относятся к своей конфиденциальной информации и не задумываются о том, как она может быть использована против них самих. Поэтому первое и главное правило, которое надо помнить каждую минуту нахождения в Интернете – всё, что вы делаете в сети, вы делаете публично. Всё, что вы пересылаете даже одному человеку, даже своему другу в личных сообщениях, завтра может оказаться во всех городских группах на всеобщем доступе (есть реальные примеры, и их очень много). И тут речь идёт даже не о человеческом факторе, а о технических свойствах интернет-среды.
Разберем конкретные примеры.

Шантаж интим-контентом

Основным видом преступлений против подростков, касающихся Интернета, стали уголовные дела, связанные именно с распространением интим-контента. Как это происходит? Есть одна очень распространенная в сети схема, которую вам необходимо знать, чтобы на неё не попасться.
Мальчику, к примеру, начинает писать девочка, или наоборот, и у них завязывается вроде как дружба, причём это только онлайн дружба, в реальной жизни они не видятся. И потом, в один момент эта виртуальная девочка предлагает ему обменяться интимными фото, получив которые, она резко меняет поведение, и переходит

к шантажу. «Переводи деньги, или я твои фото разошлю всем твоим друзьям»…

Понятно, что в этой интимной переписке шантажист отсылает не свои фото, он работает с фейковой страницы и может быть, как правило, не того пола и возраста, как указывал в переписке. Сейчас этим способны заниматься даже боты. Такой вид шантажа может быть осуществлен через любой мессенджер или соцсеть, через любой ресурс, где есть виртуальное общение.

Если такому шантажисту нужны от жертвы только деньги, то это еще полбеды. Страшнее, когда шантажист сажает жертву на крючок и заставляет её регулярно присылать подобный контент, полностью подчиняя ребёнка себе и накапливая на него материал.

Есть и другие варианты начала такого шантажа. Иногда сообщения детям приходят от якобы «детских журналов» или «детских конкурсов красоты», для участия в которых надо «прислать свои фотки разного вида». Был случай, когда ребенку писали якобы продюсеры Моргенштерна. Они сообщили, что ребёнок подходит им для съёмок клипа, он якобы победил в конкурсе, и если он хочет принять участие в этих съёмках, то должен выслать свои фото в полуобнаженном виде… Как только он это сделал, мошенники сразу же переходили к шантажу.

Вариаций подобных схем с каждым годом будет всё больше, поэтому запомните главное правило: никогда и никому, ни при каких обстоятельствах не пересылайте в сети свои интимные фотографии. Более того, никогда их не делайте в принципе: даже просто храня их в телефоне, вы уже попадаете в группу риска. Эти фото, например, могут быть украдены с него шантажистами при помощи тех вредоносных фишинговых программ, о которых мы говорили ранее.

Псевдошантажисты

Отрывок из книги «Цифровая гигиена»*: «Кроме различных вариантов социотехники, втягивающей пользователя в сложные сценарии, основанной на его желании получить много денег, существуют разнообразные схемы вымогательства с запугиванием,*

где крючком служит страх. Наиболее показательный пример последних лет – письмо от «хакера», который якобы взломал ваш компьютер.

Я видел, как ты скачивал порно! Довольно известный современный пример вымогательства – электронное письмо от «хакера» примерно следующего содержания:

«Это твой пароль – XXXXXXX, верно? Откуда я его знаю? Я установил на твой компьютер шпионскую программу и знаю, и вижу через камеру всё, что ты делаешь. Я записал, как ты просматривал очень нехорошее порно! Если не хочешь, чтобы я опубликовал видео с этим порно и твоим лицом (хе-хе-хе) во время его просмотра, перечисли столько-то биткоинов/долларов/рублей на такой-то кошелёк».

Никакого видео у «хакера» нет, а пароль, которым он щеголяет, скорее всего, какой-нибудь временный вариант, который вас попросили придумать и ввести для скачивания чего-то с сетевого диска или пиратского сайта несколько месяцев назад, и который владельцы этой файлопомойки «слили», то есть передали (продали) мошенникам.

Этот пароль ни на что не влияет, не имеет никакого отношения к угрозам вымогателя и к выдуманному «взлому» вашего компьютера. Но письмо кажется достаточно убедительным: пароль-то действительно ваш, вы его вроде бы даже помните.

В 2019 году вымогатели усложнили схему: они предлагают получателю письма убедиться в наличии у «хакера» этого «стыдного» видео, для чего нужно перейти по ссылке в письме, которое содержит фишинговую программу и заражает ваш компьютер.

Подобные письма нужно удалять сразу же, не открывая их и не читая. Это мошенники, и никаких ваших видео у них нет. Но при этом важно понимать, что если на вашем компьютере или ноутбуке не стоит антивирус (нормальный, а не бесплатный!), то злоумышленники на самом деле при желании могут получить доступ к вашей веб-камере через вирусные программы или приложения, которые вы легкомысленно скачали из Интернета. Так что заклеивание камеры на ноутбуке и отключение веб-камеры на

компьютере, пока она не нужна – это не паранойя, а вполне разумное поведение в условия современных реалий.

Еще один вид псевдошантажа бывает связан с угрозами убийств родителей или родственников. Да, к сожалению, и такой вид шантажа иногда встречается. Чаще всего он бывает связан с попаданием жертвы в какую-нибудь суицидальную или сектантскую группу, где с ней под видом друзей работают кураторы. Такие угрозы пишут, как правило, детям младшего или среднего возраста, потому что они в силу возрастных особенностей ещё верят всему на слово, и их легко напугать.

Угрозы могут сопровождаться данными о месте работы родителей или адресом их проживания. Такие данные в наше время очень легко получить, чем шантажисты и пользуются, но дети этого не понимают и начинают думать, что за ними реально следят.

Между тем, не известен ни один случай, когда бы такие анонимные интернет-угрозы убийства родителей или родственников были осуществлены. Зато случаи получения реальных сроков людьми, писавшими подобные угрозы, – предостаточно.

Угроза убийством – крайне серьезное преступление, и если вам угрожают таким образом, то нужно сразу писать заявление в полицию, где без особого труда вычислят анонима, которого гарантированно будут ждать серьезные последствия.

Откуда шантажисты берут материалы?

Выше мы говорим о тех случаях, когда за жертвой кто-то наблюдал без её ведома, и получил таким образом на неё компромат, но чаще всего бывает по-другому. В большинстве случаев жертвы шантажа сами заливают в Интернет или хранят у себя на телефоне (что часто одно и тоже) материалы, которые их компрометируют, и которые потом используют шантажисты.

Не забывайте, что в Интернете давно нет ничего приватного, и всё, что вы в него загружаете, будет там навсегда, вне зависимости от того, удалите вы это потом или нет. Интернет помнит всё, и любую вашу удаленную фотографию можно будет потом легко найти и восстановить через специальные сервисы.

Кроме того, все ваши фотографии, сделанные когда-либо на телефон, в зависимости от настроек могут сразу же дублироваться в облако, причем вы можете об этом и не знать, но любой злоумышленник, взломавший ваш аккаунт, сможет их легко просмотреть.
Что касается мессенджеров, то необходимо всегда помнить, что если вы пересылаете кому-то фотографию, видео или какой-либо другой медиафайл, то он автоматически сохраняется в папке мессенджера на всех телефонах участников группы, и даже если вы его тут же удалите «для всех», то он всё равно останется в этой папке на всех телефонах участников, и удалить они его смогут только вручную, перейдя в эту папку.
Будут ли они это делать? А если их телефоны также будут подвержены атаке? И вот тогда компрометирующие вас фотографии или видео могут также оказаться в руках злоумышленников, которые вас найдут мгновенно через систему распознавания лиц, либо по другим признакам. Поэтому главное правило тут такое – никогда и никому не передавать никаких интимных материалов через мессенджеры. Даже если это тот человек, которому вы доверяете.

Что делать, если вы подверглись шантажу?

Первое, и самое главное правило – никогда не платить вымогателям. Если вы заплатили один раз, то будьте уверены, что заплатите и второй раз, и третий – шантажист никогда не остановится, если поймет, что вы для него стали источником дохода.
Спасти может только обращение за помощью к родителям и заявление в полицию. Иных вариантов нет. Ни в какие заверения шантажиста о том, что после получения нужной суммы всё прекратится, верить нельзя: шантажисты всегда пойдут на второй и последующие круги шантажа, как только убедятся в вашей платежеспособности.
Между тем, статья «шантаж» – это достаточно тяжкая уголовная статья, за которую шантажист практически наверняка получит реальный срок, и найти его для полиции не составит большого труда. А после того, как вымогатель будет найден, он, поверьте, не захочет добавить к своему сроку ещё и статью за разглашение ваших

данных. Для полиции раскрытие подобных дел не представляет особой сложности, просто самонадеянные преступники уверены, что человек будет испытывать такой стыд, что не пойдёт подавать заявление в полицию.

Обычно преступники думают, что «это была просто глупая шутка», а в итоге получают весьма серьезные сроки, так как кроме всего прочего, в случае шантажа интим-контентом закон оценивает подобные действия по ст. 135 и 132 УК РФ – «Развратные или насильственные действия сексуального характера».

Как быть, если компрометирующие вас данные всё же попали в сеть?

Первое – не паниковать, второе – написать в службу поддержки соцсети (или другой платформы) требование об удалении компрометирующих вас материалов. По закону они обязаны это сделать, особенно если вам еще нет 18 лет.

И если вы не популярный блогер и не известный музыкант, то с большой степенью вероятности после удаления ваших данных про них уже на следующий день никто не вспомнит и не будет их искать. А постоянно форсить эту тему шантажист тоже не будет: после публикации для него вы станете завершенным проектом, и он переключится на следующего.

Другое дело, если это знакомый вам человек, действующий из мести, и тогда, как говорилось выше, необходимо обращение в полицию. Поверьте, что там работают профессионалы, и им хватит всего одного разговора для того, чтобы шантажист не только прекратил свои действия, но и собственноручно удалил все материалы.

К тому же не стоит переоценивать значение компрометирующих вас материалов для других пользователей. Вы можете считать это катастрофой и даже начать думать о том, что теперь все только об этом и говорят, но это не так. Память постоянного пользователя соцсетей сравнима с памятью аквариумной рыбки. Мы через тридцать минут забываем информацию, которую читали только что.

Проверьте себя – вы можете назвать любые десять постов, которые читали сегодня? А хотя бы пять? Нет? Но как же так, ведь вы же их прочитали не один десяток!

Современный пользователь настолько привыкает к постоянному и беспрерывному потоку пустой информации, что он уже физически не может её запоминать и держать в голове, так что и ваш компромат, равно как и вас самих, все очень быстро забудут и переключатся на другую тему.

6. МАНИПУЛЯТОРЫ

«Плохо, когда цифровые злоумышленники украли у пользователя пароли или деньги, но гораздо хуже, когда они украли у него мозги», – говорится в книге «Цифровая гигиена».

Кроме мошенников в сети оперирует огромное количество манипуляторов, цели которых отличаются от целей мошенников. Если мошенникам от вас нужны только деньги, то задачи манипуляторов гораздо шире, и основная их цель – установление над вами контроля.

Это могут быть представители деструктивных субкультур, тоталитарных сект, экстремисты, радикалы, продавцы паники или, что чаще всего, – просто психически больные люди, жаждущие общения и власти над другими.

Главная проблема со всеми видами сетевых манипуляторов состоит в том, что они практически всегда входят к вам в доверие под видом друзей. Об их настоящих целях жертва узнает чаще всего тогда, когда бывает уже слишком поздно.

Начинается всё, как правило, с простого знакомства, которое может состояться где угодно. Это может быть игра, группа, чат – любой ресурс, где есть возможность интернет-общения. Общение поначалу идёт чаще всего в мягком и непринужденном русле, вербовщики крайне редко действуют «в лоб».

Руководитель Межрегионального Центра информационной безопасности и судебной экспертизы Н.Ю. Васильева, говоря о типичном механизме вовлечения в экстремистские организации,

указывает, что существует пошаговый способ манипулятивной вербовки, состоящий из 5 этапов.

Для наглядности приведём пример схемы, по которой многие подростки пропадают в тоталитарные секты и экстремистские движения. Знание основных принципов манипуляции поможет оградить вас в будущем от вовлечения в подобные схемы.

1-й этап (работа наводчика). На этом этапе вычисляют потенциальный объект вербовки (грустные статусы в сети, проблемы с родителями, сложности в коллективе) – таким образом определяется жертва.

Проще говоря, манипуляторы смотрят ваш аккаунт и определяют по нему ваши интересы, через которые будут в будущем вами манипулировать и на вас влиять. То же самое касается ваших комментариев. Поэтому кроме того, что ваш аккаунт должен быть закрытым, в нём должно содержаться минимум личной информации (подробно о том, как должен выглядеть ваш аккаунт, разберём в конце).

Кроме личной информации также не стоит публиковать и свои интересы, выставлять напоказ те группы, на которые вы подписаны, так как по списку групп также легко определятся целевая аудитория для манипуляторов. Например, если вы увлекаетесь единоборствами, то вы будете интересны в качестве жертвы для групп оффников и прочих криминальных субкультур, которые потом будут использовать вас в своих целях. Поэтому первый принцип – минимум информации о себе и своих увлечениях.

2-й этап (подготовительная работа мотиватора). С жертвой завязывается знакомство, мотиватор входит в доверие, обсуждает существующие проблемы, указывает на наличие у себя таких же, преувеличивает их. В результате жертва подготовлена.

Это то, о чём мы говорили в начале: вовлекают на самое дно всегда те люди, которых вы будете считать своими лучшими интернет-друзьями. Они вас выслушают, дадут советы, якобы во всем поддержат, а на самом деле они собирают о вас информацию для следующих этапов, чтобы потом более эффективно вами манипулировать.

Для этого онлайн «друзья» создают у жертвы иллюзию того, что в общении именно с ними она получает всё то, чего ей якобы не хватает в реальном мире. Втеревшись в доверие, манипулятор начинает давать «правильные ответы» на важные для неё вопросы. Если ему это удается, и жертва становится от него зависимой, то далее он уже сам меняет темы разговоров и переходит к «перепрошивке» жертвы, к навязыванию ей нужных ему ценностей, идей и убеждений.

Задача всех манипуляторов – внедрить пользователю чуждую ему систему мировоззрений и ценностей и поставить его под свои знамёна как минимум в виртуальном, а часто и в реальном мире.

Сейчас отложите книгу и подумайте, а нет ли среди ваших «друзей» подобных примеров? Вспомните с кем и о чём вы недавно переписывались, кто и что у вас спрашивал, задайте себе вопрос, зачем незнакомый человек потратил на вас столько времени?

3-й этап (идеологическая работа мотиватора). Жертве показывают «выход из ситуации» – это вступление в «прекрасный мир», где «ты значим, где ты нужен, где ты можешь сделать что-то важное, спасти себя и даже всё человечество»; в итоге жертва идеологически обработана.

4-й этап (завершающий). Предложение «уникальной» возможности встретиться с «очень важным человеком».

5-й этап (работа вербовщика). «Мы тебя заметили, мы тебя понимаем, ты уникален, мы ценим твои способности, только ты можешь с этим справиться, мы готовы поручить тебе важное дело».

В третьем, четвёртом и пятом пунктах приведены примеры, больше относящиеся к практике вовлечения в тоталитарные секты и террористические организации, но в общедеструктивных течениях механика вовлечения примерно та же самая, только цели ставятся немного другие (подробно это разберём в следующей главе).

Всё вышеперечисленное сейчас могут выполнять боты, т.е. специально созданные программы, ведущие общение автоматически, без участия человека. Хотелось бы составить инструкцию, как отличить реального человека от бота, но на дворе уже 2022 год, и различить их теперь практически невозможно: современные боты умеют вести диалог, они эмоционально реагируют, соблюдают

разные паузы при ответе на сообщения, записывают голосовые сообщения и даже научились дышать в трубку. Вы можете год общаться с таким ботом и ничего не заподозрить, и это уже реальность!

Количество таких ботов не ограничено ничем, есть даже целые чаты, где большинство участников – боты, профессионально имитирующие человеческое поведение. Естественно, они настроены на работу с жертвами и на выполнение ими определённых целей.

Как уже отмечалось ранее, отличить бота-манипулятора (а других ботов и не бывает) от живого манипулятора сейчас практически невозможно, хотя, по большому счету, это и не нужно. В плане безопасности не имеет большого значения, кто вас обрабатывает – живой человек или программа, – в любом случае, вы уже находитесь в опасности, поэтому разберём признаки, которые могут прямо указывать на то, что с вами уже работают, и что вас хотят использовать в своих целях. Первые 7 признаков взяты из книги «Цифровая гигиена».

- **Настойчивость, назойливость**. Незнакомец чересчур настойчиво хочет установить с вами близкие дружеские отношения, даже в тех случаях, когда вы отвечаете отказом, грубите, игнорируете.
- **Склонность к определенной тематике**. Постоянно советует изучить конкретные материалы одной и той же направленности, некоторые из них присылает сам (книги, видео, аудио, картинки) или советует изучить биографию (либо конкретные инциденты) известных преступников, сумасшедших или самоубийц.
- **Чрезмерное любопытство.** Пытается узнать личную информацию (фамилию, имя, отчество, адрес проживания, место учебы, часто посещаемые места).
- **Присвоение, «приватизация».** Пытается отделить вас от общения с другими, убеждая, что они вас не понимают, и только он видит, насколько вы уникальны.
- **Всезнайство, уверенность.** У него есть ответы на все вопросы, причем эти ответы часто сводятся к одной теме.

- **«Влезание под кожу»**. Регулярно обсуждает, интерпретирует ваши чувства и эмоции, пытается объяснить, что вы сейчас чувствуете.
- **Персонализированные обещания.** Обещает пользу, выгоду именно в той области, которая интересна вам.

К этим признакам мы добавим еще несколько.
- **Настрой против родителей**. Это один из основных и главных приемов, используемых манипуляторами абсолютно всех деструктивных групп и тоталитарных сект. Причина вполне прагматична и очевидна. Для того, чтобы манипуляторам сформировать у вас новые, нужные им связи, небходимо сначала разорвать старые. Кроме того, они прекрасно понимают, что ваши родители – это те люди, которые вас любят больше всего, поэтому они будут вас защищать и не позволят никому вами манипулировать, особенно «друзьям» из Интернета.
Следовательно, первое, что делают все представители деструктивных культов – пытаются маргинализировать в первую очередь ваших родителей именно для того, чтобы они не смогли спасти вас в будущем от их влияния. Для этого манипуляторы часто используют псевдонаучные околопсихологические статьи и ролики, которые ненавязчиво подсовывают жертвам «ради общего ознакомления». Поэтому если вы видите, что ваши новые «друзья» слишком активно обсуждают эту тему и пытаются втянуть в неё, – скорее всего, вы уже находитесь на первых этапах обработки.
- **Многократное повторение, работа группой**. Многократное повторение одних и тех же идей или убеждений прекрасно работает. Это проверено на рекламе, и такой же приём используют манипуляторы. Для этого они создают вокруг жертвы дополнительную сеть из новых «друзей», которые транслируют точно такую же информацию на заданную тему, полностью погружая в неё жертву. Для этих целей часто используются боты.
Если манипуляция происходит в соцсетях, то алгоритмы соцсети сами начинают автоматически помогать манипуляторам окутывать жертву, предлагая ей «нужный» контент.

- Бомбардировка любовью. Притворная забота. Данная методика заключается в излишней заботливости по отношению к новичку со стороны всех членов группы. Это позволяет снять защитные барьеры личности новенького, ослабляет его способность к критике, позволяет выяснить его социальный статус и материальное положение.

Если вы вдруг попадаете в новую для вас группу или беседу, где никого не знаете, и вас тут же со всех сторон начинают окружать заботой и любовью, пытаются вам помочь, узнать, как у вас дела и начинают думать, какую бы ещё пользу вам причинить, то будьте уверены – вы в руках манипуляторов. В обычной жизни люди, к сожалению, так себя не ведут, хотя иногда очень хотелось бы.

- **Унижение и программирование на неполноценность**. Явление, абсолютно противоположенное предыдущему, но, как ни странно, часто идущее сразу же за ним следующим этапом. Делают это те же самые люди, которые только что окружали вас заботой и любовью и пытались причинить вам всю возможную пользу. Это называется «эмоциональные качели».

Членов культа могут эксплуатировать и унижать, внушать чувство неполноценности, лишая веры в собственные силы решать проблемы во «внешнем» мире. Такое программирование приводит к печальным последствиям. Даже покинув культ, пострадавший долгое время не воспринимает его деструктивным и искренне полагает, что сам оказался неполноценной личностью.

Такие эмоциональные качели не проходят без последствий для психики, так что если вы заметили нечто подобное в общении со своими новыми сетевыми «друзьями», то лучший способ уйти из-под их манипуляции – резко разорвать общение без объяснения причин. Блокировка, игнорирование и, желательно, смена аккаунта и номера телефона, если он был где-то назван. Резко и одномоментно, никому из группы ничего не объясняя, это важно! Иначе вы можете столкнуться с шантажом, угрозами и другими неприятными для вас последствиями.

Однако, лучший способ избежать таких неприятностей – изначально их избегать. Существует хороший алгоритм, который вы

должны научиться применять каждый раз, когда начинаете в сети какое-то новое общение.

ПОСТАРАЙТЕСЬ ПРИ КАЖДОМ НОВОМ ИНТЕРНЕТ-ЗНАКОМСТВЕ ЗАДАВАТЬ СЕБЕ ТАКИЕ ВОПРОСЫ:

1. Каковы мои цели общения с этим человеком?
2. Что я хочу получить, поддерживая это общение?
3. Что привело меня к общению с этим человеком?
4. Почему для меня важно общаться с этим человеком или быть членом этого сообщества?
5. Как отнесутся мои друзья, мои родители, мои учителя к этому общению?
6. Приходится ли мне скрывать факт этого общения? Если да, то почему я это скрываю, что именно может вызвать негативную реакцию моих друзей, учителей, родителей, и обоснована ли она?
7. Есть ли в этом общении что-то, что настораживает меня? Есть ли что-то, что создаёт мне проблемы?
8. От чего мне придётся отказаться ради этого общения?
9. Что мне известно об этом человеке или данном сообществе? Почему я верю этой информации?
10. Зачем этому человеку общение со мной? Что он может получить от общения со мной?
11. Что произойдёт, если я прекращу это общение?

7. ОПАСНЫЕ ГРУППЫ. МАНИПУЛЯТИВНЫЕ ДЕСТРУКТИВНЫЕ СООБЩЕСТВА

Деструктивные группы

Всё перечисленное в главе «Манипуляторы» происходит в Интернете в определенных местах, в искусственно созданной деструктивной среде, в группах и сообществах деструктивной направленности. Именно там чаще всего манипуляторы ищут своих жертв. Более того, именно они эти сообщества, как правило, для того и создают.

Основное назначение деструктивных групп – формирование определенной среды, выгодной для манипуляторов. Тут уместно будет привести пример из живой природы, в которой, как в Интернете, тоже есть своя среда, своя флора и фауна.

Если вы в любом уголке мира придёте на болото, то там обязательно будут лягушки, пиявки и змеи. Если вы в любом месте мира окажетесь в пустыне, то там будут скорпионы, ящерицы и вараны. Флора (растительный мир) формирует фауну (животный мир), точно такие же процессы происходят и в Интернете.

Если вы видите «черную» группу с депрессивными картинками и грустными фразами, то в ней стопроцентно будут обитать люди с психическими околосуицидальными расстройствами, психопаты и суицидальные кураторы. Если вы видите группу, в которой присутствует околокриминальная «романтика», то в ней будут обитать наркоторговцы, радикалы и криминальные элементы, ищущие именно в этой среде своих жертв.

Если мы начнём подробно разбирать любую деструктивную группу или субкультуру, то практически всегда найдём в ней чей-то финансовый след. На группах оффников зарабатывают производители брендовой одежды определенных марок, на группах анорексичек – продавцы средств для экстремального похудения, на сообществах, пропагандирующих смену пола, – продавцы гормональных препаратов и т.д.

Есть простой способ понять, что хочет от вас группа. **Что вам показывают, то от вас и хотят.**

Еще подобные группы часто организуют сбор денег на что-то близкое по смыслу к их основной теме. Ауешники (АУЕ – запрещенная в России эктремистская организация) собирали средства якобы на «грев» зоны, оппозиционеры – на помощь «узникам режима», зоозащитники – на корм для животных и т.д. Как вы понимаете, все эти деньги, как правило, уходят не на заявленные цели, а на «нужды» админов данных пабликов. Кроме того, идёт постоянная монетизация за счет показа рекламы в группах.

Что касается околополитических и идеологических групп, то тут принцип тот же, только зарабатывают они не на товарах, а на людях. Любая деструктивная идеологическая группа – это всегда чей-то заработок, в котором главный товар – обработанные на определенную тему подписчики, готовые к нужным для заказчика действиям. Люди, «подогретые» таким образом и транслирующие

нужные идеи, потом перепродаются организаторами этих групп уже более крупным заказчикам.

Большинство участников группы свято уверены, что они в ней, потому что: «*Это наше личное мнение, к которому мы сами пришли на основе объективной информации*». Так думают абсолютно все, любой сектант или представитель радикальных маргинальных меньшинств. Именно так вам скажет каждый из них, и переубедить его вы, скорее всего, уже не сможете.

Практически все эксперты за последние два года отмечают резкий рост числа несовершеннолетних, вовлечённых в деятельность деструктивных сообществ социальных сетей. Почему это происходит и почему именно дети и подростки так привлекательны для манипуляторов всех уровней? Зачем детей массово вовлекают в эти, казалось бы, такие взрослые темы?

Причин несколько, они схожи с теми, что мы называли ранее. При этом все они, как ни странно, не имеют прямого отношения к Интернету и к современным технологиям и, более того, они неизменны уже на протяжении многих веков и даже тысячелетий.

Причины интереса деструктивных групп к детской аудитории:

1). Стремление к справедливости. Это стремление заложено в каждом человеке, но именно в детском и подростковом возрасте оно проявляется максимально. Подросткам свойственно иметь обостренное чувство справедливости, это абсолютно нормально и даже хорошо. Проблема заключается в том, что этим чувством очень легко манипулировать, направляя его в нужную заказчикам сторону, что они и делают.

2). Отсутствие жизненного опыта. Плохое знание истории и некоторых закономерностей жизни общества делает подростков уязвимыми перед даже самыми примитивными, классическими манипуляциями, которые очевидны для взрослых.

3). У детей, в отличие от взрослых, как правило, есть свободное время, которое эти группы будут пытаться монетизировать, вовлекая детей в разную активность, нужную для раскрутки.
4). Базовое доверие к миру. У подростков, в отличие от большинства взрослых, ещё нет привычки ко всему относиться с недоверием. Это неплохо, но это играет на руку манипуляторам.
Теперь перейдем к конкретике. В 2019 году прошёл всероссийский форум «Цифровая гигиена. Молодёжь в сети». Одним из самых содержательных докладов там был доклад Натальи Касперской. Её выступление было основано не на предположениях, а на точных цифрах и на многолетнем анализе социального ландшафта Интернета, составленного профессионалами.
На основе больших данных было установлено, какие доминирующие идеи внедрялись в сознание подростков в последние годы. В 2017 году с российских интернет-страниц в сознание внедрялся посыл – «быть плохим – хорошо». В 2018 году в сети появились такие деструктивные направления, как сатанизм и терроризм, а также идеи обесценивания своей и чужой жизни. В 2019 году эти идеи усугубились, началась пропаганда хаоса и террора. Если в марте 2017 года в подобные сообщества был вовлечен 21% подростков, то в марте 2019 – уже 40% подростков.
Сейчас 2022 год, и эти тенденции не только сохранились: все старые деструктивные направления, даже те, которые не отличались большой агрессией, сейчас мутируют в сторону радикализации, а также появляются новые направления.
Тема деструктивных групп и сообществ очень большая и обширная, и в данной книге мы не будем их перечислять, чтобы лишний раз не рекламировать. Но для того, чтобы вы могли самостоятельно идентифицировать такие группы и направления, мы обозначим некоторые общие признаки, объединяющие подобные группы.
В упомянутом выше докладе Натальи Касперской даются довольно четкие признаки сетевых деструктивных сообществ. В них прививают, навязывают, либо стимулируют у подростков следующие качества:

- инфантильность;
- эгоцентрическую картину мира;
- исполнение любых пожеланий;
- разрушение авторитета родителей;
- разрушение традиционных семейных ценностей;
- навязывание идеи секс-насилия вместо любви;
- обесценивание норм морали;
- инверсию понятий добра и зла;
- симпатию к аморальному поведению;
- приверженность злу;
- склонность к разрушению на всех уровнях бытия;
- готовность к действию по команде извне и т.д.

Если вы видите подобные признаки в тех группах, в которых сейчас состоите, то вы должны понимать, что они на самом деле вас не развлекают – они создают ту среду, которая расчеловечивает пользователей, делает их легко манипулируемыми и склонными к вовлечению в ранее разобранные схемы.

Да, вы можете сказать, что на вас это не действует и, возможно, это на самом деле так, но все люди разные, и то, что не подействовало на вас, подействует на других, а что не подействовало на других, – подействует на вас. Поэтому не становитесь соучастниками формирования той агрессивной среды, которую создают подобные сообщества, ведь ваше участие в этих группах, а также любая ваша активность, ведут к их росту и вовлечению в них новых жертв.

Кроме того, данные группы часто являются первым этапом вовлечения подростков в еще более опасные и радикальные темы, выгодные заказчикам. Пользователей как-бы постепенно приучают к нужным заказчикам темам. Для обозначение этого явления используется понятие **«воронка вовлечения»**. В своем докладе Наталья Касперская так описывает процесс вовлечения детей и подростков в деструктивные сетевые сообщества:

Первый уровень. Сначала это группы широкого охвата, открытые группы по деструктивным темам. Их задача – общее информирование о всех деструктивных направлениях. На первом этапе это происходит, как правило, в лёгкой форме. Сейчас эту роль зачастую выполняют околоюмористические паблики с аморальным юмором.

Второй уровень. Группы для тех, кто «созрел» – группы более узкой тематики, специализирующиеся на каком-то более конкретном направлении. Здесь уже могут появляться условия вступления в группу и требование выполнения заданий.

Третий уровень. Частные группы – «для своих». Определённые задания, субкультура, которой нужно следовать, чтобы быть «своим». Тут организаторы уже начинают выбирать жертв для дальнейшего использования.

Четвертый уровень. Закрытые чаты для приватного общения с «созревшими», где осуществляется подготовка к действиям. Потом идут команды на выполнение действий в реальном мире. За их выполнение могут начисляться бонусы, повышаться статус в группе, раздаваться соответствующие звания, которые, по сути, просто фантики, которые ничего не стоят для организаторов.

Описанный алгоритм – условное разделение. Этапов вовлечения может быть больше, а может и меньше, важно понимать сам принцип, чтобы не попасть в подобные ловушки. Кроме того,

независимо от типа деструктивной группы в «воронках вовлечения» преследуются и реализуются скрытые цели, **жертв буквально дрессируют по следующим пунктам:**
- *снижение способности критически мыслить и принимать взвешенные решения, дрессировка, отбор наиболее внушаемых;*
- *«перепрошивка»: обесценивание традиций, человеческих ценностей, разрушение норм морали, отрицание ответственности и формирование искажённых ценностей, снижение ценности собственной жизни подростка, ценности жизни других людей, ценности жизни общества в целом;*
- *«накрутка»: создание ощущения неблагополучия и опасности объективной реальности, приучение к идее насилия;*
- *формирование стремления к разрушению, полная подготовка к действиям;*
- *дестабилизация социальной и политической жизни общества.*

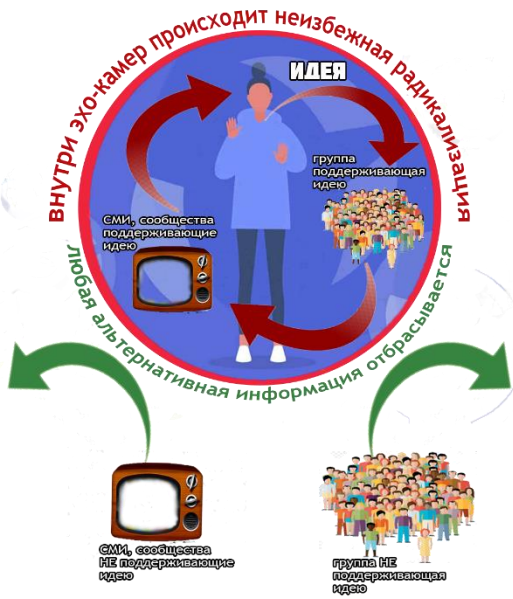
Если вы уже заметили такие признаки в группе или чате, в котором вы состоите, то лучше немедленно его покинуть, не объясняя причин, резко оборвав в нём все контакты.

Семантические капсулы. Эхо-камеры социальных сетей.

Главная цель соцсетей – заработать денег с пользователя за счёт показа ему рекламы, а для этого нужно сделать так, чтобы пользователей было не только много, но и самое важное, чтобы они проводили на платформе как можно больше времени.
А как этого достичь? Необходимо сделать так, чтобы пользователь был с головой вовлечён и погружён в какую-нибудь важную для него тему, причём неважно, интересовался ли он ею до того, как поспал в соцсеть. Если у человека нет никаких интересов, то это не проблема: платформа сама ему их сформирует, мягко предлагая разные варианты.

Вы, наверное, заметили, как последнее время соцсети все чаще стали «подсовывать» вам в ленту информацию с тех групп, на которые вы не подписаны, и как часто они стали вам что-то

предлагать. Это делается именно для того, чтобы вы что-то для себя выбрали, а потом, как только вы отреагируете, алгоритмы тут же это многократно усилят и погрузят вас в так называемую семантическую капсулу, эхо-камеру, информационный кокон, и т.д. У этого явления много названий, но смысл один: соцсети умышленно усиливают влияние любых, в том числе и деструктивных групп через «подсовывание» пользователям похожего контента. В итоге каждый пользователь со временем оказывается в своеобразном информационном узкотематическом коконе, под который уже не попадает никакая другая информация.



Самое интересное, что такие же процессы происходят и внутри самих групп, где полным ходом идёт саморадикализация.

Приведём ещё одну цитату из книги «Цифровая гигиена»: «*Обитатели семантической капсулы большую часть времени проводят внутри своей капсулы, «эхо-камеры», где участники непрерывно рассказывают друг другу одно и то же. Там происходит постоянное повышение концентрации одних и тех же идей, ментальных шаблонов, мемасиков. Участники «просаливаются» ими, как огурцы в банке. Какой бы ты ни был свежий или толстокожий*

огурец, в банке ты станешь соленым. А вот снова стать свежим, скорее всего, уже не получится.

Для повышения концентрации идей и убежденности в них в сообществах смысловых капсул используются простые ментальные шаблоны:

- господствующая моральная высота: *иметь другое мнение абсолютно безнравственно, все люди доброй воли думают одинаково с нами;*

- шкурные мотивы оппонентов*: носитель противоположных мнений всегда негодяй, он куплен нехорошими людьми, кланами, государством, у него шкурные, корыстные причины иметь свои настолько безнравственные мнения;*

- расчеловечивание оппонента*: в крайнем случае человек, высказывающий мнение, отличающееся от правильных, – идиот, быдло, школота, малообразован, неполноценен в том или ином смысле;*

- тем хуже для фактов*: мотивация важнее логики; если цепочка фактов и/или рассуждений приводит к нежелательному результату, противоречащему высшим целям сообщества, значит, все приведенные факты и рассуждения изначально неверны;*

- апофения*: все события в мире подтверждают нашу правоту, в крайнем случае мы просто отказываемся их замечать и обсуждать».*

Если вы обнаружили описанные признаки в тех группах, в которых состоите, то вам следует как минимум задуматься над тем, какую роль вы там играете, куда и зачем вас в них ведут. Практика показывает, что долгое участие в подобных сообществах, как правило, ни к чему хорошему не приводит и, как минимум, наносит вред психике.

Радикализация. Переход обычных групп в разряд деструктивных.

Особенность соцсетей такова, что описанная выше радикализация встречается не только в деструктивных, но и в изначально нейтральных группах. Многие деструктивные явления стали

таковыми не сразу, а именно в процессе их постепенной радикализации. Приведем конкретные примеры.

Группы зоозащитников. Изначально правильная и благая идея помощи беспризорным животным во многих зоозащитных сообществах превратилась в фетиш и в фанатичный культ, в котором жизнь животного – абсолютная и непререкаемая ценность. Она стала важнее всего остального, в том числе и жизни людей. Например, такие радикальные группы «зоозащитников» «совершают набеги» «организованными стаями» в группы охотников, где устраивают массовую травлю всех участников. Сейчас уже дошло до того, что стоит любому охотнику выложить в сеть фото с добычей, как к нему сразу же прибегут активисты с безумными комментариями, с проклятиями и угрозами в его адрес. Таким образом, благая на первых порах идея спасения животных достаточно быстро трансформировалась в идеологию ненависти и травли.

Сообщества феминисток. Изначально заявленная цель движения – защита прав женщин. Если мы говорим про историю феминизма, зародившегося в прошлом веке, то тогда это так и было. Но за последние лет 20 феминистское движение кардинально поменяло свои цели, которые теперь уже не имеют никакого отношения к защите прав женщин. В настоящий момент группы феминисток транслируют безумную, крайне радикализированную и близкую к экстремистской идеологию, в основе которой лежит ненависть. Причем это ненависть не только к мужчинам, но и ко всем несогласным с их идеями.

Как видим, примеров такой саморадикализации движений в сети предостаточно. Поэтому если вы состоите даже во вполне безобидной на первый взгляд группе, декларирующей какие-то правильные вещи, всегда обращайте внимание на то, чем группа готова пожертвовать ради достижения своих целей. Если цена становится всё более высокой, или начинают декларироваться лозунги типа «всё ради достижения цели, невзирая на последствия», или звучат призывы к организованной травле всех несогласных, то такую группу лучше покинуть.

Околосектантские группы.

Кроме реальных людей и ботов, ведущих вербовку и «перепрошивку» своих жертв, в сети есть масса групп и сообществ манипулятивной направленности, стремящихся вовлечь в свою орбиту как можно больше пользователей с целью их последующей монетизации. Это могут быть политические авантюристы, продавцы паники, «открыватели истин», переписыватели истории, сектанты, анархисты, радикалы и прочие подобные им движения и персонажи.

Чтобы не попасть под влияние таких групп, всегда избегайте постов и роликов, содержащих кричащие названия: «Настоящую историю давно переписали!», «От вас это скрывали веками!», «О подлинной истории пишет канал…!», «Только мы расскажем вам правду» и т.д.

Такие группы и каналы, зачастую имеющие околосектантскую или политическую направленность (давно пора вводить термин «политические секты»), ради своего роста и продвижения пытаются ввести пользователя в состояние так называемого «инсайта», то есть озарения или прорыва в мыслительном процессе (в данном случае ложного). То есть они пытаются искусственно, на основе каких-то своих безумных теорий (которые для неподготовленного человека могут показаться вполне логичными) фактически поменять человеку привычную ему картину мира и заставить его воспринимать реальность другим образом, нужным манипулятору.

Человек, подсаженный на предложенную ими альтернативную картину мира, начинает воспринимать только такой контент и становится не только их постоянным подписчиком, но ещё и бесплатным распространителем.

Такая быстрая «перепрошивка» пользователя, оказавшегося в рассматриваемых группах, происходит ещё и потому, что соцсети в силу своего функционирования усиливают любое влияние и создают вокруг каждого пользователя его персональный информационный пузырь. Вы, наверное, замечали, что стоит вам заинтересоваться какой-то темой, как соцсеть тут же создает вокруг вас

карусель из предложенных групп, друзей и роликов заданной направленности.

Так, многим людям помимо их воли настойчиво предлагаются в том числе и эти группы. Они начинают читать все больше подобных материалов, закрепляя для себя эти навязанные кем-то альтернативные точки зрения. Противоположенной информации они уже не получают, отчего становятся ещё более уверенными в своей правоте. Это может прозвучать странно, но фактически соцсети алгоритмизировали принципы тоталитарных сект… Алгоритмы в них выполняют роль «гуру», который даёт только «нужные» знания, замыкает человека на них, постоянно их уплотняет и не допускает никакой альтернативы.

Конечно, вышесказанное вовсе не означает, что нужно избегать в соцсетях любой альтернативной информации – вовсе нет! Просто нужно уметь ее фильтровать. Поэтому никогда не реагируйте на кричащие и всё объясняющие заголовки, обещающие простые ответы на сложные вопросы, «переворачивающие» классические представления о мире. За такими заголовками чаще всего стоят манипуляторы, желающие пополнить ряды своих адептов.

Пропаганда насилия.

Речь идёт не только о пропаганде насилия по отношению к другим людям, но и к себе. Дело в том, что если вы видите подобный контент в своих группах, то это говорит о том, что вы находитесь в зоне интересов не только экстремистов, но и, вероятнее всего, психически нездоровых людей, цели которых могут быть какими угодно. К сожалению, Интернет давно стал излюбленным местом для маньяков, психопатов и психически неуравновешенных людей, жаждущих общения.

Такие люди создают экстремистские и террористические сообщества, привлекающие к себе как соответствующих подписчиков, так и случайных пользователей. Пропаганда насилия, ненависти и наличие шок-контента – ключевые признаки таких групп. И если вы видите группу с таким содержанием и материалами, то они там

размещаются не просто так. Здесь работает всё тот же принцип: **что вам показывают, то от вас и хотят!**

Подобные материалы в группе всегда служат безусловным маркером её манипулятивности и опасности для вас. Единственная ваша возможная роль в данной группе – роль жертвы. Вы будете ею являться даже независимо от того, выйдет ли с вами на связь кто-то из манипуляторов или нет, потому что сам по себе просмотр такого контента крайне негативно сказывается на вашей психике. Его действие подобно радиации – оно проникает незаметно, и видимые последствия наступают, как правило, только тогда, когда уже поздно что-либо предпринять.

Вы можете не знать всех запрещённых экстремистских течений и направлений, поскольку их очень много, и можете даже не догадываться о настоящих целях организаторов таких групп, однако здесь срабатывает всем известный принцип: **незнание закона не освобождает от ответственности**. Поэтому если вы видите, что в группе содержится любой контент, пропагандирующий насилие к себе (самоповреждения) или окружающим, то такую группу стоит немедленно покинуть.

Необходимо также отметить, что подобные группы отслеживаются, и ваше нахождение в любой из них может довольно серьёзно испортить ваше будущее. На базе многих престижных ВУЗов уже сейчас запущены программы, анализирующие сетевое прошлое каждого абитуриента, и если они обнаружат, что вы когда-то состояли в подобной группе, это вполне может стать основанием для отказа вам в поступлении. Как мы выяснили, Интернет помнит всё, и ваше удаление старого аккаунта перед поступлением не решит проблему, поэтому всегда придерживайтесь простого принципа – **берегите свою цифровую честь смолоду!**

Экстремистские группы.

Направлений и видов таких групп с каждым годом становится всё больше. Они могут отличаться по направленности и степени «отмороженности», но в них всегда присутствуют общие черты, которые вам необходимо знать для того, чтобы не попасть под их

обработку. Главный и безусловный признак таких групп – **пропаганда ненависти**. Это та база, вокруг которой строится вся последующая манипуляция. Объектом ненависти может быть государство, народ, этническая группа, политическая партия, социальный строй, социальная группа и т.д. Пропаганда ненависти в подобных группах, как правило, сочетается с взываниями к справедливости (в искажённом понимании этого слова), назначением виноватых (по мнению группы) и призывами (часто завуалированными) к насильственному изменению ситуации.

Решение проблемы всегда предлагается максимально простое и примитивное, рассчитанное на самого необразованного и некомпетентного пользователя. Именно такие подписчики в первую очередь интересуют организаторов этих групп: им гораздо проще внушать «нужные» идеи. По той же причине умные люди, попавшие в такие группы случайно и начинающие задавать ненужные вопросы, моментально банятся, чтобы не спугнуть основную аудиторию.

Объяснения лидеров мнений таких сообществ сводятся к простым правилам: «Делайте то, что мы вам говорим, и это решит все ваши проблемы!» (на которые мы искусственно обратили ваше внимание).

Практически всегда в таких группах присутствует какая-то одна ключевая сверхидея, искусственная сверхценность, на которую активно подсаживают адептов. Это цель, которая ставится во главу угла, и через неё, как через фильтр, протаскивают чуть ли не все мировые события. Подобные технологии также используются в большинстве сект.

Несмотря на кажущуюся сложность, сделать это на самом деле не так уж и трудно, тем более разработкой таких концепций, как правило, занимаются профессионалы. Путём подобных манипуляций они могут перевернуть картину мира практически любого человека в нужную им сторону. Про то, что такое экстремизм, и какая бывает ответственность за распространение экстремистских материалов, мы подробно разберем в отдельной главе.

Почему люди так доверяют всему прочитанному в сети?

Главная ложь Интернета заключается в простом тезисе, в который многие верят, и который вы не раз слышали, а, возможно, даже и сами декларировали. Он звучит примерно так**: СМИ всегда врут, а вот в Интернете только правда, потому что там мнения обычных людей**. Правда, когда так говорят, конкретных «обычных людей» почему-то не называют. Было бы здорово, если бы это соответствовало действительности, но реальность гораздо прагматичнее.

Официальные СМИ подчиняются закону о СМИ, и по нему отвечают за каждое слово, поэтому в случае трансляции новостных фейков они несут серьёзные репутационные и финансовые убытки. Это, конечно, не значит, что они не врут – они делают это по-другому, через нужную им интерпретацию реальных фактов, но не через трансляцию откровенно недостоверной информации.

А вот блогеры, ВК-группы, Ютуб и Телеграм-каналы у нас до сих пор не относятся к СМИ, ввиду чего они транслируют всё, что считают нужным, в том числе и грубые фейки. Существует огромное количество каналов, транслирующих откровенную ложь.

Один из таких каналов – печально известный проект Ютуба «Крамола». В апреле 2020 года на нём был размещен ролик, содержащий заведомо ложные сведения на тему коронавируса. Примечательно в этой истории то, что осужденный руководитель «Крамолы» полностью признал свою вину, честно заявив, что таким образом он пытался повысить количество подписчиков.

Но этот случай, скорее, исключение, так как большинство подобных каналов и групп годами транслируют всё, что угодно и, в отличие от официальных СМИ, не несут за это никакой ответственности. Поэтому именно Интернет стал сейчас основным инструментом, используемым манипуляторами всех мастей и расцветок.

Сами же социальные сети в силу принципов своего функционирования формируют легко манипулируемых и податливых людей, склонных к любому воздействию извне. Особенно явно это воздействие проявляется через такие технологии дрессировки масс,

как флешмобы и челленджи, где люди массово и бездумно повторяют любые действия, вброшенные заказчиками.

Особенно это актуально в Тик-токе, где существует даже официальный прайс для крупных фирм, желающих запустить коммерческий челлендж ради продвижения своих товаров или идей.

Так что если вы видите челлендж, где используется какая-то известная марка или бренд, то будьте уверены: вы увидели его только потому, что заказчик за это заплатил и, участвуя в нём, вы становитесь его бесплатным рекламным агентом. Вам оно надо? Любой флешмоб или челлендж – это всегда манипуляция толпой и выработка у нее инстинкта бездумного повторения. Поэтому еще одно важное правило, которое вам необходимо запомнить ради сохранения своего собственного «я» – **нельзя никогда и ничего делать вместе с толпой!**

Политические манипуляторы. Использование детей в качестве протестной силы.

К сожалению, данная тема с каждым годом становится всё более актуальной. Почему это происходит? По миру за последние несколько лет прокатилось уже несколько так называемых «цветных революций», осуществляемых по одному и тому же сценарию. И в этом сценарии всегда на начальных этапах использовалась технология «онижедети». Суть её заключается в том, чтобы при помощи медиатехнологий любой ценой вывести детей на протест, а далее, при помощи отдельных групп провокаторов, подставить этих детей под дубинки или даже под пули силовиков. Делается это для того, чтобы вызвать у общества максимальную ответную реакцию, при этом сами дети приносятся в жертву целям организаторов без особых сожалений.
Именно эта технология крайне эффективно сработала на Украине в конце 2013 года, когда получила толчком ко всем дальнейшим

военным событиям, чудовищные последствия которых мы можем наблюдать и по сей день.

Вице-президент Российской криминологической ассоциации, доктор философских наук профессор Игорь Сундиев в 2017 году высказал мнение, что Евромайданом и информационными возможностями «новых медиа» была порождена технология использования детей в протестной активности, которую автор обозначил как «линия инфантицида (умышленное лишение жизни ребёнка) — «онижедети». Таким образом, зачастую для политических манипуляторов дети нужны в качестве протестной силы не как участники общественного процесса, а как жертвы, причём в самом прямом смысле этого слова.

В России последний раз попытка осуществления такой технологии была предпринята зимой 2021 года, когда Ютуб и Тик-ток искусственно вывели в топ нужный контент и смогли вывести на улицы тысячи школьников. К счастью, тогда серьезных провокаций удалось избежать.

Далее приведём отрывок из книги «Цифровая гигиена» с **подробным описанием механизмов политической мобилизации несовершеннолетних.**

«Развить в подростке чувство неудовлетворенности и несправедливости довольно просто, следующий шаг – приучить его к «игровому» протесту, в основном в форме сетевой активности. Таким образом подростковую аудиторию можно крайне быстро «натаскать» на протестную деятельность и одновременно приучить к нужной шкале ценностей.

Следующий этап политической мобилизации – перенесение действий в реальность. Для начала речь идет о совершенно безобидных акциях, но в реальной жизни (выйди во двор и включи на телефоне фонарик в знак поддержки; выйди с друзьями на прогулку с цветными ленточками и т.д.). Эти акции сближают, сплачивают, вырабатывают привычку собираться вместе и выполнять заданную программу действий «на улице».

В результате подросток окончательно убеждается, что это весело, это тусовка единомышленников, аналог карнавала с отменой привычных правил, что за свои действия он не понесет

никакого наказания. При этом формируется «игровой» характер политической активности и вырабатывается привычка к участию в массовых акциях.

Таким образом, после нескольких этапов подобной обработки подросток будет морально готов к участию в массовых акциях (в том числе массовых беспорядках). При этом у него формируется ощущение полной безнаказанности в этой «протестной игре». В сети можно писать и делать что угодно, за участие в сетевой протестной активности никак не наказывают.

А в жизни манипуляторы обещают полный иммунитет при участии в митингах, протестах и беспорядках, успокаивая и заверяя их, что детей не сажают и не наказывают, что конечно, неправда».

Самым известным примером является обещание А. Навального отсудить 10.000 евро в пользу каждого задержанного на организованных им протестных митингах 26 марта 2017 года. Подобные обещания очень похожи на обещания наркоторговцев, которые уверяют: «*работайте, вам ничего не будет, у нас всё схвачено*».

Это точно такое же вранье, и технология та же самая. Кстати, меньше, чем через месяц, в апреле 2017 года школьники провели еще одну протестную акцию, но на этот раз уже против самого

Навального, наивно требуя от него обещанные им деньги, которых им, конечно же, никто так и не отдал.

Вообще дети как отдельная категория граждан очень интересны политическим манипуляторам ещё и как бесплатные распространители нужного им материала. Интерес обусловлен тем, что у детей, во-первых, еще нет необходимого жизненного опыта, который бы позволил критически осмыслить вбрасываемые публикации, а, во-вторых, у них есть самое главное – свободное время!
Дети проводят в сети гораздо больше времени, чем взрослые люди, постоянно занятые работой, и поэтому они являются более активными распространителями нужного заказчикам контента. Это известно всем, кто работает с медиа. Профессионалы прекрасно знают, что количество комментариев в поддержку или в осуждение какой-либо темы вовсе не говорит об общественном мнении, потому что основной возраст людей, пишущих комментарии, как правило, достаточно низкий. Соответственно, такое «общественное мнение» никогда не даёт и не давало реального мнения всего общества. Поэтому не сильно надейтесь на то, что ваш комментарий, поддерживающий мнение толпы, может на что-то повлиять.

Как не попасть под обработку таких групп?

1). Всегда во всём сомневайтесь и перепроверяйте любую информацию, какой бы правдоподобной она ни казалась на первый взгляд. Просто имейте такую привычку, и она вас не подведёт.
2). Не поддавайтесь эмоциям – они в данном случае ваш враг! Манипуляции в таких группах всегда основываются на эмоциях. Как только вы видите, что какая-то группа или человек активно пытается вас вывести на эмоцию – отписывайтесь. Вами однозначно пытаются манипулировать. Умение подходить к любой информации с холодной головой – основа выживания в современных интернет-джунглях.
3). Смотрите на лидеров мнений. Они есть у любого направления, как деструктивного, так и позитивного. Если вы видите, что в какой-нибудь субкультуре имеется медиа-лидер, который

транслирует определенные деструктивные идеи или модели поведения, значит, они присущи всей группе. И если вы останетесь в этой смысловой воронке, то эти идеи незаметно для вас самих могут стать вашими. Ничего хорошего это вам не принесёт, поэтому старайтесь избегать просмотра таких материалов.

4). Не позволяйте себя радикализировать! Как только вы видите, что в группе вам пытаются внушить какую-то «сверхценную» идею или усиленно стараются поменять привычную для вас картину мира – отписывайтесь! Любая радикализация начинается с возведения одной отдельно взятой проблемы над всеми остальными. Далее следует её усиление и накрутка вас на нужные заказчику действия.

5). Не позволяйте собой манипулировать. **Никогда и ни при каких обстоятельствах не выполняйте никаких заданий, какими бы безобидными они не казались**. Просто имейте такой железный принцип, не имеющий исключений. То же самое касается всех челленджей и флешмобов. Если вы хотите вырасти здоровой и всесторонне развитой личностью, то вы всегда должны руководствоваться в сети озвученным выше правилом: **нельзя никогда и ничего делать вместе с толпой!** Выполнение этих двух простых правил поможет вам избежать большинства манипуляций.

6). Не пытайтесь «играть в журналиста». Есть масса примеров, когда дети и подростки уходили в такие группы ради развлечения, чтобы посмотреть на то, что там происходит. Некоторые из них теперь находятся в местах заключения, а многих из них уже нет в живых. Запомните главное, что как в обычной жизни, так и в Интернете – есть места, в которые лучше не попадать. Известны случаи, и их немало, когда дети в подобных группах подвергались обработке определенными технологиями, про которые мы почти ничего не знаем. **Жертвы таких манипуляций впадают в тяжелое измененное состояние психики, вывести из которого их бывает зачастую просто невозможно.**

Поэтому всегда старайтесь избегать негативного контента, чтобы не попадать в такие ситуации. В обычной жизни мы всегда стараемся присоединяться только к чему-то хорошему и позитивному и

стараемся окружать себя такими же людьми. Этим же принципам необходимо всегда следовать и в сетевом общении.

Темные места Интернета.

Кроме деструктивных групп и каналов существует масса закрытых ресурсов, привлекающих многих пользователей своей якобы анонимностью, отсутствием правил и полной вседозволенностью в плане наличия запрещенного контента. Многим пользователям сама идея нахождения на таком ресурсе кажется привлекательной, потому что они видят в этом иллюзию безопасности, хотя в реальности дело обстоит с точностью до наоборот.

Приведём простую аналогию. Давайте сравним городской парк какого-нибудь областного центра с пригородом какой-нибудь африканской страны, где нет власти, нет законов и постоянно идёт гражданская война, в которой выживает сильнейший.

Когда вы гуляете по городскому парку, то за вами смотрят сотни камер, ходят сотрудники службы безопасности, из урн вывозят мусор, в нём травят клещей и т.д. Десятки служб незаметно для вас поддерживают в нем базовый уровень вашей безопасности, и именно поэтому вы там можете свободно гулять. В африканском же пригороде всего этого нет. В любой момент на вас могут напасть, ограбить, убить, взять в заложники и т.д. И там не будет никого, кто бы мог вас защитить, потому что не работают законы и отсутствует базовая безопасность.

Естественно, такое положение дел выгодно в первую очередь организаторам подобных банд, которые специально для себя создают такие районы. Делают они это именно для того, чтобы заниматься беспределом, и им очень нужны «исследователи темных мест».

Точно такая же разница между Интернетом и Даркнетом. Даркнет был создан примерно такими же людьми и с такими же целями. Поэтому если вы приходите туда «погулять» или «просто посмотреть», то будьте уверены, что в этих джунглях вы будете выполнять роль добычи. Готовы стать едой для хищников, обитающих на этой территории? А ведь там вам уже никто не поможет, потому

что вы сами выбрали «защищенное и безопасное общение», как вам говорили «друзья», не уточнившие, правда, что защищенное и безопасное оно будет именно для преступников и манипуляторов, но не для вас…

Что же касается официальных и открытых соцсетей, таких как ВК, то здесь ситуация не сильно лучше. Но, по крайней мере, там есть хоть какая-то надежда на помощь и защиту в случае возникновения у вас определенных проблем. Кроме того, в отличие от темного Интернета, на официальных платформах манипуляторы ведут себя не так нагло и открыто.

8. ОТВЕТСТВЕННОСТЬ ЗА РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ

Самые распространенные заблуждения.

Все мы пишем комментарии, ставим лайки и делаем репосты, но при этом часто ли мы задумываемся над тем, какие могут быть для нас последствия за неосторожно сказанное в Интернете слово? Как правило, про это мало кто задумывается по причинам, приведенным ниже.

1). Иллюзия анонимности. Я же в сети не под своим именем, да еще и через ВПН, с купленной возле метро сим-картой, оформленной непонятно на кого, да кто же меня такого продуманного найдет?

Еще лет 10 назад такое утверждение могло быть отчасти верным, но сейчас на дворе 2022 год, и с настоящей анонимностью в соцсетях и мессенджерах давно покончено. Кроме сим-карты, точки подключения вай-фай и вашего IP-адреса, который вы даже не можете скрыть различными средствами, имеется огромное количество способов установления вашей личности. Например, мало кто задумывается над тем, что все ваши действия идут первоначально

через провайдеров – поставщиков Интернета, а они, по закону Яровой, хранят о вас всю информацию, и по первому же требованию выдают её органам государственной безопасности. Более того, у них есть не только записи всех ваших разговоров, но и полный список всего вашего интернет-трафика, а также времени отправки всех ваших, как вы думаете, анонимных сообщений.

Проще говоря, в случае распространения каким-либо пользователем противоправной информации, органами правопорядка запрашивается выписка с точным временем всех действий данного аккаунта. Затем это время сверяется с массивом больших данных всех провайдеров, и по совпадениям устанавливается реальный адрес и личность пользователя, вне зависимости от того, где и каким образом он зашел в Интернет. Так вычисляется абсолютно любой пользователь, ведь у сотовых операторов есть информация о всех перемещениях абонентов, а у сетевых операторов реальные адреса всех точек подключения.

Этой информации более чем достаточно для того, чтобы вычислить любого пользователя. Всего по четырем привычным GPS-точкам в городе с легкостью идентифицируется любой человек, есть даже такой термин в геоаналитике «цифровая географическая сигнатура» или географический «отпечаток пальца. Передвижения каждого человека уникальны, и по ним легко можно узнать любого человека по данным сотового оператора. А по данным за несколько дней о времени входа в Интернет и размещении публикаций в соцсетях однозначно раскрывается любой анонимный ник в сети. По таким же принципам раскрываются все аккаунты, принадлежащие одному пользователю, и даже всего его окружения. И, конечно же, нельзя забывать об уличных камерах, которые также хранят информацию. В сочетании с данными о времени и месте отправки сообщений они также помогают полиции в поимке злоумышленников.

То же самое касается и мессенджеров. Да, они используют защищенное шифрованное соединение, но на своих серверах они хранят логи (текстовые файлы, в которых содержится информация о пользователях) со всеми вашими действиями, в том числе и со стёртыми вами сообщениями. В случае запроса

правоохранительных органов вся информация им выдается. Более того, в России с 2019 года по закону владельцы мессенджеров обязаны хранить логи переписок и идентифицировать пользователей. И таких косвенных следов, о которых мало кто задумывается, в Интернете очень много, поэтому любое ваше действие в сети оставляет свой уникальный цифровой след, по которому органам безопасности вычислить вас не составит особого труда.

2). Ложная уверенность в том, что информация с данной группы (страницы, беседы, чата, форума, закрытой группы) больше никуда не уйдет, и моё сообщение больше никто кроме участников не увидит.

Само по себе словосочетание «личное сообщение» — это некая условность. В Интернете не существует ничего личного, и ваше, как вы думаете, приватное сообщение может быть тут же переслано ещё кому-то. Вы об этом никогда не узнаете и никак не сможете проконтролировать его дальнейшее распространение.

Однако если оно содержало либо радикальный призыв, либо оскорбление, то вы должны понимать, что любое сообщение написанное в соцсети, закрытом чате, мессенджере, компьютерной игре, и т.д., считается публичным действием, распространением информации со всеми вытекающими последствиями, которые разберём далее.

Исключением может быть только закрытый чат, в котором состоят ваши родственники, но стоит там появиться хотя бы еще одному человеку, – и он становится публичным. Равно как и ваше сообщение, отправленное кому-то в личной переписке, может быть им переслано и стать публичным. Поэтому важно иметь привычку: всё, что вы пишете лично, пишите так, будто вы делаете это публично в открытой группе областного ГУВД. Эта привычка убережёт вас от многих необдуманных действий в будущем.

3). Иллюзия безнаказанности. Да кому я нужен, никто не будет меня искать за какой-то там пост или комментарий, все же такое пишут.

Да, пишут многие, и привлекают на самом деле не всех, но точно также можно сказать и про другие виды правонарушений, так что

тут дело не в системе, а в случае. Может оказаться и так, что именно в тот момент, когда вы оставите свой противоправный комментарий, ту же новость, которую вы только что откомментировали, зайдет посмотреть человек, имеющий прямое отношение к органам безопасности. Либо, что бывает чаще, человек «особо ответственный», и кроме того, категорически не согласный с вашим комментарием, который может крайне быстро, не вставая с места, написать на вас заявление в электронном виде, которые органы правопорядка с удовольствием рассмотрят. Почему с удовольствием? Потому что это практически 100% раскрытое дело – найти вас, не вставая с места, им не составит особого труда по причинам, описанным ранее.

4). Правовая безграмотность. Незнание списка экстремистских направлений и запрещенных течений. Незнание законов.

Эти пункты более подробно мы разберём позже, а начнем с базовых понятий, которые вам необходимо знать, поэтому постараемся изложить их суть максимально простыми словами.

Несмотря на то, что мы уже очень давно живём в интернет-пространстве, правовая грамотность большинства пользователей до сих пор находится на крайне низком уровне. Периодически приходится читать наивные комментарии: «Разве могут меня оштрафовать, или даже посадить за какой-то комментарий или репост»?

Да, могут. Если ваш комментарий, репост или видеоролик нарушает закон, то вам придётся нести за это ответственность. Есть даже такой термин, как «речевое преступление». Его используют в своей практике судебные лингвисты.

Кроме того, если вы состоите в какой-нибудь «нехорошей» группе, где обсуждаются радикальные или противоправные темы, то в любой момент данной группой, пусть даже и закрытой, могут заинтересоваться правоохранительные органы, в результате чего вы, независимо от того, писали что-то запрещенное или нет, можете стать невольным участником уголовного расследования. И вот тогда, будьте уверены, его фигуранты – ваши бывшие «одногруппники» – будут крайне заинтересованы в том, чтобы свалить часть вины на других участников группы, например, на вас! Возможно,

вам удастся доказать свою невиновность, но само участие в данном процессе крайне негативно скажется на вашем будущем.
Поэтому в сети всегда следуйте правилам обычной жизни и всегда смотрите за тем, кто и что делает рядом с вами. Если в реальной жизни вы попадаете в преступную компанию, то ваши шансы оказаться в тюрьме начинают стремительно приближаться к 100%. Увы, статистика такова, что те же правила действуют и в Интернете.
Про закрытые группы. Стоит иметь ввиду, что термин «закрытые группы» – бытовой, внутрисетевой, и он вовсе не говорит об их приватности. В нашем законодательстве не существует такого понятия, как «закрытая группа» или «закрытый чат», поэтому все действия, осуществляемые в этих сообществах, считаются публичными наравне с открытыми группами.
Теперь разберём конкретные примеры контента, за распространение которого в нашей стране предусмотрена ответственность.

Экстремизм.

Итак, что такое экстремизм? Ниже приведен текст полного определения, взятого с официального сайта МВД.
«1. Экстремистская деятельность (экстремизм):
- насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации (т.е. любые призывы к насильственному отделению какого-либо региона, либо призывы к насильственному свержению власти);
- публичное оправдание терроризма и иная террористическая деятельность (под этот пункт подпадают любые оправдания как терроризма в принципе, так и конкретных людей, совершивших теракты);
- возбуждение социальной, расовой, национальной или религиозной розни;
- пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой,

национальной, религиозной или языковой принадлежности или отношения к религии;

- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

- совершение преступлений по мотивам, указанным в пункте "е" части первой статьи 63 Уголовного кодекса Российской Федерации;

- использование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, за исключением случаев использования нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, при которых формируется негативное отношение к идеологии нацизма и экстремизма и отсутствуют признаки пропаганды или оправдания нацистской и экстремистской идеологии;

- публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

- публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей

деяний, указанных в настоящей статье и являющихся преступлением;
- организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;
- финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.
2. Экстремистская организация – общественное или религиозное объединение либо иная организация, в отношении которых по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.
3. Экстремистские материалы – предназначенные для обнародования документы либо информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы.
4. Символика экстремистской организации – символика, описание которой содержится в учредительных документах организации, в отношении которой по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности».

Так как мы говорим в первую очередь об ответственности в Интернете за публикацию экстремистских материалов, то далее условно разделим это явление на два направления. Первое – распространение контента собственного производства. Второе – распространение контента, содержащего пропаганду экстремистских организаций, а также литературы, фильмов, символики, и т.д., включенных в реестр экстремистских материалов.

Как правило, в уголовных и административных делах по статье экстремизм речь чаще всего идет о комментариях. В большинстве случаев это те ситуации, когда обычный человек, прочитавший какую-нибудь горячую новость, слишком эмоционально на неё отреагировал. Поэтому будьте всегда сдержаны в комментариях, а еще лучше – никогда их не пишите. Не давайте соцсетям о себе ту информацию, которую они потом будут обязательно использовать против вас. К тому же самая страшная правда Интернета заключается в том, что ваши комментарии на самом деле ни на что не влияют и никому не интересны (о ужас!).

Как понять, что ваш комментарий может подпасть под статьи экстремистской направленности? Прежде всего, смотрим определения, данные выше, – это основа. Тем более если комментарии содержат **интенцию** – намерение или конкретный замысел что-то сделать. Например, вы сообщаете о том, что хотите вызвать реализацию определенного положения вещей. Если эти вещи есть в списке выше – то это экстремизм.

Побуждение, подталкивание, мотивация. Такие слова как: «ты должен», «давайте сделаем», «давай», «пусть» и т.д. Все призывы и побуждения всегда содержат глагольность, т.е. глаголы императивной формы, а если до или после императивов размещен текст, подпадающий под пункты из списка, – то это тоже экстремизм.

Если вы пишите о том, что представители какой-нибудь национальности, веры, языковой группы и т.д. должны быть высланы за полярный круг, помещены в лагеря или должны быть лишены социальных благ, то данные высказывания, даже если они и не содержат прямых призывов к насилию, также подпадают под статьи про экстремизм. Призывы к сегрегации – тоже экстремизм. Это же

касается и распространения идей о расовой исключительности и о превосходстве над другими людьми какой-либо нации или народа. Как говорят эксперты-лингвисты, на самом деле нет разницы, какой это призыв – прямой или косвенный. Даже непрямые призывы в отдельных случаях могут подпасть под статью, если имеется соответствующий контекст.

И это ещё не все критерии. Запомнить все пункты, подпадающие под экстремистскую деятельность, не так просто, но, тем не менее, их всё же лучше знать или хотя бы понимать общий принцип, а он достаточно прост. **Экстремизм = возбуждение ненависти**.

Возбуждение ненависти – главный признак экстремизма, и если вы в комментариях захотите написать что-нибудь плохое в адрес не конкретного человека, а какой-нибудь большой группы людей, объединенных национальностью, религией, убеждениями или ещё чем-либо, то лучше лишний раз подумайте. Любой ваш порыв ненависти, особенно содержащий призыв к насилию, может вылиться в экстремистскую статью. Это может произойти даже с вашими старыми комментариями, оставленными много лет назад, про которые вы уже давно забыли. Такие случаи бывают, так что если вы сейчас вспомнили о том, что где-то когда-то писали нечто подобное, то лучше потратить время, найти и удалить свои старые комментарии.

Вторая причина, по которой чаще всего возбуждаются дела, это распространение заведомо экстремистских материалов, т.е. материалов, включенных в Федеральный список экстремистских материалов, – он находится в открытом доступе на сайте Министерства юстиции. На данный момент он содержит 5268 записей. Это книги, брошюры, видеоролики, записи и т.д. Список огромен и полностью его изучить невозможно, но это и не нужно. Каждый пункт из указанного списка был внесён на основании нарушения тех пунктов статьи, которые мы разбирали в начале, соответственно зная эти пункты, вы интуитивно сможете понимать, какой материал является экстремистским, а какой нет.

Конечно, точно вы это определить не сможете, но, тем не менее, понимание общих правил может вас оградить от неприятных

последствий. Не стоит быть слишком самоуверенными, и в случае сомнений в законности материала лучше его вообще избегать. И, конечно же, если вы видите, что человек экстремистских взглядов в сети предлагает вам что-то почитать, посмотреть или распространить, то практически наверняка речь идет об экстремистских материалах.

Что будет, если вы по незнанию опубликуете какой-либо материал из списка запрещённых, не зная, что он является таковым?

На этот счет Генеральной прокуратурой РФ было разъяснено, что: «*Цель возбуждения ненависти является одним из основных признаков состава преступления, предусмотренного ст. 282 УК РФ, что отсутствие такой цели исключает привлечение к уголовной ответственности по этой статье, а сам факт размещения в сети «Интернет» изображения, аудио- или видеофайла, пусть даже и содержащего признаки возбуждения вражды и ненависти при отсутствии иных признаков состава преступления, не является основанием для привлечения к уголовной ответственности».*
Здесь речь идёт о том, что есть некие условия, при которых публикация таких материалов не будет считаться наказуемой, но важно учитывать два фактора. Во-первых, данная оговорка сделана, прежде всего, для устранения проблемы публикации подобных материалов в учебных целях, так что если вы не преподаватель криминалистики, то вам такие материалы лучше всё же не публиковать. И, во-вторых, решение о том, что ваша публикация с экстремистским содержанием подпадает или не подпадает под это ограничение, будет принимать суд, и судебный эксперт будет руководствоваться своими, неизвестными вам правилами.
Некоторые блогеры намеренно искажают это исключение и пишут о том, что если вы репостите очевидно фейковую новость или какой-то экстремистский материал, то отвечать будете только в случае, если осознаёте, что транслируете запрещенные новости или материалы. Если же вы искренне приняли фейк за правду или посчитали, что это не противоречит статьям про экстремизм, то вы

не будете привлекаться к ответственности, поскольку тогда в ваших действиях не было умысла, а, следовательно, и состава преступления.

Звучит на первый взгляд вполне логично, но на практике это не работает. Если бы такие аргументы принимались, то так бы поступали все и избегали бы ответственности. Поэтому сослаться на незнание не получится, судебные эксперты-лингвисты в таких случаях, как правило, оперируют принципами «осознанности коммуникации». То есть, в данной ситуации снова работает всем известное правило: **«Незнание закона не освобождает от ответственности»**.

Ещё вы должны знать о том, что до суда будете находиться под следствием, а это значит, что у вас могут заблокировать все счета и карты, как минимум до решения суда. Данная мера применяется во всех делах, связанных с экстремизмом.

Для того, чтобы заморозить (заблокировать) денежные средства на счёте физического лица, у компетентных органов нет необходимости даже встречаться с этим физическим лицом – достаточно просто вынести процессуальное решение о признании лица подозреваемым в совершении определённых преступлений. С заблокированных счетов вы будете вправе снимать не более 10 тыс. рублей в месяц. При этом каждый раз для снятия денег необходимо писать заявление, которое потом банк согласует с Росфинмониторингом. И рассматриваемая нами мера будет действовать всё время, пока идёт следствие, и ещё долгое время после вынесения приговора. Даже в случае оплаты штрафа (если дело кончится штрафом) мера будет действовать ещё на протяжении года.

В большинстве случаев подростки пишут в соцсетях с аккаунтов, созданных с зарегистрированных на их родителей сим-карт. Соответственно, именно родители сразу же подпадают под все ограничительные меры, связанные со статьей за экстремизм, в результате чего многие семьи остаются без средств к существованию на длительный период. Поэтому не подставляйте своих родителей и всегда думайте о том, что, кому и как вы пишете!

Сейчас данная статья частично декриминализована, и на первый раз дела рассматриваются по Административному, а не по Уголовному Кодексу (за второй раз уже придётся нести уголовную ответственность). Но это касается только действий, направленных на возбуждение ненависти либо вражды (статья 282.1), за все остальные экстремистские статьи ответственность осталась прежней.

И ещё один неприятный нюанс, о котором мало кто знает. Большинство административных статей, относящихся к теме экстремизма, предполагают конфискацию предмета административного правонарушения. Проще говоря, у вас конфискуют компьютер или ноутбук.

Но более весомыми будут репутационные последствия, такие как невозможность в будущем поступить на госслужбу или в престижный ВУЗ. Ответственность по статье за экстремизм наступает с 14 лет, и все лица, подпавшие под неё, ставятся на спецучет. Кроме того, подобные правонарушения не имеют срока давности по той причине, что пока ваше сообщение или публикация есть в сети, считается, что преступление продолжает совершаться. Поэтому если вы вспомнили, что когда-то писали нечто подобное, то не пожалейте времени, найдите и удалите запись.

Учитывая вышесказанное, руководствуйтесь простым правилом: сначала подумали, потом репостнули или прокомментировали. Всегда помните, что, нажав кнопку «Поделиться», вы уже не сможете отозвать свой репост обратно, и он останется в сети навсегда. Как он может отразиться на вашем будущем – большой вопрос.

Травля, буллинг.

Многие из вас, скорее всего, сталкивались в сети с этой проблемой. Если вы стали жертвой сетевой травли, то первое и главное, что вы должны понять – дело не в вас. Сама интернет-среда с её отсутствием правил (даже неофициальных) и иллюзией безнаказанности и анонимности порождает людей, лишенных сочувствия, воспитания и интеллекта. Именно они, как показывает практика, чаще всего и становятся инициаторами травли.

Вместо понятного слова «травля» сейчас многие используют слово «буллинг», которое не меняет сути этого социального явления. Отсутствие государственной идеологии, воспитания в школах и наличие пропаганды индивидуализма и принципов «каждый сам за себя» – всё это способствует тому, что детей, участвующих в травле, становится с каждым годом всё больше. Потребительское мышление и идеи конкуренции сейчас стали основными и повсеместно транслируемыми. Соответственно, в сети это выливается в соответствующее поведение, тем более сами соцсети, особенно ВК, никак не препятствуют продвижению самой идеи травли – они даже не удаляют группы, пропагандирующие травлю.

Однако нельзя забывать, что для несовершеннолетних правонарушителей, совершающих подобные действия в отношении своих товарищей, существует гражданско-правовая, административная и даже уголовная ответственность. Оскорбление, т.е. унижение чести и достоинства другого лица, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме, согласно ч. 1 ст. 5.61 КоАП РФ может повлечь наложение административного штрафа, при этом использование сети «Интернет» является отягчающим обстоятельством и грозит наложением штрафа от пяти тысяч до десяти тысяч рублей.

Кроме того, оштрафуют и родителей, которые не научили своих детей уважительному отношению к товарищам. По статье 5.35 КоАП РФ им грозит небольшой штраф, но последствия применение такой статьи в будущем могут повлечь крайне неприятные последствия.

Если еще лет 10 назад уголовные и административные дела за оскорбления в сети были в диковинку, то теперь они стали повседневностью. Причем если вы просто оскорбили человека, то это одно, но если ваше высказывание содержит унижение достоинства человека либо какой-то социальной группы по признакам пола, расы, национальности, языка, происхождения, отношения к религии, то такие сообщения могут быть расценены в суде уже не как оскорбления, а как проявления экстремизма.

Если ваше высказывание будет признано таковым, то на первый раз вас будут судить по административной статье (20.3.1 КОАП). По ней предусмотрен штраф от десяти тысяч до двадцати тысяч рублей, или обязательные работы на срок до ста часов, или административный арест на срок до пятнадцати суток.

Клевета.

Тема травли часто бывает сопряжена с клеветой. Нередки случаи, когда зачинщики травли начинают распространять клеветнические материалы и приписывать жертве какие-нибудь ложные действия или обстоятельства. Между тем, клевета – это достаточно серьёзная статья, и такие «шутки» караются по закону штрафом до миллиона рублей либо обязательными работами сроком до 240 часов.

Если же клевета касается обвинения невиновного человека в совершении им преступления против половой неприкосновенности и половой свободы личности, либо другого тяжкого или особо тяжкого преступления, то за такое деяние клеветник может получить до 5 лет лишения свободы.

Конфликты споры, оскорбления.

Если вам нравится ругаться в сети или кого-то троллить, то вы должны понимать, что ничуть не анонимны. Вы никогда не можете точно знать, с каким человеком сейчас вступаете в конфликт. На аватаре может быть кто угодно, а за ним скрываться человек, который не прощает обиды и способный легко вас найти в реальной жизни. Как уже не раз говорилось, сейчас не существует гарантированного способа скрыть себя в сети. Даже если вы пишете со старой сим-карты, купленной в метро и оформленной не на вас, помните – вы не анонимны. Ваша деанонимизация зависит только от желания и возможности человека, которого вы обидели, потратить на поиски вас своё время и ресурсы. Зачастую для этого ему будет достаточно обычных «бытовых» программ.

Необходимо понимать и помнить, что вероятность навлечь на себя серьёзные неприятности в результате конфликта в Интернете сейчас гораздо выше, чем в реальной жизни.

Взлом аккаунта.

Все любители взламывать чужие аккаунты должны иметь ввиду, что это не шалость, а уголовно наказуемое деяние, которое подпадает под действие 138 статьи УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений». Ответственность в случае взлома чужого аккаунта наступает вне зависимости от того, воспользовались вы информацией, находившейся в нём, или нет.

Уважайте чужую личную жизнь и никогда не распространяйте никакой компрометирующей другого человека информации. Никогда не становитесь участником травли и не поддерживайте тех, кто этим занимается. Если вы видите, что в сети идет травля вашего знакомого, не стесняйтесь за него заступиться. Большинство участников такой травли зачастую не имеют своего собственного мнения и придерживаются обезьяньих инстинктов повторения всего за всеми, и если ваши аргументы будут убедительны, то вы сможете помочь человеку. Своими действиями вы способны прекратить его травлю и, возможно, тем самым спасёте ему жизнь.

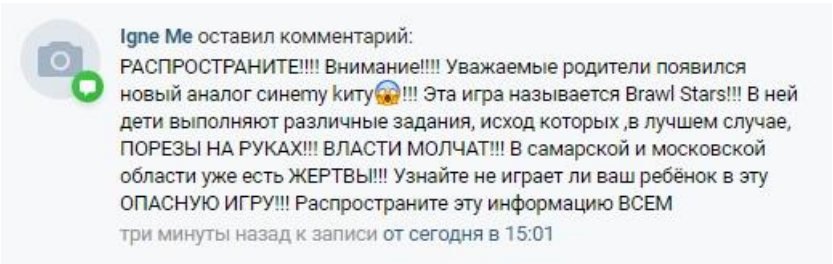
9. ФЕЙКИ

Слово «фейк» происходит от английского «fake», что можно перевести как «фальшивый, поддельный». Это слово чаще всего употребляют по отношении к новостям. Фейковые новости – это заведомо ложная или вводящая в заблуждение информация, выдаваемая за реальные новости. При этом фейки небезобидны, и они чаще всего создаются не просто так, а ради достижения определенных деструктивных целей. Среди них могут быть банальный «хайп» для раскрутки канала, создание паники, раскачка людей на

определенные действия и даже воспрепятствование работе некоторых жизненно важных служб.

Ради достижения этих целей фейковая новость всегда создается в максимально эмоциональном стиле, с обилием восклицательных знаков и заглавных букв, с шокирующими подробностями события, яркими картинками, обилием смайликов и в конце – с обязательным призывом к репосту! Кроме перечисленных признаков в фейках почти всегда отсутствует конкретика относительно места происшествия (города), потому что их цель – максимальное распространение. По этой же причине фейковая новость чаще всего делается так, чтобы она подходила под любой населенный пункт, и автор «новости» не указывается по этим же причинам. Сгенерированный таким образом фейк, как правило, распространяется в 5-10 раз быстрее обычной новости, что и нужно заказчикам.

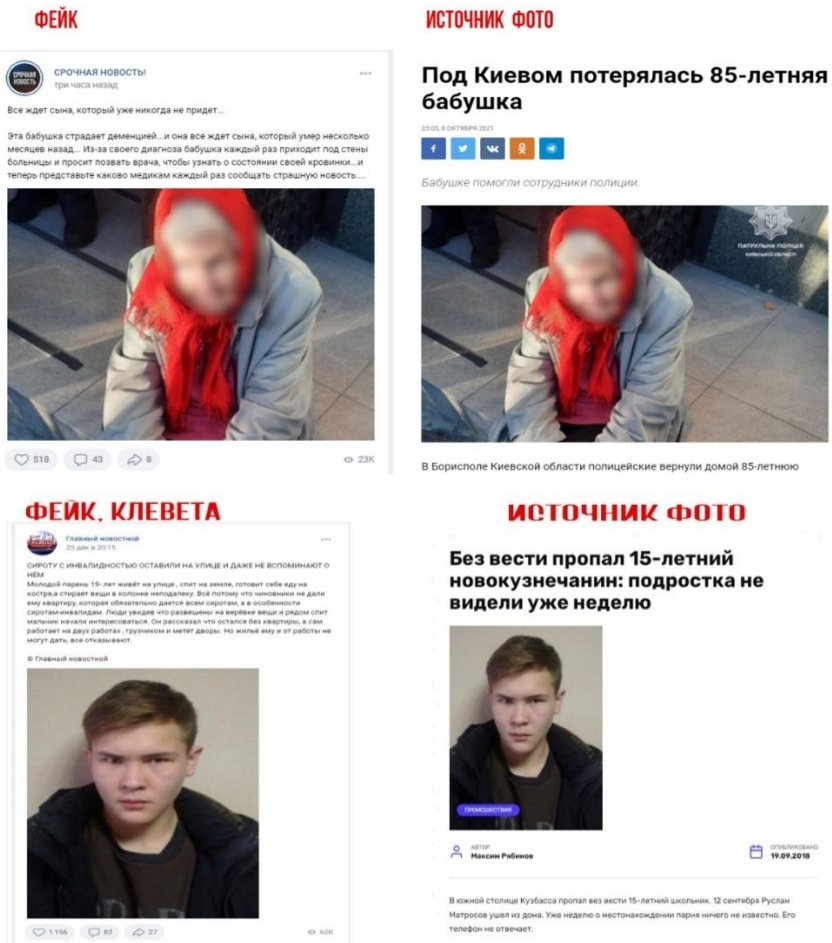
Бывают и коммерческие фейки, цель которых через создание искусственной паники вокруг несуществующего события привлечь внимание к какому-то конкретному продукту. Вот так, например, несколько лет назад рекламировали игру «Бравл Старс».


Igne Me оставил комментарий:
РАСПРОСТРАНИТЕ!!!! Внимание!!!! Уважаемые родители появился новый аналог синему киту!!! Эта игра называется Brawl Stars!!! В ней дети выполняют различные задания, исход которых ,в лучшем случае, ПОРЕЗЫ НА РУКАХ!!! ВЛАСТИ МОЛЧАТ!!! В самарской и московской области уже есть ЖЕРТВЫ!!! Узнайте не играет ли ваш ребёнок в эту ОПАСНУЮ ИГРУ!!! Распространите эту информацию ВСЕМ
три минуты назад к записи от сегодня в 15:01

Да, именно рекламировали, это не опечатка. Суть приведённого фейка заключается в том, чтобы заставить родителей поинтересоваться у детей, не играют ли они в эту игру. Расчёт идет на то, что дети после этого начнут её искать. На самом деле ничего из описанного в сообщении в игре, разумеется, не было.

Ниже приведены примеры групп ВК, системно зарабатывающих на откровенных фейках, которые они сами же и производят. Такие фейки легко найти и вычислить. Берёте картинку публикации, сохраняете её на компьютере и вставляете в поиск картинок Яндекса. Он выдаст все места в Интернете, где использовалось данное изображение. Казалось бы, всё просто, но в этих группах миллионы

подписчиков, и никто из них не сомневается в правдивости этих «новостей». Судя по комментариям, они даже и не пытаются проверить достоверность вброса, а тупо реагируют на него.



Развивайте в себе критическое мышление, никогда не поддавайтесь эмоциям и всегда проверяйте увиденную информацию!

Распространение.

Мессенджеры в плане распространения фейков и прочего нечистоплотного контента – сейчас, пожалуй, безусловные лидеры. В соцсетях же чаще всего такого рода информация появляется в городских группах типа «Подслушано в...», «Объявления», «Барахолки», «Мамочки…» и т.д. Их администраторы с помощью таких сообщений накручивают рейтинги и популярность.
Основную часть информации в сети и мессенджерах распространяют не люди, а боты. Интернет наполнен ботами, более 50% трафика публикуют именно они, а не люди. Так, боты разносят фейки, которые потом подхватывают реальные люди. В каждой информационной войне есть как сценаристы и режиссеры, так и рядовые исполнители.

Ответственность за фейки.

С 2019 года в наше законодательство были внесены изменения, касаемые ответственности для граждан за распространение фейков. До этого времени ответственность за фейки могли нести только официальные СМИ, но теперь по этой статье может быть привлечён любой человек.
Фейком, за распространение которого может последовать привлечение к ответственности и наказание, по новому закону считается только **заведомо недостоверная** информация, способная нанести реальный вред обществу и государству.
За распространение фейковой информации в России грозит ответственность в соответствии со ст. 207.1 («Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан») и ст. 207.2 («Публичное распространение заведомо ложной общественно значимой информации, повлекшее по неосторожности вред здоровью, смерть человека или иные тяжкие последствия»).
Нарушителю грозит штраф от 300.000 до 2000.000 рублей или лишение свободы на срок до трех или пяти лет – в зависимости от тяжести последствий.

Однако в законе есть оговорки. Гражданин понесёт ответственность за распространение фейковой информации в случае, если он знал, что сообщает неправду, и выдавал ложные данные за достоверные. Об этом сообщили в Верховном суде РФ 30 апреля 2021 года. Но на это не стоит сильно рассчитывать, потому что определять ваше отношение к распространению фейка будете не вы, а суд.

Для того, чтобы вы могли отличить настоящую новость от фейка, приведём конкретные примеры.

- Если вы зарепостите фейк о том, что какая-нибудь звёздная пара что-нибудь сделала, то такая информация не подпадает под закон о фейках, потому что эта дезинформация не несёт угрозы жизни людей, безопасности государства и работе специальных или общественно значимых служб.
- Если вы транслируете фейковую новость, придуманную вами или кем-то другим, относящуюся к конкретному человеку, и серьёзно его компрометирующую, то это тоже не относится к закону о фейках, но ваше деяние подпадает под закон о клевете, по которому вас ждёт более суровое наказание.
- Если же вы распространяете ложную информацию, которая способствует сбою в работе жизненно важных служб и ведомств, либо представляющую угрозу жизни и безопасности граждан, то ваше деяние относится к этому закону. Например, распространённый фейк с призывами неважно по какому поводу срочно звонить всем в конкретную больницу парализует работу её телефонной линии на несколько дней, что может привести к прямым неблагоприятным последствиям. Соответственно, распространение такого фейка уже подпадает под статью.

Распространение фейка со списком лекарств, которые, якобы, все отравлены, и их применение ведёт к смерти, тоже несёт прямую угрозу жизни и здоровью граждан, и также подпадает под этот закон. Более того, если впечатлительный гражданин, прочитавший ваш репост, не станет принимать из-за него нужный ему препарат и умрёт, то вы уже будете отвечать по пункту 2 этой же статьи.

Штраф в размере от 1500.000 до 2000.000 рублей, либо исправительные работы на срок до двух лет, либо принудительные работы на срок до пяти лет, либо лишением свободы на тот же срок.
Приведем дословный пример такого живучего фейка, который периодически возникает с 2012 года.

Срочно передать ВСЕЕЕЕЕЕЕЕЕЕЕЕМ!!!!! В Питере Скоропостижно скончались 12 детей в возрасте от 3-12 лет. В результате вскрытия выяснилось,что все дети стали жертвой сильной аллергической реакции, вызванной лекарственными средствами. Реакция была настолько серьёзной, что никто из детей даже не доехал в больницу, все они скончались либо дома, либо по дороге в больницу. В данный момент полиция ведёт разбирательство по делу, однако изъять из продажи все лекарственные средства не получится. Удалось выяснить то, что все лекарства, в результате приёма которых погибли дети, были завезены в нашу страну контрабадным способом и являются опасной подделкой. ВНИМАНИЕ!!!! Перечень лекарственных средств, которые ни в коем случае нельзя давать детям: АМОКСИЦИЛЛИН, КАПЕСУЛА, ИБУПРОФЕН СУСПЕНЗИЯ, АЛКЛОФЕНАК, СУМАМЕД, ИНГАЛИПТ, АНТИСЕПТ, ИНФЛЮЦИД, ДЕТСКИЙ ПАНАДОЛ, САНАСОЛ. Постарайтесь ограничинить применение вашими детьми вышеуказанных препаратов, как минимум, месяц- пока вся продукция не будет изъята из аптек. РАССПРОСТРАНИТЕ ВСЕМ, У КОГО ЕСТЬ ДЕТИ, СРОЧНО!!!

Ответственность за ложные сообщения об актах терроризма.

Если вы распространяете свои либо чужие заведомо ложные сообщения о минировании или других актах терроризма, то данные действия не относятся к закону о фейках, а являются преступлением террористической направленности. За неё предусмотрена уже уголовная ответственность и реальные сроки. Максимальный срок лишения свободы за заведомо ложное сообщение о готовящимся взрыве – восемь лет.
Неважно, какими рассуждениями и целями вы руководствовались. Сделали вы это ради шутки, игры, на спор или потому что просто не хотели идти на контрольную – это уже не имеет никакого значения. В результате вашей «шутки» были задействованы серьёзные силы полиции, МЧС, скорой и прочих служб. Ресурсы этих служб не безграничны: после вашего сообщения они были

оторваны от своей работы и, возможно, из-за вас не смогли спасти чьё-то имущество, здоровье или даже жизнь. И если этот факт будет доказан, то в дальнейшем ваш приговор может быть увеличен до 10 лет (статья 207 УК РФ).

Это верхняя планка наказания и далеко не все телефонные террористы получают такой срок, но, тем не менее, минимальная планка наказания по ч. 1 ст. 207 УК РФ – штраф от 200.000 до 500.000 рублей, либо ограничение свободы до 3 лет, либо принудительных работ от 2 до 3 лет, – что, согласитесь, весьма существенно.

Не так давно Верховный суд (ВС) удовлетворил иск Генеральной прокуратуры и признал движение «Колумбайн» террористическим, а, значит, и запрещённым на территории России в любом виде. Т.е. движение «колумбайн» признали не экстремистской, как многие думают, а террористической организацией. Соответственно, публикация любых материалов, призывающих к школьным расстрелам, либо оправдывающих их, либо оправдывающих лиц, их совершивших, будет квалифицироваться не как экстремизм, а уже как терроризм, что не одно и тоже. Терроризм – более тяжкая статья, и по ней нет никаких послаблений.

Ответственность по ст. 205.2 (публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма; максимальное наказание – до 7 лет лишения свободы) или по ст. 205.4 (организация террористического сообщества и участие в нём; максимальное наказание – пожизненное лишение свободы) начинается уже с 14 лет. Прежде чем начать публиковать такие материалы или призывы даже шутки ради, вы должны сознавать, что ответственность будет крайне серьёзной, особенно в силу того, что тема терроризма активно мониторится спецслужбами и есть все шансы, что ваше сообщение или публикацию подобного содержания увидят те, кто надо.

К тому же такое деяние гарантированно навсегда оставит свой след в вашей репутации, и в будущем может не дать вам поступить на госслужбу или в престижный ВУЗ.

Дипфейки.

Это новая проблема, которая, скорее всего, с каждым годом будет только усугубляться. Дипфейк – искусственно созданный медиапродукт (видео, голос), в котором один человек заменяется другим. На Ютубе залито множество таких роликов, которые выглядят достаточно убедительно. Также сейчас можно достаточно эффектно сымитировать любой голос, если есть его образец, – и это ещё одна причина, по которой не стоит говорить с незнакомыми людьми по телефону и проходить навязываемые опросы. Подобные технологии часто используются при шантаже, что естественно, уголовно наказуемо.

10. НАРКОТИКИ

К сожалению, несмотря на всю очевидность опасности и наличия огромного количества информации о вреде наркотиков, данная тема до сих пор остаётся более чем актуальной. Кроме того, последние годы мы наблюдаем значительный рост наркопотребления. Почему это происходит?

Важно отметить, что современные наркотики – это, как правило, синтетические вещества, и они имеют ряд серьёзных отличий от наркотиков прошлого поколения, которые были распространены у нас в стране в 90-е годы.

Первое и главное отличие – это зависимость. Теперь она наступает с первого раза, и всего один раз попробовав наркотическое вещество, даже ради интереса, вы запускаете ту страшную цепь событий, которая неизбежно приведёт вас не просто к гибели, но к потере всех важных для вас социальных связей, здоровья, жизненных перспектив и, самое страшное, – к потере разума. Про это важно сказать отдельно. Все наркологи уже не первый год бьют тревогу по поводу тех последствий, которые вызывают в организме человека современные наркотики.

Еще относительно недавно, лет 10 назад, они с большим трудом, но всё же могли лечить наркоманов. Даже несмотря на

чудовищные последствия для здоровья некоторых наркоманов удавалось вернуть к нормальной жизни, но теперь такого нет. Всё дело в современных наркотиках – они стали другими! Производители изменили формулу, и любой человек, начинающий употреблять любые современные наркотики, стремительно деградирует как личность. По словам наркологов, **человек, вроде бы, есть, а личности в нём уже нет**…

Любая работа с зависимостями – это, прежде всего, работа с личностью, с волей человека. Видимо, понимая это, производители современных наркотиков делают их так, что они стремительно, за весьма короткий период ломают и разрушают саму личность человека и он, по сути, превращается в биоробота с единственной программой – найти денег на новую дозу. К сожалению, вернуть такого человека к нормальной жизни в большинстве случаев не представляется возможным.

Единожды попробовавшие уже после второй дозы, как правило, перестают получать от наркотиков тот эффект, на который рассчитывали изначально, и переходят в режим постоянного потребления уже не ради получения удовольствия, которого больше нет, а ради приглушения боли от ломок, которые появляются у них при отсутствии дозы. Усиление зависимости происходит на фоне стремительного распада личности, деградации и потери здоровья. В среднем агония человека длится около года, после чего он умирает от неизбежной интоксикации, передозировки или отравления. Последние недели и месяцы он проводит в депрессии, боли и одиночестве. Увы, но исход всегда один.

Не будем рассказывать о видах современных наркотиков, потому что в этом нет никакого смысла, практически все они ведут к последствиям, описанным выше. Вы должны понимать главное – не существует одной дозы! Никогда не верьте тому, что можно один раз попробовать, и ничего страшного не случится – это враньё!

Если вас пытаются убедить в безобидности одного раза, то почти в 100% случаев лишь для того, чтобы подсадить на свой товар и получать с вас определенный процент. Занимаются этим, чаще всего, сами наркоманы, уже утратившие возможность

зарабатывать себе на дозу. По статистике один такой наркоман по этой схеме затягивает с собой в могилу еще 6-8 человек, ранее не планировавших употреблять наркотики.
Именно поэтому вы всегда должны уметь говорить «нет». В молодежной среде свобода выбора всегда считалась и считается главной ценностью. Но наркотики, как и иные виды химических зависимостей, – это продукты по подавлению и лишению этой самой свободы. Человек, употребляющий наркотические вещества, зависим и несвободен: с момента первого употребления он становится рабом и заложником наркоторговцев.

Распространение.

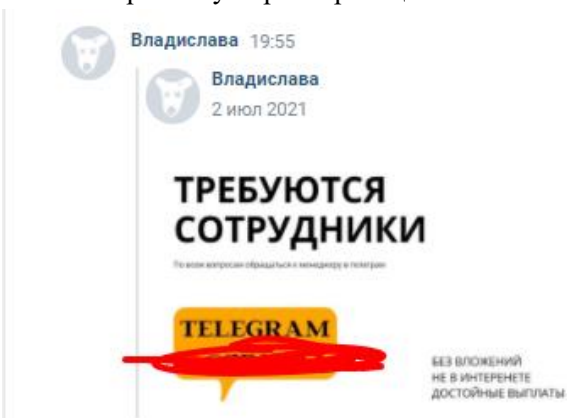
Кроме употребления есть ещё одна не менее серьезная проблема – вовлечение несовершеннолетних в распространение наркотиков. Подростков привлекают к деятельности по нанесению надписей на стенах с рекламой, рекрутируют в качестве «закладчиков» (тех, кто прячет закладки с наркотиками в условных местах) и обещают лёгкий заработок. К сожалению, не всем очевидно, что на самом деле – это миф, и никакого «лёгкого» заработка там нет.
Такая «работа», естественно, неофициальна, к тому же наркомагазин знает все ваши данные, а вот вы про своего «работодателя» не знаете ничего. Зачастую это приводит к тому, что «работодатель» может не только ничего вам не платить, но ещё и заставлять работать на него бесплатно, под угрозой сдачи вас в полицию в случае отказа. Такие угрозы более чем реальны, и нередко именно так они и поступают, сами при этом ничем не рискуя.
Именно низовые распространители-закладчики и попадают чаще всего в руки правоохранителей: их легче всего взять с поличным. Не все родители, а тем более дети, знают, что возраст, когда наступает уголовная ответственность за подобное преступление – 16 лет, и одна «закладка» может обернуться сроком от 8 до 20 лет лишения свободы. По этой статье в принципе не предусмотрено условных сроков, но подростки чаще всего про это не знают.
Попав однажды «в дело», обратного выхода они обычно уже не находят. Получив их персональные данные и имея на них

доказанный компромат, «магазин» их уже никогда не отпустит. В случае отказа закладчика работать подключается группа «коллекторов», имеющаяся в каждом таком «магазине»… Вот вам и ситуация, когда за вход платят рубль, а за выход – два (а на самом деле – намного больше).

Многих распространителей в дальнейшем втягивают в потребление и наоборот, что обеспечивает работу бесконечного «конвейера смерти». Все низовые участники этого конвейера – расходный материал. Работают они неделю-две, иногда больше, потом их ловят, и они получают от 8 лет. Самих закладчиков организаторы называют «шкуры» или «шкуроходы», и это не случайно, ведь никакой ценности они для наркомагазина не представляют. Они просто расходники, ведь благодаря соцсетям и мессенджерам обеспечивается их непрерывный поток.

Как вовлекают.

В большинстве случаев всё начинается с предложения работы. Такие сообщения приходят массово как в соцсетях, так и в мессенджерах. Рассылка идёт чаще всего со взломанных чужих аккаунтов либо с фейковых страниц. За работу предлагают суммы, не имеющие даже приблизительного отношения к реальности, но многие на это ведутся и соглашаются на предложенную «работу», оказываясь на крючке у наркоторговцев.



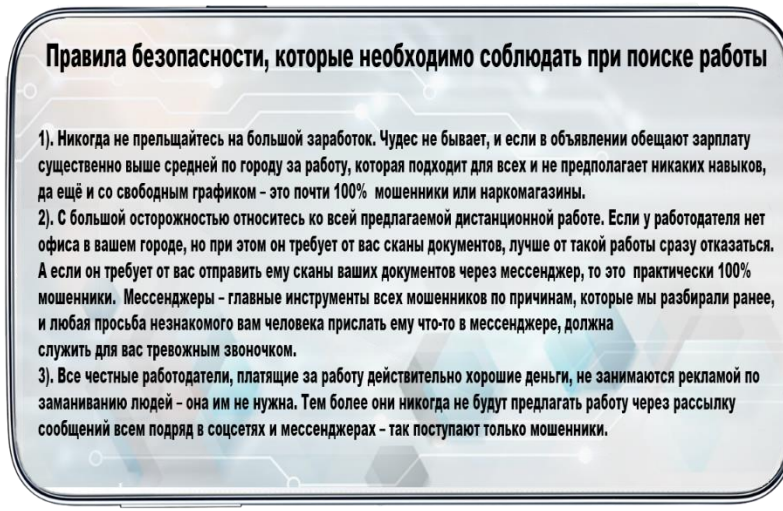
Заметьте – в таких объявлениях не всегда говорят о том, что именно нужно разносить. Чаще всего такую «работу» подростки находят по поисковому запросу «курьер». О том, что именно им нужно разносить, многие узнают уже слишком поздно – после того, как предоставили свои персональные данные наркомагазину и сделали первую закладку. Но даже если им каким-то образом потом удаётся уйти с этой работы, это не гарантирует безопасности даже спустя долгое время.

«За студентом московского мединститута оперативники из отдела по борьбе с незаконным оборотом наркотиков МВД пришли в учебную аудиторию. Ему казалось — всё, пронесло, работу эту можно забыть, как страшный сон. Прошло почти полгода, как он ничем таким не занимался. В начале прошлой весны Артём искал подработку — нужно было купить новый ноутбук. Во «ВКонтакте» он несколько раз получал сообщения от незнакомцев, предлагавших «работу курьером с высокой зарплатой раз в неделю». Написал одному из них и узнал, что сотрудники нужны интернет-магазину по продаже наркотиков. Конечно, было страшно, Артём понимал, что это нелегальная работа, но решил, что долго в закладчиках не задержится. Вот только соберёт деньги на компьютер и, может быть, ещё летний отдых, новые кроссовки…

Артём был курьером полтора месяца. Деньги платили, но он постоянно слышал о том, как другие закладчики «уезжают» на семь лет в тюрьму. В какой-то момент испугался и перестал выходить на связь с куратором. Тем временем на одной его закладке полицейские поймали покупателя. Завели дело, изъяли его смартфон, открыли мессенджер и нашли переписку с оператором интернет-магазина. В переписке — фото с локацией, где оставили закладку. Установили, с какого IP-адреса отправили снимок. Нашли владельца — Артёма. Заказали у мобильного оператора биллинг его телефона (когда человек передвигается по городу, его смартфон принимает сигнал с разных станций оператора, с помощью этой информации можно установить местонахождение пользователя). Биллинг подтвердил, что Артём был в то время там, где покупатель позже забирал сверток».

Нами приведена реальная история, описанная в статье ТАСС: «*Улики, записанные в смартфоне. Как данные из приложения становятся доказательством вины*». И таких историй сейчас сотни. Повторимся, что Интернет помнит и знает о вас всё, и вы не можете никак удалить те цифровые следы, которые оставляете. А ваш смартфон является персональным «наблюдателем», который знает о всех ваших действиях и перемещениях.

Запомните несколько важных правил, которые необходимо знать при поиске работы, чтобы избежать подобных ловушек.



Ответственность за распространение.

Как уже упоминалось ранее, распространение наркотиков – тяжкая статья, и по ней в принципе не бывает условных сроков. Полная уголовная ответственность наступает с 16 лет. Если вам исполнилось 16, вы сделали хотя бы одну закладку и получили за неё хотя бы рубль, то вас посадят на 8 лет, даже если вы круглый отличник с безупречной репутацией.

Но если вам еще нет 16, это не означает, что вы не понесёте за это ответственности. Согласно части второй статьи 87 УК РФ, к

несовершеннолетним, совершившим преступления, могут быть применены принудительные меры воспитательного воздействия либо им может быть назначено наказание, а при освобождении от наказания судом они могут быть также помещены в специальное учебно-воспитательное учреждение закрытого типа.

Специальное учебно-воспитательное учреждение закрытого типа – это фактически тюрьма для несовершеннолетних со всеми вытекающими последствиями. Учитывая, что распространение наркотиков относится к тяжким видам преступлений, шансы там оказаться крайне высоки.

Но даже если вы физически никогда не прикасались к наркотикам, не делали закладки, не получали за них деньги, но при этом имели отношение к наркобизнесу, то вы всё равно можете попасть за это в тюрьму.

Конкретный пример. В Екатеринбурге суд приговорил к 3 годам колонии 17-летнюю студентку из-за сообщений в Телеграме о «закладках» с наркотиками. При этом к наркотикам она не прикасалась и даже деньги за них не получала, она только отправляла в мессенджере описание мест, где они спрятаны. То же самое касается «работы» по нанесению надписей и рекламы в Интернете. Всё, что относится к продаже наркотиков, любая связанная с ней деятельность подпадает под уголовную статью.

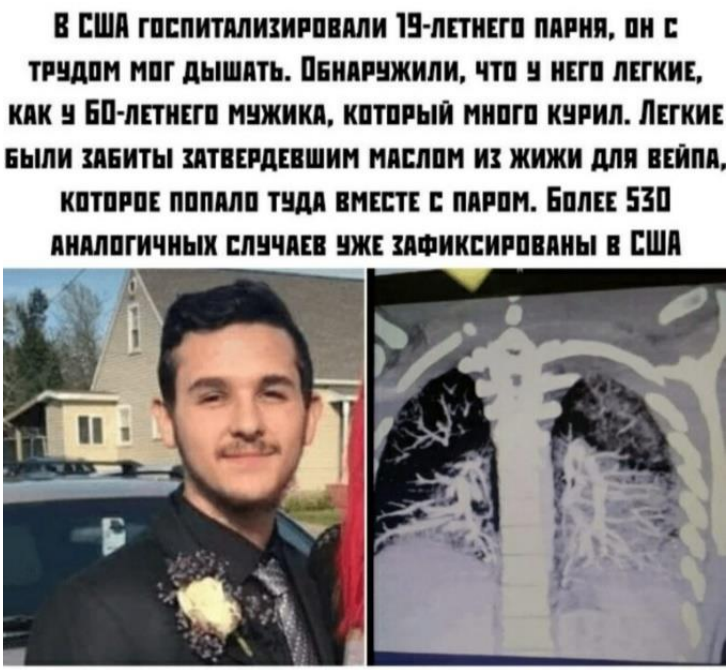
Более того, если вы знаете о том, что ваши друзья или знакомые торгуют наркотиками или склоняют кого-нибудь к употреблению, но никак этому не препятствуете или даже способствуете, то при неудачном стечении обстоятельств вас могут признать соучастником или пособником совершения тяжкого преступления. Поэтому совет – всегда держитесь подальше от этой темы – как в Интернете, так и в реальной жизни.

11. СНЮСЫ, ВЕЙПЫ, ЭЛЕКТРОННЫЕ СИГАРЕТЫ

Еще одна важная тема, как ни странно, также непосредственно связана с Интернетом. Дело в том, что основное распространение

и реклама всех электронных средств доставки никотина сейчас происходит именно через Интернет. Через него же идёт массированная кампания, организованная табачными компаниями (которые уже давно выкупили всё производство электронных сигарет) по распространению ложной информации о якобы безопасности электронных сигарет.

Давно доказано, и врачи это подтверждают, что электронные сигареты несут ничуть не меньший, а иногда и больший вред для организма, чем обычные сигареты. В США, где впервые возникла эта проблема, уже давно введены жёсткие ограничения на продажу данной продукции, поскольку есть множество пострадавших и даже погибших людей от так называемой болезни вейперов – EVALI.



EVALI расшифровывается как e-cigarette or vaping product use associated lung injury – повреждение легких, связанное с

употреблением электронных сигарет или вейпа. Эта болезнь смертельно опасна. О ней практически ничего неизвестно, но развивается она стремительно и может привести к катастрофическому поражению легких вплоть до летального исхода. По первым симптомам она похожа на двухстороннюю пневмонию, только никакие лекарства и антибиотики пациенту не помогают.

Суть болезни заключается в том, что пар, который «парят» вейперы, оседает на легких, и со временем образует на них пленку, через которую в легкие перестает впитываться кислород. Таким образом, человек долго и мучительно погибает от недостатка кислорода, и помочь ему иногда бывает невозможно.

Продавцы, рекламирующие вейпы и остальные электронные средства доставки никотина, часто говорят о том, что их средства якобы помогают бросить курить. Это наглая ложь, потому что все эти средства содержат более высокую концентрацию никотина и вызывают более быстрое привыкание, что подтверждает статистика.

Зависимость от никотина среди российских школьников после появления на рынке электронных сигарет выросла **в 6 (!) раз**. Эту шокирующую цифру озвучила научный сотрудник НИИ Минздрава РФ Галина Сахарова. Оказывается, сегодня среди юных курильщиков более 64% уже имеют признаки высокой степени никотиновой зависимости. Вы должны понимать, что употребление никотина в любом виде – это не вредная привычка. Это болезнь, причем болезнь тяжелая и мучительная, с непредсказуемыми последствиями.

Что же касается модных ещё несколько лет назад снюсов, то по ним была сделана экспертиза: в их составе нашли соли тяжелых металлов – свинца, ртути и кадмия. Особенность этих веществ такова, что один раз попав в организм, они уже из него никогда не выводятся и остаются навсегда, отравляя его всю оставшуюся жизнь.

Итак, с появлением на рынке перечисленных средств, табачники в очередной раз расширили свой бизнес за счет наивных и малообразованных граждан, поверивших в безопасность и «элитарность» нового продукта. Мы рождены в эпоху Интернета, когда такое

осознанное невежество, как употребление этих веществ, уже нельзя списать на простое незнание. В эпоху информации неосведомленность в этих вопросах – это сознательный выбор.

На самом деле даже неважно, что вы употребляете: снюс, сигареты, вейпы или одноразки – это не имеет никакого значения. Если вы это делаете, то вы стали жертвой примитивной пропаганды, воспроизводите то, чему продавцы этой отравы вас научили, и теперь вы приносите им стабильную прибыль.

Продавцы этой отравы будут всегда ставить вас перед ложным выбором, постоянно предлагая употреблять что-то одно вместо другого – вейпы вместо сигарет, электронные сигареты вместо вейпов, снюсы вместо сигарет, вейпов и электронных сигарет, а далее, когда вы окончательно потеряете разум от этих веществ, вам предложат покупать у них жевательный навоз, пропитанный никотином.

Сейчас вся пропаганда продавцов строится вокруг СПОСОБА употребления никотина: это психологическая манипуляция, известная как «выбор без выбора». Вам, по сути, предлагают разные способы того, как стать никотиновым наркоманом. Вы теперь понимаете весь абсурд происходящего?

И вам никогда не скажут о том, что самое разумное решение – не употреблять ничего, потому что для торговцев вы пчёлы, приносящие им мёд. Вы не должны думать, анализировать, читать сложные статьи и материалы, нет. Вы должны просто повторять за блогерами и вестись на дешёвый контент многочисленных сообществ, – вот и всё, что им от вас нужно.

Продажа зависимостей – крайне выгодный бизнес. К примеру, себестоимость одной пачки сигарет – примерно полтора рубля, при том, что пачка стоит больше 100 рублей, а в ситуации с продажей электронных сигарет прибыль ещё больше.

Употребление наркотиков, снюсов, вейпов, алкоголя и всего того, что вызывает зависимость и негативно влияет на мозг, во всём мире расценивается как принадлежность к социальному дну. Не отсутствие денег, как кто-то может подумать, а именно употребление психоактивных веществ говорит о социальной опущенности

человека. Человек может быть бедным, но иметь всеобщее уважение и почёт, но употребляя что-то из вышеперечисленного, он неизбежно скатывается на самое дно, где никакие деньги ему уже не помогут.

Однако продавцы никотиновой отравы всегда будут рисовать ореол элитарности и принадлежности к какой-то особой субкультуре избранных, чтобы подсадить вас на свой продукт.

В сельском хозяйстве табак используют как инсектицид, ведь содержащийся в нём никотин – это самый настоящий яд и отличное средство для уничтожения насекомых. Но вот только насекомые умирают от него бесплатно, а вы ещё умудряетесь за это деньги платить. Сельские жители вам подтвердят, что даже коровы и козы не едят табак, так как чувствуют ядовитое растение. И никакая пропаганда, никакие блогеры и ложные научные исследования не заставят козу съесть табачный лист. И только человек готов платить деньги за медленное самоубийство…

Точно ли мы являемся самыми разумными живыми существами на земле? Иногда появляются серьёзные сомнения.

12. РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ АККАУНТА И ПОВЕДЕНИЮ В СЕТИ

Некоторые рекомендации по поводу ведению аккаунта в соцсетях.

Двойная аутентификация.

Если соцсеть или любой другой интернет-ресурс даёт вам возможность использовать двухфакторную аутентификацию, то обязательно стоит ей воспользоваться. Двухфакторная защита существенно увеличивает безопасность вашего аккаунта. Обычно это выглядит так: первый рубеж – это логин и пароль, второй – специальный код, приходящий по СМС, т.е. если система увидит, что кто-то со стороны попытается зайти в ваш аккаунт, она запросит у него подтверждение, которым будет код из СМС, пришедшей на ваш телефон. Естественно, у мошенника его не будет, и даже зная пароль, он не сможет воспользоваться вашим аккаунтом. Поэтому

не пренебрегайте двойной аутентификацией, если есть такая возможность.
Но и в этом правиле всё же есть исключения. Если вы регистрируетесь на малоизвестном ресурсе ради временных задач (например, для того, чтобы что-то скачать), то лучше лишний раз не афишировать номер телефона. Важно помнить, что ваш номер телефона – это ваш самый чёткий цифровой след. Поэтому старайтесь его использовать для регистрации только в самых крайних случаях и только на известных сервисах. И, само собой, ни при каких обстоятельствах нельзя показывать его публично на своей странице или в комментариях.

Как должен выглядеть ваш аккаунт.
Никаких личных фотографий. Совсем. На аватарку можно поставить что-то нейтральное. В настройках профиля должен стоять запрет на геотеги. Профиль закрытый. Никакой информации о себе, никакого указания города, школы, и т.д. Вместо имени и фамилии лучше придумать псевдоним. Друзья и так знают, как вас зовут, и вы можете к ним добавиться, а вот посторонним знать ваше настоящее имя и фамилию ни к чему.
Список групп тоже должен быть скрыт и доступен только друзьям: если вы скрыли персональную информацию, но при этом подписаны на группу «Новости Саратова» и здесь же на группу «Школа № 999 5б», то вычислить вас уже не составит никакого труда.
В настройках лучше включить запрет на получение личных сообщений от всех, кроме друзей. Кто вам может написать, если вы всё равно под псевдонимом? Правильно, только мошенники или спамеры, а они вам зачем?
Минимум репостов, лайков, минимум комментариев к постам. Желательно, чтобы на вашей стене вообще ничего не было. Переписку с друзьями лучше осуществлять только через личные сообщения. Почему это важно? Дело в том, что все ваши действия в сети, такие, как комментарии в группах или на страницах друзей, на самом деле видят все ваши друзья. Про это мало кто задумывается, а ведь от этого могут случаться разные неприятные ситуации.

На вашей персональной странице в ВК рядом со списком друзей есть кнопка «обновления», и если её нажать, можно увидеть всё, что они пишут и комментируют. Такая же кнопка есть и у ваших друзей, и если незнакомый человек, которого вы зачем-то добавили к себе в друзья, имеет недобрые намерения, то он легко узнает ваш психологический портрет. Для этого ему будет достаточно проанализировать, что вы репостите и какие комментарии пишете. Любой человек, имеющий статус «друга», всё это видит. И затем, уже зная ваши сильные и слабые стороны, а также увлечения, он сможет вами манипулировать и завести вас куда угодно. Еще есть специальные программы, которые без труда могут найти все ваши комментарии, когда-либо оставленные в сети, и с таким «досье» будет очень легко составить ваш точный психологический портрет. Вот что пишут специалисты: «Для того, чтобы иметь довольно ясное представление о том, кем вы являетесь, не нужно много «лайков» – 10 достаточно для того, чтобы система знала о вас больше, чем коллеги по работе. 50 – и компьютерный анализ знает вас на уровне вашего партнёра или члена семьи. 200 «лайков» достаточно, чтобы рассказать обо всех ваших тайных пристрастиях также подробно, как это сделали бы ваши муж или жена после многих лет брака».

Ваши данные в сети давно и активно используют рекламщики и мошенники, а также манипуляторы и вербовщики, причём часто это делается специальными программами в полуавтоматическом режиме. То же самое делают и сами соцсети, продавая поведенческие данные своих пользователей. Так что, если вы не хотите стать их рекламным товаром, оставляйте им о себе минимум информации.

Интернет – не место для откровений.

Людям иногда бывает проще раскрыться и излить душу виртуальному знакомому, чем родным или реальным друзьям, согласно известному в психологии феномену «случайного попутчика». Но сеть – это не место для откровений. Каждое ваше признание, рассказанное кому-то, останется в сети навсегда, и в любой момент может быть найдено злоумышленниками и использовано против

вас. Как вы понимаете, вероятность того, что ваш «случайный попутчик» окажется не тем, за кого себя выдаёт, тоже крайне высока. Некоторые манипуляторы специально подводят жертву к откровенному разговору для того, чтобы выманить у неё нужную им информацию. Поэтому главное правило общения в сети – не доверять никому.

Никогда не делайте в сети того, чего бы не стали делать в реальной жизни.

Тут всё просто – будьте собой. Не нужно пытаться в сети из себя что-то изображать. Любой ваш обман рано или поздно вскроется, а вот информация о нём останется в сети навсегда. Многие используют соцсеть как громоотвод, канализируя туда свои негативные эмоции. Этого делать тоже не нужно. Интернет место публичное, и так как с реальной анонимностью в сети давно покончено, не стоит в Интернете делать того, чего бы не стали делать в реальной жизни.

Кроме того, люди постоянно меняются, и через несколько лет у вас тоже поменяются мнения и убеждения, и вам станет стыдно за то, что вы писали раньше, но удалить это навсегда и безвозвратно вы, к сожалению, уже не сможете, даже если сильно захотите.

Интернет помнит всё! Что попало в сеть, остаётся там навсегда!

Как мы уже писали ранее, человек очень быстро меняется, и все ваши публикации, репосты, комментарии и фотографии, которые вам ещё вчера казались забавными и уместными, спустя несколько лет могут довольно ощутимо испортить вашу репутацию или карьеру. Работодатели в серьёзных фирмах (в которых вы хотите в будущем работать) имеют не только системы анализа сетевого поведения своих сотрудников, но и всегда проверяют прошлое новых работников. Для этого у них есть вполне легальные системы, позволяющие без труда собрать о вас всю нужную им информацию. Никакие ваши «старые левые аккаунты» не помогут спрятать от этих систем интересующую их информацию.

С каждым годом подобные системы становятся совершеннее, и скоро они будут сразу выдавать о человеке готовый результат, с полной характеристикой на основе его больших данных. Подобные системы уже сейчас начинают вводиться в систему образования под называнием **«персональные образовательные траектории»,** несмотря на то, что такой подход мы считаем принципиально неправильным. Тем не менее, уже есть немало примеров, когда люди теряли работу и репутацию из-за своих старых публикаций и фотографий, сделанных ими когда-то давно, причём эти примеры даже не связаны с применением подобных систем.

Федерального судью уволили из-за скандальных фотографий в социальной сети. На одних фото девушка обнимает бутылку с водкой и пристально смотрит в камеру, на других – отпивает горячительный напиток из горлышка, на третьих – позирует в сомнительной позе на фоне отеля и с аквалангом. Данные фотографии были опубликованы ею в социальной сети ВК.

В мае 2020 года в Интернете мелькало видео, снятое о том, как «элита» Новороссийска расслабляется на закрытой базе отдыха в разгар карантина. На кадрах зрители рассмотрели Екатерину Демченко – вице-мэра города. Буквально через несколько часов глава городской администрации подписал приказ о её увольнении.

Директор Центра молодёжных инициатив Лидия Бузовчук поставила крест на карьере в мае 2020 года, ввязавшись в обсуждение публикации во ВК. Женщина написала, что раньше за детей вообще не платили, и все как-то жили «и не скулили». Несмотря на то, что она комментировала не со своего аккаунта, её быстро вычислили по фото в профиле, после чего уволили.

В январе 2020 года новый министр культуры РФ Ольга Любимова внезапно стала самой обсуждаемой фигурой в российском сегменте Интернета. Причиной спонтанного интереса стала фотография, сделанная много лет назад. Ольга Борисовна запечатлена на ней в футболке с неприличным принтом: «Кто вы такие? Что вам надо? Я вас не знаю! Идите на*». Она удалила это фото заранее, но… Например, с помощью простого сервиса https://web.archive.org можно восстановить удалённые публикации и фотографии, что многие пользователи и сделали. В результате

нашлись ещё более дискредитирующие нового министра публикации.
Ещё раз повторим: Интернет помнит всё, поэтому повторяем – всегда следуйте простому правилу: **берегите цифровую честь смолоду.**

В Интернете нет срока давности.
На основании вышеизложенного сформулируем ещё одно правило: **сначала подумали, потом написали.** В любой момент жизни все написанные вами когда-то давно сообщения могут быть найдены специальными программами и предъявлены на всеобщее обозрение. Вы даже можете быть привлечены за них к административной или уголовной ответственности, даже если с момента их написания прошло уже несколько лет. В Интернете работает железное правило: если комментарий противоправного содержания находится в публичном доступе, то считается, что преступление совершается прямо сейчас. Были даже случаи, когда комментарий написали до возраста наступления ответственности, а следствие по нему начали спустя много лет, когда он был зафиксирован, и автору уже исполнилось 18!

Соцсети не на вашей стороне. Они не будут вас защищать.
Если вы думаете, что в случае возникновения проблем с законом в связи с публикацией вами запрещённых материалов, соцсети будут вас защищать, то даже не надейтесь! Они могут декларировать безопасность и защиту пользователей в своих коммерческих целях, но в реальности они никогда не встанут на вашу защиту.
По запросам МВД и прочих органов они спокойно выдают все нужные им данные, и даже те, о которых вы не догадываетесь. Например, у них есть данные о времени ваших сеансов, времени написания вами сообщений или просмотра видео.
Отношение соцсетей к своим пользователям можно сравнить с отношением наркомагазинов к своим закладчикам – они расходный материал, приносящий им деньги. Точно также и здесь: для соцсетей пользователи – это пожиратели проплаченного

рекламодателями контента. Вы им интересны только для «скармливания» вам рекламы. Чем быстрее вы её просмотрите, тем скорее они получат новый заказ, а следовательно, они заинтересованы в том, чтобы пользователей было максимально много – настолько, насколько это возможно.

Что соцсетям нужно сделать для того, чтобы привлечь максимально большое количество пользователей? Правильно, разрешить им публиковать абсолютно всё, даже те материалы, которые прямо нарушают закон, и ничего не удалять. То есть соцсети подставляют своих пользователей ради собственного обогащения.

Соцсетям ничего не стоит с помощью нейросетей вычистить весь противоправный контент, который многие пользователи, особенно несовершеннолетние, публикуют по незнанию. Тем самым соцсети помогли бы таким незадачливым пользователям избежать неприятных для них последствий, но соцсети никогда не будут этого делать, потому что тогда они потеряют часть прибыли. Как говорится, просто бизнес, ничего личного.

Поэтому никогда не руководствуйтесь принципом: «ну другие же это публикуют». Эти «другие» публикуют запрещенные материалы «до поры до времени». Вы видите только то, что происходит здесь и сейчас, но вы не знаете о сотнях уже оштрафованных пользователях, публиковавших такие же материалы. Тот же ВК мог бы удалить эти материалы, прекрасно зная об их противозаконности, и спасти своих пользователей от штрафа, но ему гораздо выгоднее их подставлять и зарабатывать на рекламе, в том числе и в запрещенных группах.

13. НОВАЯ ЦИФРОВАЯ РЕАЛЬНОСТЬ

В последней главе хочется предложить некое общее описание той новой цифровой реальности, в которой нам всем теперь приходится жить. Понимание этих процессов и тенденций даст вам возможность самостоятельно анализировать и вникать во многие деструктивные явления цифрового мира.

- **Любой ваш проступок может попасть в сеть и остаться там навсегда**, принеся вам репутационный урон в будущем. Проблема в том, что в современных реалиях вы не можете проконтролировать, в каком виде вы попадёте в сеть. Сейчас можно сфотографировать любого человека на улице, а затем распознать его, и тут же найти его аккаунт и все его фотографии в соцсетях, причём выложенные не только им. Тоже самое касается вашего голоса, который также распознается. По поводу ценной для вас информации ещё один совет: никогда не храните её в облаке в облачных хранилищах, всё что вы туда положили – уже не ваше.
- **Сейчас при разборе сложных ситуаций видеозаписи используют как доказательство**. Так что кто первый толкнул рукой, кто первый проявил агрессию, тот и будет признан виновным. Кроме сотен тысяч уличных камер, установленных сейчас во всех крупных городах, еще всегда есть «свидетели с телефоном». Это граждане, считающие своим долгом снять всё, что выбивается за рамки привычного, и сразу же выложить это в сеть. Поэтому в случае каких-то конфликтных ситуаций нужно вести себя осмотрительно и сдержанно.
- **Соцсети стали показывать ваши комментарии в ленте друзей по своему усмотрению**, что не нормально, но сделать вы с этим ничего не можете. Поэтому помните, что все сообщения в соцсети – публичные.
- **Все ваши поисковые запросы тщательно собираются и хранятся поисковиками**, и в случае чего, они могут быть использованы против вас. Кроме того, такие данные могут быть не только добыты полицией, но и использованы в качестве доказательства вины. Один пример.

«Благодаря поисковику Google полиции удалось доказать вину Мэтью Шустера — работника компании Alpha Computer Service, уволенного и обиженного. После того как его выставили на улицу, Мэтью попытался взломать беспроводную сеть компании.

Его роковой ошибкой стало использование Google — Шустер вводил в строку запроса фразы вроде: «how to broadcast interference over wifi 2.4 GHZ», «wireless networks 2.4 interference» и

«interference over wifi 2.4 GHZ». Это его и сгубило: поисковые запросы фигурировали в суде как доказательство вины. В результате Шустера приговорили к 15 месяцам тюремного заключения и $20 тыс. штрафа».

- **Все ваши фото теперь автоматически распознаются**, и вы идентифицируетесь даже в тех ситуациях, когда вы не знали о том, что вас фотографируют. По вашим фотографиям можно установить очень многое: ваши привычки, места, где вы бываете, достаток, здоровье, физические данные и много чего ещё. Соединив это с данными вашей активности в соцсетях, с комментариями, подписками, лайками, интересами и т.д., несложно составить ваш полный психологический портрет. Установив ваш психотип, злоумышленники могут вами легко управлять, поэтому постарайтесь в сети оставлять как можно меньше следов.

- **Слушают всех, но зачем я кому-то нужен?** Сейчас вы никому не нужны, но через несколько лет, когда вы станете депутатом или чиновником, вы станете очень интересны, и вот тогда-то все ваши необдуманные действия в сети, совершенные в юности, могут всплыть на поверхность и серьезно испортить вам жизнь. Кроме того, такие сведения могут стать инструментом для шантажа и влияния на вас.

- **Дрессировка пользователей.** Флешмобы, челленджи – всё это элементы дрессировки пользователей на выполнение абсолютно любых, даже самых безумных действий. Если вы посмотрите Тик-ток, то он уже практически полностью построен на обезьяньем принципе повторения всего за всеми. Теряется ценность оригинальности и, как результат, через такой примитивный контент создается общество, лишенное собственного мнения и думающее толпой. Это очень опасные тенденции, последствия которых могут начать проявляться уже в ближайшем будущем.

- **Зависимость от новостного потока.** Ещё одно явление, характерное для многих пользователей сети. Люди живут новостями, постоянно листают ленту и боятся пропустить что-то важное. Если вы узнали в них себя, то вам следует задать себе один важный вопрос. Какие из тех десятков тысяч мировых новостей, которые вы прочитали за год, повлияли на ваши отношения с близкими, на

вашу жизнь, карьеру, работу, т.е. на всё то, что для вас действительно важно?

И если они действительно повлияли, то в лучшую ли сторону, или наоборот, послужили поводом для глупых споров, ругани и раздора? Скорее всего, второй вариант. А сколько из этих новостей в итоге оказались фейками, манипуляциями, ложью, или просто пустышками? Наверное, большинство. Тогда вы должны задать себе главный вопрос: а оно того стоило?

Кроме того, зависимость от новостного потока крадёт ваше время, мешает мышлению, засоряя его ненужной информацией, и приучает к пассивности. В психологии даже есть такой термин «выученная беспомощность», и им страдают, прежде всего, люди, зависимые от новостной информации.

Ещё они, как правило, страдают от депрессии, так как уровень негатива и «желтизны» прессы с каждым годом растет, что не способствует укреплению психического здоровья у читателей. Главный продукт современных СМИ – это стресс. Именно его они продают и монетизируют в первую очередь.

- С каждым годом усиливается контроль за Интернетом, и это общемировой тренд. Россия в плане контроля за Интернетом находится в самом конце списка. Если мы сравним законы, касаемые Интернета США, ЕС, Великобритании и других стран с нашими законами, то наш Интернет окажется среди них самым либеральным. Возможно, многим это покажется странным, но это действительно так. Во Франции уже есть дела, когда людей судили за лайки, в Великобритании давно работает предфильтрация всего контента, а в США любой призыв к митингам влечёт уголовную ответственность.

- Для соцсетей вы – траффик. Вы их кровь и цифровая нефть, на вас они делают деньги, вы отдаёте им своё время, а они вам взамен дают ненужную вам информацию, депрессию и сомнительные знакомства. К тому же они не обеспечивают вам даже самую минимальную безопасность от злоумышленников и манипуляторов и, более того, сами отчасти становятся ими, продавая ваши поведенческие данные налево и направо.

Так что в целом Интернет – это поле битвы, где медиаплатформы бьются за внимание пользователей с целью их захвата, манипуляции и извлечения из них прибыли. Каждое ваше действие в сети уже кем-то монетизировано, нравится вам это или нет. Всё, что вы пишите в соцсетях, нужно им для создания вашего более точного цифрового профиля, **чтобы продавать ваше внимание более выгодно.**

- Клиповое мышление. У всех активных пользователей соцсетей, вне зависимости от их желания и возраста, формируется так называемое «клиповое мышление». Проявляется оно в неспособности долго удерживать внимание на чём-то одном, в результате чего человек теряет способность сосредоточиться, потому что привыкает к постоянной и быстрой смене картинок и коротких новостей. Именно такой ритм потребления информации предлагают все медиаплатформы.

Чем дальше, тем более мелкогранулированным и не связанным между собой контентом они «кормят» пользователей. В итоге человек не просто привыкает к такому ритму подачи, но и утрачивает способность к сосредоточенному и долгому погружения в какую-либо важную тему.

Людям с развитым клиповым мышлением становится физически «больно» читать текст более трёх абзацев или смотреть видео дольше двух минут. Всё их нутро начинает протестовать и требует быстрой смены картинок, потому что мозг уже ТАК привык, вернее его к ЭТОМУ приучили…

Последствия такого расстройства внимания проявляются, к сожалению, уже не в виртуальной, а в реальной жизни. В первую очередь человек утрачивает способность учиться, потому что любое обучение – это, прежде всего, долгая концентрация внимания на какой-то сложной теме, а человек с приобретенным клиповым мышлением становится физически на это не способен.

Кроме того, ухудшается память, потому что потребление «быстрого» и не связанного между собой контента приводит к тому, что мозг перестаёт его запоминать за ненадобностью. Проверьте себя еще раз (мы об этом писали ранее): можете назвать любых 5 постов

в момент вашего последнего посещения соцсети? Нет? А ведь вы их просмотрели не один десяток…

Такой расклад весьма выгоден соцсетям, поскольку людям с клиповым сознанием можно втюхивать раз за разом одно и тоже. Тем не менее, клиповое мышление – это не приговор, и избавиться от него можно по принципу: «где вход, там и выход». Заставляйте себя всегда дочитывать объёмные тексты, смотреть длинные ролики, читать книги и старайтесь меньше проводить времени в соцсетях.

14. ЕСТЬ ЛИ У ВАС ИНТЕРНЕТ ЗАВИСИМОСТЬ? ТЕСТ

Тест на интернет-зависимость (С.А. Кулаков, 2004)

Ответы даются по пятибалльной шкале: 1 – очень редко, 2 – иногда, 3 – часто, 4 – очень часто, 5 – всегда.

1. Как часто Вы обнаруживаете, что задержались в сети дольше, чем задумывали?
2. Как часто Вы забрасываете свои домашние обязанности, чтобы провести больше времени в сети?
3. Как часто Вы предпочитаете развлечения в Интернете близости со своим партнером?
4. Как часто Вы строите новые отношения с друзьями по сети?
5. Как часто Ваши знакомые жалуются по поводу количества времени, что Вы проводите в сети?
6. Как часто из-за времени, проведенном в сети, страдает Ваше образование и/или работа?
7. Как часто Вы проверяете электронную почту, прежде чем заняться чем-то другим?
8. Как часто страдает Ваша эффективность или продуктивность в работе из-за использования Интернета?
9. Как часто Вы сопротивляетесь разговору или скрываете, если Вас спрашивают о том, что Вы делали в сети?

10. Как часто Вы отодвигаете на второй план неприятные мысли о своей жизни, заменяя их успокаивающими мыслями об Интернете?
11. Как часто Вы чувствуете приятное предвкушение от предстоящего выхода в сеть?
12. Как часто Вы боитесь, что жизнь без Интернета станет скучной, пустой и безынтересной?
13. Как часто Вы раздражаетесь, кричите, если что-то отрывает Вас, когда Вы находитесь в сети?
14. Как часто Вы теряете сон, когда поздно находитесь в сети?
15. Как часто Вы чувствуете, что поглощены Интернетом, когда не находитесь в сети или воображаете, что Вы там?
16. Как часто вы замечаете свои слова «ещё пару минут…», когда находитесь в сети?
17. Как часто Вы пытаетесь безуспешно урезать время пребывания в сети?
18. Как часто Вы пытаетесь скрыть количество времени пребывания в сети?
19. Как часто Вы предпочитаете находиться в сети вместо того, чтобы встретиться с людьми?
20. Как часто Вы чувствуете подавленность, плохое настроение, нервничаете, когда Вы не в сети, что вскоре исчезает, стоит Вам выйти в Интернет?
При сумме баллов 50-79 стоит учитывать серьезное влияние Интернета на вашу жизнь. При сумме баллов 80 и выше у Вас с высокой долей вероятности Интернет-зависимость и Вам необходима помощь специалиста.

15. ЗАКЛЮЧЕНИЕ

Закончим наш обзор отрывком из книги «Цифровая гигиена», которую мы рекомендуем для прочтения людям любого возраста, т.к. она является наиболее полным сборником наблюдений за современным цифровым миром:

«Грустный исторический опыт. До сих пор любые технологические новинки, которые можно было использовать для порабощения, принуждения или войны, человечество немедленно с этими целями и использовало. У нас нет никаких сомнений, что всё плохое, что только можно сделать с помощью цифровых технологий (эксплуатация, манипуляция, дискриминация и прямое военное уничтожение), будет сделано, как всегда, в нашей истории.

Второй довод, позволяющий делать негативные прогнозы о развитии цифры – это так называемый бухгалтерский принцип, который гласит: «Если созданы возможности для злоупотреблений, то нужно считать, что злоупотребления уже имеют место».

В отношении «цифры» это означает: если в цифровые технологии изначально заложены возможности удаленного контроля, слежки, подстройки контента на лету, сбора персональных данных и пр., то можно предполагать, что среди прочих «невинных» коммерческих и деловых целей обязательно имеются ввиду и будут достигнуты цели контроля, слежки, манипуляции, вербовки, навязывания контента, рекламы, политических идей».

Сейчас от многих можно слышать такое утверждение, что мы теперь живём в цифровой реальности. Если вы с этим согласны, то отложите книгу и посмотрите в окно. Вы видите там цифровую реальность? Очевидно, что нет, но, тем не менее, влияние цифровых технологий на многих людей столь сильно, что правильнее будет сказать, что мы сейчас все живём в мультиреальности. В слоёном пироге из двух реальностей, одна из которых создаётся медиаплатформами, рекламщиками, блогерами, манипуляторами, пропагандистами, и городскими сумасшедшими. Понимая эти механизмы, старайтесь всегда выбирать реальную жизнь, пусть и не всегда и не во всём совершенную.

16. РЕКОМЕНДАЦИИ ДЛЯ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

На уровне законодательства.

В Комитете по информационной безопасности Союза «Родительская Палата» на данный момент разработан целый ряд предложений по изменению той катастрофической ситуации, которая сложилась в нашей медиа- и интернет-среде. На данный момент есть более 20 пунктов, требующих принятия срочных законодательных мер. Так как книга предназначается в том числе для детей и подростков, мы не можем перечислить данные пункты, но в случае необходимости готовы их выслать на почту, а также принять активное участие в разработке законодательных инициатив.

На уровне Министерства просвещения РФ.

На основе информации, изложенной в книге, необходимо делать уроки по информационной безопасности в школах, начиная с первого класса. К сожалению, на данный момент таких уроков либо нет, либо информация, даваемая на них, является неактуальной или сильно устаревшей. Очень надеемся на помощь педагогов в подготовке таких уроков. В случае необходимости готовы предоставить все интересующие материалы.

На уровне Министерства культуры РФ.

Необходимо организовать работу по созданию качественных видеоматериалов, посвящённых проблемам безопасности детей в сети. Нужны как документальные, так и художественные произведения на эти темы для разных возрастов.

На уровне Минздрава РФ.

Необходимо наладить работу в школах по профилактике употребления детьми и подростками никотиносодержащей продукции и электронных средств доставки никотина. Также необходимо доносить до педагогов и родителей информацию о необходимости соблюдения временных норм пребывания детей перед экранами.

На уровне Министерства науки и высшего образования.

На базе научно-исследовательских институтов необходимо организовать работу по изучению негативного влияния различных

деструктивных направлений на человека с последующими рекомендациями по внесению отдельных направлений в список запрещённых. Также необходимо провести национальные исследования по влиянию Интернета, гаджетов и компьютерных игр на здоровье и развитие детей. К сожалению, до сих пор такие исследования не были проведены.

На уровне Министерства внутренних дел РФ.

Необходимо создание отдельных подразделений, занимающихся вопросами выявления и блокировки опасного и вредоносного контента. Также необходимо наладить работу по анализу аккаунтов детей и подростков, совершивших преступления.