

МЕДИА И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ



**9-11
класс**



МЕДИА И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ

**УЧЕБНОЕ ПОСОБИЕ ДЛЯ 9-11 КЛАССОВ
ИЗДАНИЕ ДЛЯ АПРОБАЦИИ**

Алматы, 2019
ОФ «Международный центр журналистики «MediaNet»

Банников П. В., Соколова Т., Гороховский О.,
Печищев И. М., Радзявичус Д., Усупбаева А., Шишкин Д.П.

Медиа и информационная грамотность. Учебное пособие для 9-11 классов. Издание для апробации. / П. В. Банников, О. Гороховский, Т. Соколова, И. М. Печищев, Д. Радзявичус, А. Усупбаева., Д.П. Шишкин.
– Алматы: ОФ «Международный центр журналистики «MediaNet», 2019.
– 152 с., илл.

Учебное пособие по медиаграмотности для школьников старших классов Казахстана подготовлено Международным Центром Журналистики MediaNet в рамках проекта «MediaCAMP» представительства Internews в Казахстане.

Данное учебное пособие стало возможным благодаря помощи американского народа, оказанной через Агентство США по международному развитию (USAID). МЦЖ MediaNet несет ответственность за содержание публикации, которое не обязательно отражает позицию USAID, Правительства США, или Internews.

© ОФ «Международный центр журналистики «MediaNet»

Оглавление

ВВЕДЕНИЕ	5
ГЛАВА 1. История медиа: как мы оказались в XXI веке	7
Коммуникации человека — от жеста к письменности	9
История развития медиа	11
Утром в газете, вечером в куплете	15
От телевизора к интернету	18
ГЛАВА 2. Медиополе и медиаграмотность	21
Типы медиа	23
Как накапливалось знание	25
Что же такое современные мифы?	28
Медиамир	29
Медиамир и медиаграмотность	30
ГЛАВА 3. Фейк и фантазия: чему мы верим и почему	37
Вымысел в искусстве: кино, театр, тексты	39
Чем отличаются сказки для детей и для взрослых	40
Детские сказки как терапия	41
Нужны ли сказки для взрослых?	42
Музыка и эмоциональные манипуляции в кино	42
История кино. Как повлиять на людей за 50 секунд?	43
Слово против технологии	44
ГЛАВА 4. Информация. Источники информации	45
Информация и ее признаки	47
Искажение признаков информации и его последствия	48
Современные источники информации и их признаки	53
Что такое «информационная деревня»	54
Механизм искажения информации (принцип каскадности информирования)	56
Факторы влияния на информацию: шум, цунами, троллинг и их угрозы	59
Информационный шум	59
Информационные волны	60
Информационный троллинг	61

ГЛАВА 5. Формальная логика: курс молодого бойца	65
Виды манипуляций и как с ними бороться.....	67
История манипуляций и борьбы с ними	69
Классификация логических уловок (ошибок).....	71
Разновидности petitio principii	73
ГЛАВА 6. Медиа и реклама	77
Реклама и медиа.....	79
Виды визуальных материалов.....	81
Функции рекламы.....	85
Приёмы и стереотипы в рекламе	87
ГЛАВА 7. Кибербезопасность	91
Безопасность в социальных сетях	93
Какие проблемы возможны в социальных сетях?	93
Как защитить свой аккаунт в соцсетях	95
Уровень второй. Защита с подтверждением	99
Опасности входа в аккаунт на чужом компьютере	101
ГЛАВА 8. Конфиденциальность в социальных сетях	103
Источники проблем	105
Как обезопасить себя от цифровых преступников	108
Что знают правоохранительные органы.....	115
ГЛАВА 9. Проверка на достоверность фото и видео	121
Инструменты проверки фото и видео на достоверность.....	123
Кто производит фото- и видеофейки	124
Казахстанский кейс	126
Проверка видео	130
Казахстанский кейс от Factcheck.kz	130
ГЛАВА 10. “Темные” социальные медиа	135
Что такое Dark Social.....	137
Как проверять рассылки в мессенджерах	138
ГЛОССАРИЙ	142

ВВЕДЕНИЕ

За последние десять лет мир кардинально изменился. На нас всё большее влияние оказывает не сама физическая, осязаемая реальность, в которой мы существуем и взаимодействуем друг с другом, а информационный фон, в котором мы находимся. Факты отходят на второй план, на первый выходят мнения, причём не всегда основанные или хотя как-то связанные с реальностью, а партнёр по онлайн-игре оказывается гораздо более ценным источником информации, чем сосед по дому.

В таком дивном новом мире всякую секунду мы подвергаемся информационной атаке, которая может как просто испортить нам настроение или дезинформировать, так и привести к более печальным последствиям, например мы можем стать жертвой мошенников, других преступников, а то и вообще попасть в сферу влияния экстремистов.

И только критическое мышление, основанное на понимании того, как работают и воздействуют на нас современные медиа, может помочь нам избежать манипуляций и сохранять независимость суждений и действий. Когда мы говорим о мире информации, такое мышление называют медиаграмотностью.

Перед вами первый экспериментальный учебник по медиаграмотности в Казахстане. И коллектив авторов надеется, что он поможет вам ориентироваться в современном информационном поле, отсекал лживую информацию и её источники, а также повысить свою цифровую безопасность.

Кроме того, программы, описанные в книге, позволят вам сделать свой смартфон или ноутбук инструментом, возможно, превосходящим весь арсенал Шерлока Холмса, если конечно, не забывать про его превосходное мышление и критический взгляд на действительность. Это — самое главное, и вместе с вами мы разберёмся в том, как устроен мир информации и как вы сами можете проводить расследования, защитить своё личное пространство, а возможно — защитить своих близких от информационных атак и обмана.

ГЛАВА 1

ИСТОРИЯ МЕДИА: КАК МЫ ОКАЗАЛИСЬ В XXI ВЕКЕ



В первой главе мы посмотрим на историю человечества как на историю коммуникаций между людьми. И она неожиданно предстанет перед нами совсем не так, как мы привыкли её видеть.

Коммуникации человека — от жеста к письменности



Коммуникация — это процесс передачи информации от одного носителя к другому или к другим.

В истории человечества зафиксировано всего пять способов коммуникации: жест, речь, изображение, письменность и музыка (специфический статус. В настоящее время крайне сложно найти музыку как форму коммуникации, она почти целиком превратилась в искусство, выйдя из сферы коммуникаций).



Жест — это самый разный способ коммуникации, он появляется еще до 100 000 года до нашей эры. Жест в первую очередь использовался на охоте и означал что-то, связанное только со «здесь» и «сейчас». Похожая жестовая коммуникация присутствует у некоторых животных, которые охотятся в стае, в частности у волков. Жест появляется задолго до того, как в ходе эволюции человек научился говорить, его голосовые связки и легкие еще недостаточно развиты для коммуникации, но простейшие обозначения руками, понятные соплеменникам, он уже способен произвести.

К доисторическому периоду речевые органы человека развиваются настолько, что позволяют появиться речи. Именно речь является единственным натуральным способом коммуникации. Это значит, что речь — достижение эволюции, природы, а не изобретение самого человека. Речь носит мультимодальный характер, то есть предусматривает сразу несколько уровней, в частности, включает в себя не только содержание, но и интонацию, высоту, скорость и так далее. Речь является главным носителем информации. На сегодняшний день в мире насчитывается более 7 000 языков, однако их число стремительно сокращается. По данным ЮНЕСКО, в мире исчезает приблизительно один язык в две недели. Одна из причин исчезновения языков — неравномерность их распространения, $\frac{2}{3}$ живущих на Земле разговаривают на 40 самых распространенных языках, и лишь $\frac{1}{3}$ приходится на все остальные языки. Язык считается умершим, когда умирает последний его носитель,

поэтому языки, которые не обзавелись письменностью, подвержены такому риску сильнее.

Изображение появляется между 50 000 и 30 000 годами до нашей эры. Изображение носит универсальный характер — символ, обозначающий, например солнце, одинаково легко могли понять носители любого языка. Изображение появляется тогда, когда возникает потребность в передаче и сохранении информации, не касающейся «здесь и сейчас».



Письменность — это самый молодой способ коммуникации, около 6 000 лет до нашей эры появляются первые письменные системы. Вначале они достаточно примитивны — конкретный рисунок подразумевает конкретный объект, каждый такой символ называется пиктограммой, а письменность — пиктографией. Сохранились такие письменные свидетельства на разных материальных носителях — глиняных табличках, камнях, выделанных шкурах. Поздние образцы пиктографии называют клинописью, она существовала приблизительно до 70 года до нашей эры и носила в основном утилитарный характер подсчета. Примерно в это же время начинает появляться иероглифическое письмо.

Следующий шаг в развитии письменности происходит тогда, когда количество значков, обозначающих отдельные предметы, становится слишком большим. Более того, появляется необходимость фиксации каждого определенного языка. Таким образом, появляется идеограмма — письменность, кодирующая не материальные объекты, а их акустические элементы. Теперь каждый символ кодирует некое слово или часть слова. Например, символ, обозначающий «вол», теперь начинает использоваться и в словах «волынка», «волна», «волк».

Последней появляется силлабическая письменность — в ней идеографические знаки кодируют звуки слова один за другим. Это же называется и алфавитным письмом. Самое древнее алфавитное письмо — греческое. Кодирование всех звуков слова подряд делают чтение и письмо автоматическим занятием, к тому же имеющим только один вариант толкования. Платон и Аристотель отмечали крайнюю важность письменности, так как она позволяет сохранить речь и открывает простор для ее толкования или критики.

После появления письменности новые способы коммуникации перестают появляться. Инновация отныне проявляется лишь в изменении способов доставки (транспорта) этих традиционных видов коммуникации и их комбинациях между собой (но это уже носители информации, а не способы коммуникации).



УПРАЖНЕНИЕ 1

Какие способы коммуникации существуют?

- а) Попробуйте по очереди передать вашим одноклассникам простые сообщения: «это мой дом», «на охоте я добыл оленя» или «приближаются враги». Каждое сообщение можно передать разнообразными способами коммуникации, кроме письма. Вы сами можете их придумать.
- б) Придумайте ситуацию, в которой коммуникация с помощью музыки является наиболее эффективной.

История развития медиа

Как уже говорилось выше, любой из способов коммуникации имеет целью передачу какой-то информации. Вначале информация носит исключительно утилитарный и сиюминутный характер. Первобытный человек делится такой информацией: «этот фрукт вкусный и неядовитый», «этот зверь опасен, беги и прячься». В его языке недостаточно параметров, чтобы описать фрукт, которого нет в поле зрения, и уж тем более классифицировать его. С развитием языка развивается и абстрактное мышление, становится возможным говорить не только о вещах «здесь и сейчас», но и об отвлеченных, обсуждать не только происходящие события, но и события прошлого или будущего, а также гипотетические.

Стоит отметить, что также вне зависимости от способа коммуникации она может быть состоявшейся или нет, успешной, частично успешной или нет. Если один человек говорит только по-казахски, а другой — только по-норвежски, и у них нет возможности общаться с помощью жестов или изображений, скорее всего такая коммуникация будет несостоявшейся. Так же произойдет и в ситуации, если жесты в их культурах несут разную смысловую нагрузку (вы же знаете, что для отрицания болгары кивают головой, а для согласия — покачивают из стороны в сторону?). Частично успешной может стать коммуникация между носителями разных языков, которые тем не менее смогут как-то объясниться с помощью, например, английского языка.

Коммуникация играла важнейшую роль в формировании человеческого общества. Первобытные племена охотников и собирателей постепенно превращаются в более крупные образования («вождества»

или государства) с целью лучше координировать свои усилия. Экономические системы развиваются параллельно с развитием специализации и необходимости вести торговые отношения.

Способность общности укрупняться и развиваться зависела в первую очередь от социальной идентификации себя как ее представителя, что было бы невозможно без наличия письменной культуры. При этом важную роль в развитии государства играли и формы коммуникации. Так Месопотамия представляла собой более локальное государство из-за того, что носители информации были крайне несовершенны и плохо транспортабельны. А Египет с развитием более транспортабельных носителей информации приобрел больший территориальный охват. Вместе с тем Египет все еще пользовался менее совершенной пиктографической, а позже идеографической письменностью, поэтому государства, перешедшие на силлабическую письменность, достигли большего расцвета. Эту гипотезу разрабатывали канадский культуролог Маршалл Маклюэн и канадский экономист Гарольд Иннис, ее также называют «общественной зависимостью от коммуникативной эффективности».



Именно эти ученые и ввели понятия «медиа» — существует краткий афоризм Маклюэна: *Media is the message*, что можно перевести как «медиа — это само сообщение» или «носитель информации (посредник) и есть сообщение».

Исторически под медиа подразумевалась любая коммуникация, а под массмедиа — то, что относится к массовой коммуникации. Например, папирус с записью древнеегипетского торговца в счетную книгу «продал 10 рыб, купил мешок муки» будет считаться медиа (сообщением), направленным узкому кругу лиц, — себе и помощникам в лавке. А каменные таблички с законами Хаммурапи, выставленные на ознакомление всем жителям страны, — массмедиа. Если переводить это все на современный язык, то сообщение, отправленное другу, относилось к медиа, а сообщение, отправленное в школьный чат, — уже массмедиа. Однако с распространением интернета эти понятия стали синонимами.

Исторически самым древним письменным документом являются Тэртрийские надписи — глиняные таблички, найденные на территории современной Румынии и датированные в районе 5500 года до нашей эры. Предположительно, их содержание носит хозяйственный характер, следовательно, они попадают под категорию «медиа». Во всех только обретающих письменность культурах сначала под запись

отправляются данные для хозяйственно-экономических целей, и лишь потом — школьные, медицинские и юридические тексты. Наиболее крупным и известным первым памятником массмедиа являются таблички Хаммурапи, так как они уже адресовались неограниченному кругу лиц.

Далее на протяжении веков сохраняются различные памятники медиа (медицинские, научные, литературные и исторические тексты), а также массмедиа — объявления о торговле, изменениях законов, розыске преступников и так далее. Все появляющиеся медиа при этом доступны крайне ограниченному кругу лиц, а массмедиа носят нерегулярный характер.



Это интересно!

Первый каталог книг появился в III веке до нашей эры в Александрийской библиотеке. И именно принцип каталога лег в основу всех поисковых систем (Google, Yandex, Yahoo и т.д.).

Всему этому сопутствует эволюция медианосителя — вначале им является громоздкая и нетранспортабельная каменная плита, а затем появляются глиняные таблички, свитки, и наконец, кодексы.

Однако именно в эту эпоху зарождается почтовая связь — с возникновением рабовладельческих государств у правителей появляется необходимость получать свежую информацию о положении дел на подконтрольной им территории. Вначале почтовые сообщения носили преимущественно экономический и военный характер, однако известно, что в Древнем Египте богатые граждане пользовались своими рабами-курьерами, чтобы передать друг другу сообщения. Затем стали использоваться конные всадники, а также почтовые голуби.

Прародителями регулярных массмедиа являются древнеримские новостные сообщения, они рассказывали о произошедших в городе событиях, назывались *Acta diurna populi romani* («Ежедневные дела римского народа»). Они распространялись путем развешивания свитков в местах скопления людей, также знатные горожане и политики получали индивидуальный экземпляр переписанного от руки свитка. Именно в Древнем Риме и появилась первая платная профессия в сфере медиа: когда знатные римляне уезжали в провинцию, их корреспонденты узнавали важные политические и экономические новости и переправляли своим нанимателям.

Позднее в Древнем Риме появляется прообраз газеты. Интересно, что и регулярные газеты, и единая система почты возникают в одно

и то же время и усилиями одного и того же человека. Это римский правитель Гай Юлий Цезарь. Он обязывает распространять отчеты о заседаниях сената, донесения полководцев и послания правителей соседних государств. И он же распоряжается о создании единой государственной почтовой системы, которая позволяет связать самые удаленные уголки Римской Империи.

Первая печатная газета появляется в Древнем Китае — «Столичный вестник», возникший в VIII веке, содержал в себе указы императора и сообщения о важных событиях. Для получения печатной версии на досках вырезались иероглифы, затем доски покрывались тушью и прикладывались к листам бумаги для получения оттиска. Однако в Европе в эти годы и несколько столетий позже продолжают пользоваться исключительно рукописными массмедиа.

Важно отметить некоторые принципиальные характеристики европейского тиражирования. Во-первых, почти ни один древний автор не писал ничего сам — книги было принято диктовать секретарю, ведущему записи на табличках, покрытых воском. После правок и корректировок автора секретарь же переносил утвержденный текст на бумагу. Копирование чаще всего также проводилось под диктовку, только с развитием монастырской письменной культуры появляются индивидуальные копировальщики текстов.

Первоначальной формой таких записей являлся свиток. Это крайне сложная форма организации текста — приходилось удерживать написанное сразу с двух сторон, что значительно затрудняло работу сразу с несколькими свитками. Также существенным минусом свитка являлась невозможность сразу перейти к требуемому разделу текста. На смену свитку приходит формат кодекса — переплетенная и собранная книга, состоящая из отдельных листов пергамента (или иного носителя). Первоначально кодексом называли скрепленные вместе дощечки с воском, используемые в основном для черновиков или хозяйственного учета. Возможность писать на обеих сторонах и возможность перейти сразу к нужному разделу стали основными преимуществами кодекса. В I веке кодекс как форма использовался лишь в 17% латинских и 1% греческих манускриптов, а в V веке его доля достигает соответственно 100% и 96%.

Деление кодекса на устойчивые элементы (развороты) позволяло сделать чтение более частичным и, соответственно, было логичным шагом на пути к организации книжной навигации. Кроме того, кодекс легче было переписывать (можно было работать с книгой постепенно), а также можно было открывать на определенной странице.



УПРАЖНЕНИЕ 2

Носители информации

Каждый современный носитель информации так или иначе связан с носителями информации в прошлом. Составьте список из пяти-шести сайтов, которые вы посещаете регулярно. На что они больше всего похожи: на свиток, манускрипт, стену с петроглифами или на что-то иное? Обсудите ваши ассоциации вместе с одноклассниками.

Утром в газете, вечером в куплете

До появления печатного станка газеты распространяются по-прежнему в форме индивидуальных оттисков. Все меняется в 1450-х годах, когда Иоганн Гуттенберг изобретает печатный пресс. Это позволяет полностью отказаться от услуг переписчиков, стандартизировать форму и удешевить процесс.

В XVI веке в речи появляется слово «газета», от названия мелкой венецианской монеты «газетты», столько стоил листок с последними новостями. Можно сказать, что именно в Венеции появляются прообразы современных информационных агентств и платная профессия писателя новостей. Постепенно газеты стали публиковать не только новости политической жизни, но и частные объявления. Так, английский король Карл II с помощью объявления в газету нашел свою любимую пропавшую собаку. В 1700-х годах газеты стали публиковать и частные высказывания, похожие на современные газетные статьи. Параллельно с распространением газет набирает обороты и книгопечатание. Для бедных слоев населения, не умеющих читать, выпускают особый вид книги, где вся история рассказана с помощью картинок. Такая книга представляет собой по сути первый комикс.

Следующий шаг развития медиа происходит тогда, когда человек задается целью передавать информацию на расстояния. Вначале исполь-



Парадокс Гуттенберга

Изобретение печатного станка Гуттенбергом дало отсчет новой информационной революции и положило начало новой эре. Но, к сожалению, одновременно с массовой коммуникацией, массовым книгопечатанием и массовым словом появился и массовый обман.

зуется метод семафора — расположение приемопередаточных постов на достаточном для прямой видимости расстоянии. Таким образом каждый пост передавал сигнал следующему. Этот метод усовершенствовал француз Клод Чапп, создав систему линз, способную кодировать 195 различных символов. Для сравнения: на стандартной клавиатуре 104 клавиши, при этом для полноценного набора текста мы используем не только сами клавиши, но и их комбинации. Вначале оптический телеграф использовался только в военных целях для координации действий армии, затем его ценность понимают и торговцы — с помощью телеграфа передают котировки валют и сигналы о приходе в порт кораблей с товаром. Интересно, что само слово «сеть» вначале появляется именно в применении к линиям телеграфа, устроенным по принципу узлов связи.

Изобретение телеграфа радикальным образом изменило скорость коммуникации и саму скорость жизни. Что во времена Юлия Цезаря, что на пороге XIX века письмо из Парижа в Марсель, если его не вез отдельный гонец, шло в среднем 15-20 дней. А с изобретением телеграфа новость доходила за 15 минут!

Главным недостатком такой системы была ее полная зависимость от погодных условий и видимости. Поэтому ученые стали изучать принципы кодирования сообщений с помощью электричества. Большинство предложений строилось на том, что надо создать аппарат с количеством проводов, соответствующим количеству букв в языке. Однако это было крайне неудобно для передачи сообщений на других языках. Американский учитель рисования Самюэль Морзе предложил радикально новую систему — от всех проводов остался только один, все буквы кодировались с помощью его замыкания или размыкания. Универсальным языком телеграфа стала азбука Морзе.

Следующий глобальный рывок в скорости передачи информации произошел тогда, когда изобрели телефон. 14 февраля 1876 г. Грэм Белл получил патент на телефонный аппарат. Важно отметить, что телефон в отличие от телеграфа связывает собеседников напрямую, а не через посредника (оператора телеграфа). Интересно, что в отличие от всех предыдущих средств связи, которые в первую очередь обслуживали военные, государственные и экономические нужды, телефон использовался больше для личных разговоров. Из исследования телефонных разговоров в 1909 г.: 20% звонков — коммерческие заказы, еще 20% — звонки из дома на работу с распоряжениями, 15% — приглашения и 30% — просто «болтовня». С течением лет телефон все сильнее приобретает функцию социализации, в 1920-х даже появляется такое понятие, как «телефонный визит» — вместо личного посещения родственников с ними общаются по телефону.

До XIX века человечество могло сохранять только письменную информацию. С изобретением фотографии и фонографов становится возможным хранить и визуальную, и аудиальную информацию. Интересно, что изобретатели сохранения звука позиционировали свои аппараты как прообразы современных автоответчиков, автосекретарей и диктофонов, необходимых скорее для ускорения работы. Когда же устройства для воспроизведения звука стали популярны из-за воспроизводимой ими музыки, многие изобретатели были огорчены таким «бесмысленным» использованием.

Кино появляется во Франции в 1895 г. у изобретателей братьев Люмьер. В отличие от Томаса Эдисона, параллельно работающего с фиксацией на пленку движущихся объектов с научной целью, братья Люмьер сразу позиционировали свое изобретение как способ досуга. Почти все современные кинокомпании выросли из системы кинозалов — коммерсанты арендовали помещения и показывали там выкупленные или снятые их же компанией фильмы. Так появились киногиганты Парамаунт, Уорнер Бразерс, Метро Голдвин Майер (MGM), XXВек и RKO. Юниверсал, Коламбия и Юнайтед Артистс своих залов не имели, поэтому развивались намного медленнее.

В наши дни мы можем пойти, например, в «Кинопарк» и посмотреть там фильмы, снятые всеми компаниями, а в начале XX века за просмотром каждого фильма требовалось идти в кинозал той компании, которая сняла фильм.

Вначале кино было немым, затем стало звуковым. Интересно, что именно кинозалы стали приучать аудиторию к разнообразию жанров — перед самим фильмом или в перерывах показывали документальную хронику и новости.

Что касается радио, невозможно выделить одного человека, который бы изобрел радио. В странах бывшего СССР господствует теория, что радио изобрел А. Попов, Европа, Америка и весь остальной мир считают первым в этом Г. Маркони. И тот, и другой вариант являются упрощением, потому что и Томас Эдисон, и Никола Тесла и даже Бенджамин Франклин совершили ряд открытий, создающих возможность передачи радиоволн. Интересно, что радиосвязь в отличие от телеграфной линии и начали называть «беспроводной связью».

Как и в случае с радио, у телевизора нет одного установленного изобретателя — над его созданием трудились параллельно разные ученые из разных стран. Владимир Зворыкин, эмигрировавший в Америку, смог собрать разные технологии и добиться наилучшей четкости изо-

бражения. И в США, и в СССР стали создаваться системы вещания, но первый регулярный телеканал появился в 1934 г. в Германии. А Берлинская Олимпиада 1936 г.— первым событием, с которого велась прямая трансляция. В 1950 г. телевидение становится цветным, а в 1990-х годах появляются технологии цифрового вещания.

От телевизора к интернету

Первый ЭВМ (электронно-вычислительная машина) появляется в 1945 г., хотя разработки ведутся еще с 30-х годов. Он назывался ЭНИАК и весил целых 30 тонн. Только в 70-е годы появляются микро-ЭВМ «всего-то» с платяной шкаф. В 1976 г. на рынке появляется первый компьютер Apple. Эта же компания придумала мышку как способ управления компьютером и графический интерфейс (до этого взаимодействие с ЭВМ осуществлялось путем набора специальных команд на клавиатуре). В 1981 г. на рынок поступила тогда инновационная модель компьютера, которую согласно рекламе «было удобно носить с собой» — она весила «всего» 11 килограммов. Постепенно ноутбуки и компьютеры становились все компактней и легче. В 2010 г. появился первый планшет, он весил всего 680 грамм.

Разработка глобальной сети обмена данными началась в 1950-е годы. Прототип сети появился в 1969 г., как и многие другие изобретения, вначале он был поставлен на исключительно военную и государственную службу. Благодаря исследователю Тиму Бернерсу-Ли в 1984 г. появилась открытая для всех желающих сеть, что сделало возможным такие вещи, как электронная почта, мгновенный обмен сообщениями, телефонная связь по интернет-протоколу, видеосвязь, а также Всемирная паутина с дискуссионными форумами, блогами, социальными сетями и интернет-магазинами.

В развитии Всемирной паутины есть пока три основных периода развития:

- Web 1.0 был наиболее распространен в 90-е и начале нулевых годов. В этот период большинство сайтов были сугубо информационными, не содержали никаких интерактивных элементов, почти не было ни лайков, ни комментариев; диалоги между пользователями происходили редко, обмен файлами был длительным процессом. В те годы скорость работы сети была значительно ниже, порой интернет-трафик проходил

по линиям телефонной связи, что делало невозможным одновременно находиться в интернете и кому-то звонить. Основным местом общения были специальные разделенные по темам форумы и чаты.

- С появлением высокоскоростного интернета наступает эпоха Web 2.0 — пользователи активно делятся картинками, музыкой, видео. Скачивание файла происходит быстро, не перегружая линию. Сайты наполняются во многом пользовательским контентом, появляется возможность комментирования, зарождаются и развиваются социальные сети и мессенджеры. В эпоху Web 2.0 резко возрастает количество информации в сети, можно найти все и обо всех. Вместе с тем становится очевидным новый вызов — в такой сети почти невозможно сохранить анонимность.
- Когда смартфоны с высокоскоростным интернетом становятся доступными почти каждому пользователю и обеспечивают его присутствие в сети почти круглосуточно, начинается эпоха Web 3.0. Она характеризуется тем, что социальные сети почти полностью поглощают весь остальной интернет. В них теперь можно не только общаться, но и учиться, работать, смотреть фильмы, слушать музыку, заниматься творчеством и его продвижением, и так далее. В эпоху Web 2.0 каждый мог находить и распространять контент, в эпоху Web 3.0 каждый может производить контент сам и распространять на всемирную аудиторию. Активно развиваются и обучаются нейросети.



Домашнее задание

1. “Кодекс Хаммурапи” в переводе Якобсона В.А. (Хрестоматия по истории Древнего Востока. 1. М.: 1980. С.152-177) и в частичной обработке Немировского А.А. содержит 61 645 знаков. Вес носителя составляет 4 тонны.
 - а) Посчитайте, а сколько бы весила ваша любимая книга?
 - б) Узнайте у школьного библиотекаря, сколько приблизительно книг в библиотеке; посчитайте, сколько бы весила такая библиотека, если бы средний вес книги равнялся весу вашей любимой книги?
2. Интернет больше не является инновацией, он уже наша повседневность. А какую бы инновацию вы хотели бы получить в ближайшие 10 лет в области коммуникации и информации? А в других областях? Напишите ваш прогноз технологического развития до 2030 года.

ГЛАВА 2

МЕДИАПОЛЕ И МЕДИАГРАМОТНОСТЬ



Типы медиа

В современном мире понятия «медиа» и «массмедиа» почти не имеют различия. Более того, появляется новое слово — мультимедиа. Это такая технология, когда контент передается с помощью сразу нескольких средств — компьютерная графика, музыка, звук, брендированные товары, книги и так далее.

В развитии технологий существует такая закономерность — вначале появляется инновация (нечто новое, не используемое широким кругом людей), потом происходит проникновение инновации (в обществе начинают ценить технологию и большинство стремится ею обладать, а ученые в это время развивают инновацию и насыщают ее множеством функций). Наконец закрепление в повседневности (все, кто хочет получить доступ к технологии, имеют такую возможность). Как только технология закрепилась в повседневности, она перестает значительно изменяться и прогрессировать, освобождая научное и творческое пространство для будущих инноваций.

Рассмотрим это на примере интернета. Когда технология всеобщей сети только появилась, к ней имели доступ только ученые и ограниченный круг специалистов. С развитием интернета он стал представлять интерес и пользу для широкого круга лиц, так как у него появилась не только научная, но и практическая функция. Сейчас интернет закрепился в повседневности в большинстве стран мира, а в Финляндии доступ к широкополосному интернету даже признан неотъемлемым правом человека. Такая стадия развития науки, где место инновации в коммуникационном пространстве освободилось, позволяет предположить, что в ближайшие несколько лет мы увидим следующую ступень развития коммуникации.

Интересная закономерность: развитие коммуникаций шло по схеме «жест — речь — изображение — письменность», а развитие технологий идет в обратном порядке. Вначале для взаимодействия человек-компьютер использовалась письменность — с помощью клавиатуры пользователь вводил определенные текстовые команды. Далее появляется графический интерфейс — теперь большинство операций с компьютером проводится с помощью клика по «иконке», аналогу древней пиктограммы. Причем, вне зависимости от операционной системы большинство пиктограмм интуитивно понятны: так, шестеренка обозначает «настройки», а лупа — «поиск». Следующий шаг произошел, когда электронные устройства стали

управляться простыми голосовыми командами: мы просим Сири или Алису найти что-то в интернете, засесть время или подсказать погоду. Программисты во всех странах сейчас также разрабатывают электронные устройства, полностью управляемые с помощью жестов. Тем более что большинство жестов уже универсальны и понятны всем. Так, разведение в стороны сомкнутых указательного и среднего пальца обычно означает увеличение, а свайп — переход к следующему материалу.



УПРАЖНЕНИЕ 1

Реальность или фантазия?

Как вы думаете, существует ли уже такая технология или это пока возможно только в фантастических фильмах?

- 1) на 3D принтере можно напечатать жизнеспособные ткани и органы для человека;
- 2) с помощью программы на расстояние можно передать не только голос или картинку говорящего, но и некоторые его прикосновения (т.н. тактильный звонок);
- 3) заплечный ранец с двигателем позволяет его владельцу перелетать расстояния до нескольких километров;
- 4) изобретен принтер со специальными «ароматическими» картриджами, который позволяет пользователю на расстоянии понюхать любой предмет из каталога;
- 5) человеку можно пересадить целиком руку, ногу или голову и пересаженная часть тела будет полностью функционировать;
- 6) появились программы голографической связи, проецирующие целиком собеседников друг другу;
- 7) автопилот в современных автомобилях совершенен настолько, что водитель не требуется вообще;
- 8) нейросети, обученные на авторском стиле художника или музыканта, могут создавать абсолютно неотличимые произведения;
- 9) Если у человека есть генетическая предрасположенность к определенной болезни, врачи могут извлечь этот поврежденный участок ДНК и вставить на его место здоровый;
- 10) ученые создали бионических насекомых для мониторинга планет и для помощи людям, попавшим в зону стихийных бедствий;

- 11) с помощью улучшенной версии МРТ-сканера можно посмотреть, что снится человеку;
- 12) существуют бионические линзы для сверхчеловеческого зрения (приближение и отдаление по команде от мозга), также они способны записывать то, что человек видит, на чип, вшиваемый под кожу;
- 13) в некоторых городах начинают высаживать биолюминесцентные деревья с геном светлячков на замену электрическим фонарям;
- 14) ученые создали 5D диск размером чуть больше ногтя, но способного хранить 360 терабайт данных;
- 15) существует технология, позволяющая двигать курсор на экране силой мысли, которая считывается прикрепленными к коже головы сенсорами;
- 16) изобретены специальные линзы, воспроизводящие экран вашего смартфона или ноутбука прямо у вас перед глазами.

Как накапливалось знание

Как мы уже поняли, коммуникативные технологии развиваются по спирали: появляется что-то новое, активно совершенствуется, становится частью повседневности, освобождая место для очередной новинки. Теперь давайте проследим, как человечество реагирует на такие изменения в информационном обмене.

Мир информации древнего человека состоял из личного опыта (попробовал — не вкусно, больше есть не буду), опыта ближнего круга общения, переданного устно (еще бабушка говорила: бойся леопарда, он может тебя съесть) и широкого круга необъяснимых вещей. Чаще всего необъяснимые, непонятные, непонятые и непредсказуемые вещи пугают и создают дискомфорт. Поэтому социализированный человек старается всему найти объяснение. Так, древние люди объясняли гром — ударом богов, засуху — карой небес за то, что не приносили жертвы, а создание мира — рухнувшей с небес огромной черепахой, на спине которой мы все живем.

С первым витком развития науки некоторые закономерности стали более объяснимы. Открытия египетских, греческих и римских ученых позволили убедиться, что засуху можно победить человеческими сила-

ми с помощью грамотной системы орошения; были получены базовые знания о планетах и других небесных телах; значительно продвинулась медицина, в частности, было открыто кровообращение и роль в нем сердечных сокращений. Нельзя сказать, что человечество разом отказалось от мифов, но полученные знания помогли разобраться со многими заблуждениями.

На смену античному стремлению к точности приходит Средневековье, иначе называвшееся Темными веками. Многие античные достижения разрушены и позабыты, над стремлением постичь все с помощью разума начинает преобладать стремление постигать мир исключительно усилиями веры. Отвергнуты старые мифы, что солнце — это отдельный Бог, который проходит надо всей землей, теперь смена дня и ночи объясняется исключительно волей Божьей. Страшные эпидемии чумы и холеры снова объясняются карами, которые прогневали теперь единого Бога. Земля уже стоит не на черепахе, но абсолютно плоская и сотворенная опять же высшими силами. Вера творит собственные мифы, тормозя развитие науки.

Следующий этап разрушения мифов и торжества разума приходится на начало Возрождения и длится до начала-середины XIX века. В первую очередь, эта эпоха знаменита своими Великими географическими открытиями, окончательно позволяющими убедиться в объемной форме планеты. Медицина делает огромный прорыв — анатомы в деталях изучают человеческое тело. Множество важных открытий происходит в области физики и химии.

Однако за любым научным подъемом следует спад — он наступает в середине XIX века, когда уже многое изучено, но инструментов для следующего шага еще не изобретено. Это время характеризуется развитием псевдонаук — одна из них, френология, якобы находит закономерности между формой черепа и социальным поведением, другая, физиогномика, предлагает по чертам лица полностью определить характер и наклонности человека, третья, графология, искала возможность предсказания будущего человека по его почерку.

И снова развитие технологий смогло развеять мифы прошлого. Инновационные методы исследования и масштабный анализ доказали беспочвенность этих утверждений. Конец XIX — начало XX века стали эпохой так называемой технологической революции, человечество смогло отправиться в космос, научилось проводить сложнейшие операции и наблюдения за человеческим телом, разобрало окружающий мир буквально по атомам и собрало заново.

Такое количество исследований и открытий просто не могло не повлечь за собой новый этап отрицания. В нем-то мы и оказались в самом начале XXI века. Современные ученые называют это время эпохой постправды. Сложно предсказать, сколько продлится этот период, из истории видно, что лишь каждый следующий — короче предыдущего. Прошлый, в начале-середине XIX века длился где-то лет 50-70, поэтому есть надежда, что мы сумеем пройти эпоху мифов за 15-20 лет.

Помимо выделенной закономерности про накопление знаний и технологий существует такое наблюдение.

Эпоха древнего человека	Знание только у избранных
Эпоха античности	Полученные знания через публичные лекции доступны каждому заинтересованному
Эпоха Средних веков	Знание в книгах, книги только у избранных; публичных лекций не проводится
Эпоха Ренессанса и Нового времени	Книга доступна каждому заинтересованному, однако поля для собственных экспериментов нет
Эпоха лженаук	Собственный эксперимент может поставить каждый, общественной систематизации и верификации гипотез нет
Эпоха технической революции	Каждый может поставить собственный эксперимент, но только избранные могут донести его суть до массы
Эпоха постправды	Каждый может донести свою мысль до неограниченного количества людей и создавать собственный контент без особых затрат, формализованного контроля за его достоверностью и распространением нет

Что же такое современные мифы?

Это устойчивая вера, не опирающаяся на факты и часто противоречащая им, однако основанная на собственном убеждении в правильности происходящего. Вот несколько наиболее распространенных сегодня мифов.

- Теория плоской земли — лжетеория, согласно которой Земля имеет форму диска.
- Телегония — лжетеория, согласно которой все дети имеют биологический материал первого партнера матери, а не своего отца.
- Гомеопатия — лжетеория, согласно которой «подобное излечивается подобным» — в организм пациента вводят сильно разведенные препараты, которые якобы у здорового пациента и вызывают такое же заболевание.
- ВИЧ-диссидентство — лжетеория, согласно которой вирус иммунодефицита человека — выдумка, а СПИД вызывается неинфекционными факторами.
- Астрология — лжетеория, согласно которой положение небесных тел в момент рождения ребенка и в другие значимые моменты его жизни может повлиять на внешние обстоятельства.
- Экстрасенсорика — лжетеория, согласно которой человек может воспринимать реальность с помощью паранормальных чувств.
- Антивакцинация (антипрививочное движение) — лжетеория, отрицающая пользу прививок для иммунитета и считающая, что прививки могут вызвать аутизм и другие особенности развития.
- Абсолютная вредность ГМО — лжетеория, согласно которой все продукты с генной модификацией несут опасность и вред для человеческого организма.



УПРАЖНЕНИЕ 2

Медиаполе и медийная грамотность

Составьте вашу персональную карту медиа. Перечислите на листе бумаги все средства информации, с которыми вы регулярно взаимодействуете.

Схема расположения: в центре листа вы, а вокруг на разном расстоянии (в зависимости от частоты контакта) — разные медиа.

Попробуйте найти своего «единомышленника» — человека с максимально похожей картой.

Подумайте, какие источники информации прямо сейчас присутствуют в классе, с какими вы столкнетесь по дороге домой, с какими — уже дома.

Медиамир

Современный человек живет полностью в медиамире. От влияния источников информации почти невозможно укрыться. Медиа — это не только просмотр новостей или чтение ленты социальных сетей.

Важно понимать, что музыка, играющая в автобусе, — тоже медиа, рекламный билборд на обочине и даже объявление на столбе — медиа, футболка с надписью или принтом — медиа, даже модель телефона может являться источником информации. Каждую секунду человек получает огромный поток информации, большую часть которого он не отслеживает и сознательно не запоминает, однако эта информация может все равно откладываться в нашей памяти.

Совокупность всех медиа вокруг нас создает нашу медиасферу. Медиасфера у людей, живущих в одном пространстве и ведущих схожий образ жизни, выглядит довольно одинаково. То есть медиасферы каждого школьника Алматы очень похожи между собой, но будут иметь отличия от медиасфер каждого школьного учителя Алматы. Вместе они (медиасферы школьников и учителей) имеют много общего, но сильно отличаются от медиасфер школьников и учителей США.

В каждой медиасфере есть одна составляющая, которую мы не замечаем сознательно, и другая, которой мы активно пользуемся и за которой активно следим. Вторую, сознательную, называют медиаполем. А вот медиаполе у каждого ученика может быть абсолютно свое и непохожее на других. Например, ученик, интересующийся дизайном, будет отмечать для себя важным все то, что его интересует, а ученик, увлекающийся музыкой, полностью проигнорирует медиаполе первого, зато составит свое, с отдельным вниманием к звукам.

Медиамир и медиаграмотность

Информацию принято делить на фиксированные категории.

	Журналистика	Энтертейнмент
Цель	Информировать	Развлекать или вовлекать людей во время досуга в деятельность, в которой они пассивные участники
Методы	Верификация, независимость, ответственность	Story-telling, перформанс, визуальное искусство и музыка
Участники	Репортеры, фотографы, видеооператоры, редакторы, продюсеры	Писатели, актеры, художники, музыканты, дизайнеры
Результат	Усиливает гражданскую информированность	Отвлечение граждан от повседневной жизни. Изменение или критика социальных норм

Таблица Журналистика и ее соседи

Промоушн	Пропаганда	Сырая информация
Продавать товары, продвигать талантливых людей, чтобы привлечь к ним потребителей	Выстроить массовую поддержку для идеологии путем канонизации лидеров и демонизации оппозиции	Обойти институциональные фильтры и затраты на распространение, чтобы иметь возможность продвигать точку зрения и информировать
Оплаченная реклама, PR, пресс-релизы, публичные заявления, постановочные события, спонсорство, продакт плейсмент, веб-сайты, виральные видео	Односторонняя или сфальсифицированная информация, основанная на эмоциональных манипуляциях, апеллирует к ценностям большинства	Facebook, Twitter, YouTube, блоги, веб-сайты и комментарии на них, сетевая рассылка, флаеры, граффити
Рекламные агентства, публицисты, эксперты PR, официальные публичные лица	Политики и организации	Любой человек с доступом к интернету, фотооборудованию или иным любительским путям распространения информации
Рост продаж продуктов или услуг, зарабатывание денег теми талантами, которые промоутируются	Помогает идеологическим группам захватить и удержать власть, влияя на публичное мнение и мотивируя их действовать в удобном ключе	Самовыражение или любительское производство энтертейнмента, промоушена, защиты общественных интересов или пропаганды



УПРАЖНЕНИЕ 3

Как ориентироваться в этой таблице:

Задайте себе вопросы, какую главную цель преследовал автор материала? Какие методы он использовал? Где размещена информация? Ответы на эти вопросы помогут легко сориентироваться в таблице и соотнести информацию с правильным ее видом. При этом абсолютно не значит, что только журналистика — это хорошая и правильная информация, полезной может быть любая из категорий. Главное — отдавать себе отчет, с каким типом информации мы имеем дело и чего автор материала на самом деле хочет от нас.

Как уже говорилось выше, в современном мире, эпохе постправды, распространено множество мифов. Миф — это по сути целая альтернативная вселенная со своими законами, отличающимися от нашей реальности. Каждый миф поддерживается с помощью пропаганды и десятка фейков.



Фейк — это ложная новостная история или визуальный материал, затрагивающий общественно важные темы, созданный для массового распространения онлайн с целью увеличения трафика или дискредитации общественного движения, публичной персоны, политической кампании и т.д. Журналистская утка будет обладать всеми признаками фейка, с уточнением, что создается исключительно журналистом и распространяется изначально в СМИ, поэтому выделять её в отдельную категорию нет необходимости. Помимо фейка есть еще две сходных категории.



Сплетня (слух) — бытовой неподстроенный разговор или сообщение о других людях, включающее неподтвержденные сведения.



Пранк — намеренная шутка или розыгрыш.

Стоит отметить для начала сходства этих категорий: все они, хотя и могут быть созданы журналистами, чаще всего создаются обычными людьми; их предмет — недостоверная и/или искаженная информация; процесс создания не требует от автора наличия специальных знаний или квалификаций. Различия между ними представлены в таблице ниже.

Параметр	Фейк	Сплетня	Пранк
Намерение	Есть	Может отсутствовать	Есть
Задача	Массовая дезинформация	Дискредитация личности	Развлечение, получаемое в результате раскрытия правды
Вид создания	Создается с использованием технических средств коммуникации	Создается в ходе устной коммуникации*	Может создаваться как в ходе устной коммуникации, так и с использованием технических средств
Как развивается	Не изменяется при передаче	Могут появляться новые детали	Передача отсутствует, так как пранк адресован чаще всего конкретному человеку
Аудитория	Потенциально неограниченная	Ограничена кругом личных взаимодействий автора/ субъекта. При публикации сплетни в медиа аудитория стремится к неограниченной	Отдельный человек или группа лиц. При публикации пранка в медиа аудитория стремится к неограниченной

** Под устной коммуникацией подразумевается как устная речь, так и письменная, работающая по законам устной (например, чаты).*

Важно отметить, что авторы фейка и сплетни всегда стремятся, чтобы их информация до последнего принималась за истину. В отличие от

них автор пранка заранее готов разоблачить себя, его цель — ввести аудиторию или объект розыгрыша в заблуждение лишь на время, а затем сообщить ей, что информация не соответствовала действительности.

Для того, чтобы не стать жертвой фейка, сплетни или пранка, необходим определенный комплекс навыков. Такие навыки бывают двух типов — фактчек и верификация. В следующих главах будут подробно рассмотрены инструменты каждого.

В таблице представлены основные различия между фактчеком и верификацией.

Параметр	Фактчек	Верификация
Кому выгодно?	Всем окружающим	Самому человеку
Предмет	Информация, массово распространённая с помощью технических средств	Любая информация
Что нужно знать?	Законы функционирования медиа и методы работы с информацией	Нет необходимости в специальных знаниях
Задача	Приведение информационного пространства в соответствие с реальностью путем установления достоверности информации	Установление достоверности или уточнение информации
Продукт	Новое знание	Уточнение старого знания

Навыки верификации и фактчека лежат в основе такого понятия, как **медиаграмотность**. Под этим термином в современном мире подразумевают совокупность знаний, помогающих пользователю анализировать и оценивать достоверность полученной информации. Для развития медиаграмотности ключевым навыком является критическое и аналитическое мышление — умение задавать себе вопросы не только

о содержании информации, но и сопоставлять с ранее полученными сведениями. Помимо работы с уже полученными знаниями в ключевые умения, формируемые медиаграмотностью, входит поиск информации с максимальной скоростью и точностью.



Домашнее задание

1. Опросите своих родных и друзей, в какие из современных мифов они верят. Не раскрывайте им сразу, что это миф. Попробуйте такой подход — ознакомьтесь с доводами сторонников каждой теории, а затем расскажите им, что прочитали и спросите их мнение. Если они легко соглашаются с доводами лжетеории, попробуйте поменять позицию и начать разрушать мифы. Будут ли они настаивать на своем и приводить аргументы в защиту? Попробуйте посчитать, сколько из них верят в каждый из мифов. Обсудите в классе полученные данные. Если кто-то из родных и друзей твердо убежден в своей вере в лжетеории, дайте им почитать этот учебник.
2. Подумайте, какие фейки, сплетни и пранки вы встречали в реальной жизни. Объединившись в группы, подберите каждой группой в новостных лентах по три-четыре материала, подходящие под категории фейка, сплетни или розыгрыша. Обязательно наличие всех трёх категорий(!). Представьте заголовки материалов вашим одноклассникам, пусть они попробуют распознать, что именно — фейк, сплетня или розыгрыш — кроется под броским заголовком.

ГЛАВА 3

**ФЕЙК И ФАНТАЗИЯ:
ЧЕМУ МЫ ВЕРИМ И ПОЧЕМУ**



Задумывались ли вы, почему мы порой верим герою фильма больше, чем своим близким? Как мы воспринимаем «высокий обман» (так часто называют искусство) и как он на нас влияет? В этой главе мы попробуем разобраться с вопросами, с которыми мы сталкиваемся ежедневно.

Вымысел в искусстве: кино, театр, тексты

Слово «манипулятивный» имеет естественное негативное значение. Манипулировать — это не просто убеждать, оно подразумевает контроль над мнениями или даже жизнью человека. Поэтому, когда мы говорим о манипулирующих персонажах в истории кино, сразу же думаем о злодеях. Хороший парень не манипулирует; он убеждает или влияет своим примером.

Тем не менее в кино, театре или даже в книгах плохие или хорошие персонажи не становятся такими случайно. Они созданы писателями, режиссерами, сценаристами. Все эти люди обычно остаются за кадром, а зрители остаются очарованными персонажами. Есть один очень интересный парадокс. Когда мы идем на популярное театральное представление или в кино, выбираем роман или детектив, мы обычно заранее знаем, что эти истории не настоящие. Это плод чьей-то фантазии. Но чем больше эта фантазия убеждает нас в своей реальности, тем больше мы отдаемся эмоциям и влиянию творцов. Посмотрев интересный фильм или прочитав роман талантливого писателя, мы непроизвольно формируем мнение о Героях и Антигероях. Однако, если бы мы задали себе несколько вопросов и обратили внимание на ряд важных деталей, то поняли, что иногда мы излишне героизируем одних и превращаем других во врагов и «плохих парней». Всего лишь потому, что нам страшно даже подумать, что зло может победить, особенно в кино, где плохой парень почти всегда проигрывает в конце.



УПРАЖНЕНИЕ 1

Вспомните самых известных героев фильмов, которых вы знаете, и ответьте на несколько вопросов:

Какие эмоции вызывают у нас персонажи:

1. Почему наш герой такой позитивный и добрый (или наоборот — злой)?

2. Фильм показывал всю его жизнь или только некоторые детали?
3. Почему фильмы часто показывают хорошее и плохое с исключительными особенностями: некоторые герои злы, ревнивы, предатели, лжецы и даже физически безобразны (особенно в фантастических фильмах, таких как «Властелин колец»), в то время как другие чувствительны, самоотверженны, спешат помочь, искренние и даже ангельски красивые (например, эльфы, ангелы и т. д.)?



УПРАЖНЕНИЕ 2

Как вы думаете, насколько образы в искусстве связаны с реальностью?

Вы много раз в кино и в анимационных фильмах видели викингов. Опишите, как выглядят викинги и каковы их характеристики, во что они одевались?

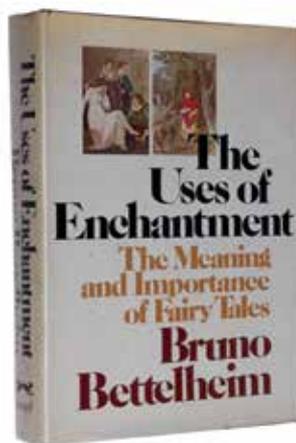
Знаете ли вы, как на самом деле выглядели шлемы викингов?

Давайте попытаемся осветить некоторые технические детали, которые заставляют нас верить в определенные вещи в искусстве и даже не думать о других важных вещах. И начнём с прародительницы любого искусства — сказки.

Чем отличаются сказки для детей и для взрослых

Немецкий поэт Фридрих Шиллер однажды сказал: «Истории, которые я слышал в детстве, имеют более глубокий смысл, чем уроки жизни».

Один из самых известных исследователей и аналитиков сказок был психоаналитик, доктор Бруно Беттельгейм. Он написал широко известную книгу «Польза от волшебства». В этой книге ученый анализирует сказки и механизмы их влияния.



Он помогает нам понять, почему они так важны для нашей несовершенной цивилизации.

Давайте попробуем вспомнить ваш опыт изучения литературы и ответить, что такое традиционная сказка?

По сути — просто история с более или менее строгой моралью в конце. В ней существуют магические силы, заклинания и магические существа — феи, волшебники, великаны, драконы или единороги. На протяжении веков сказки выполняли одну главную задачу — морального воспитания подрастающего поколения.

Сказки, созданные для детей, помогают им запомнить основные правила, принятые в определённой культуре. Они подобны путеводителям, сводам универсальных культурных правил.

Детские сказки как терапия

Бруно Беттельгейм считает, что родители часто совершают ошибку, защищая своих детей от суровой реальности. Ведь действительно сказочные ужасы могут помочь понять, что ждет человека в жизни, которая отнюдь не безмятежна.

Сказочные персонажи делятся на хороших и плохих, чтобы ребенку было легче различать их. Например, два брата умные, но бессердечные, а третий глупый, но хороший. Такая поляризация и счастливый конец сказки помогают ребенку отождествиться с сочувствующим, хорошим героем. Но есть и тип сказок, которые не осуждают героя даже если он обманывает злодея или ворует что-то у злого великана. Таким образом фиксируется модель, в которой и слабый человек может победить, если он умен.

Вторая важная цель сказок — обогатить жизнь, пробудив воображение. По словам Бруно Беттельгейма, это формирует интеллект и очищает эмоции. Помогает понять проблемы, с которыми человек сталкивается, и показывает, как их можно решить.



Это интересно!

Различные испытания героев, например, отражают обычаи общества. Например, крупное событие в мировых культурах, такое как переход или посвящение мальчиков и девочек во взрослую жизнь. Чтобы стать мужчиной или женщиной в традиционных культурах, нужно преодолеть некое препятствие, называемое *посвящением*.

Нужны ли сказки для взрослых?

Возрастающая популярность телевизионных реалити-шоу и сериалов показывает, что многие люди хотят верить или хотя бы представить, что можно создать некий совершенный мир.

Когда мы говорим о созданном творцом-человеком мире, мы обычно имеем в виду его прекрасную сторону. Мы счастливы, когда герои, преодолев препятствия, получают награду в виде руки принцессы или половины королевства. Начинается праздник, и все живут долго и счастливо. Но до счастливого конца еще предстоит пройти долгий путь — бороться за жизнь, обманывать демонов или гигантов и так далее. Если так рассудить, по большей части эти истории — не более чем фильм ужасов.

Режиссер Дэвид Кроненберг говорит, что наши детские страхи совпадают со страхами взрослого. Только когда мы становимся взрослыми, мы понимаем их иначе. Но это все еще страхи. Поэтому фильмы ужасов и сказки связаны не только с тем, что сюжетные линии таких фильмов часто создаются с использованием сказок, легенд или мифов разных стран. Они помогают зрителям всех возрастов преодолевать глубинные фобии. Это одна из форм психотерапии, которая утверждает нас в мысли, что нам повезло больше, чем персонажам фильмов. Так что фильмы ужасов или фэнтези для взрослых — это и выход из реальности, и лекарство.

Музыка и эмоциональные манипуляции в кино

Использование музыки в фильмах — это секретное оружие, которое продюсеры используют, чтобы манипулировать нашими эмоциями и формировать нашу реакцию на историю. Одни и те же кадры могут показаться романтическими, грустными или даже зловещими из-за выбора музыки. Могут возникать более тонкие градации эмоций.

Небольшое личное размышление подтвердит, что музыкальное произведение может изменить то, что мы чувствуем в течение всего нескольких секунд. В реальном мире мы не окружены музыкой, у нас нет таких ярких эмоций при наблюдении за людьми или окружающей средой. Хотя мы можем эмоционально реагировать на окружающие звуки, например, пение птиц, но наши чувства не связаны с его реальным назначением или его значением для издающего звук существа. Кроме того, музыкальные звуки имеют гораздо более яркую структуру, чем естественные звуки. Существенные параметры включают в себя не только мелодию и ритм, но также качество звука (тембр), гармонию и тональность (мажорную или минорную).



Несмотря на некоторые исключения, музыка, которая вызывает счастливые или положительные эмоции, более вероятно будет в мажорной тональности и в быстром темпе. Меланхоличные, миролюбивые или романтические пьесы, как правило, либо медленные, либо в минорных тональностях, либо в обеих. Музыка, предназначенная для испуга, часто нерегулярна по ритмам и подвержена большим изменениям динамики.

Различные аспекты музыки обрабатываются в разных областях мозга. Там, где есть ритм, мы чувствуем желание постучать, кивнуть или даже танцевать. Однако большая загадка — влияние музыки на ментальные и физические измерения наших эмоций. Наши психические реакции могут быть связаны с физическими реакциями, такими как увеличение частоты сердечных сокращений, изменение кровотока и ощущение покалывания волос на коже. Почему это так эффективно остается загадкой, так как некоторые из особенностей музыки (например, гармония) являются недавними человеческими изобретениями и не могли сыграть никакой роли в формировании эволюции нашего мозга.

Наконец, в фильме одна из самых интересных особенностей, как это ни парадоксально, — использование тишины или окружающих звуков для сопровождения большей части истории (так, один из самых ярких и жутких фильмов братьев Коэнов «Старикам тут не место» вообще поставлен без музыки). Очень часто в кино используют полную тишину перед экстремальными событиями. Чем дольше тишина, тем напряженнее эмоции. Любое внезапное действие и исключительно громкий звук вызывают чрезвычайно сильные эмоции. Это давно известный трюк для создания драмы на экране или сцене.

История кино. Как повлиять на людей за 50 секунд?

Короткометражный фильм 1896 г. «Прибытие поезда на вокзал Ла-Сьота» (<https://www.youtube.com/watch?v=0YSJ31wMmXc>). Безмолвный фильм длиной в 50 секунд был создан Огюстом и Луи Люмьерами, которые были одними из первых, кто создал движущиеся картинки. Вы, вероятно, слышали какую-то версию истории об этом фильме. Если бы мы поверили во всемирно известную историю, то, когда тихое черно-белое изображение движущегося локомотива заполняло экран фильма в Париже, люди в киноте-



атре думали, что он собирается въехать прямо в них. Они запаниковали и бросились к выходу.

Многие из ранних работ братьев едва ли можно было классифицировать как фильмы даже в то время, в основном это были короткие фрагменты. Этот фильм запоминается среди всех остальных 1400 одноминутных фильмов. Сам фильм — сцена на платформе поезда. Черный паровоз тянется к камере, установленной близко к краю рельсов. В этом фильме четко видна идеальная сцена поезда, въезжающего на станцию. С точки зрения человека, ожидающего на платформе, стоящего рядом с рельсами, локомотив входит в раму с правой задней стороны и движется к левому низу. Фильм был прекрасен своей простотой и способностью привлечь зрителей к действию на экране.

Слово против технологии

Мир меняется, и детям больше не нужно читать сказки. Они играют в игры на компьютерах, и у них обычно есть мобильный телефон вместо книги. Тем не менее, писатели настойчиво пишут сказки. А в некоторых случаях они поражают успехом. Создатель серии «Гарри Поттер» доказал скептикам, что в наши дни слово все еще преобладает над технологиями.



Домашнее задание



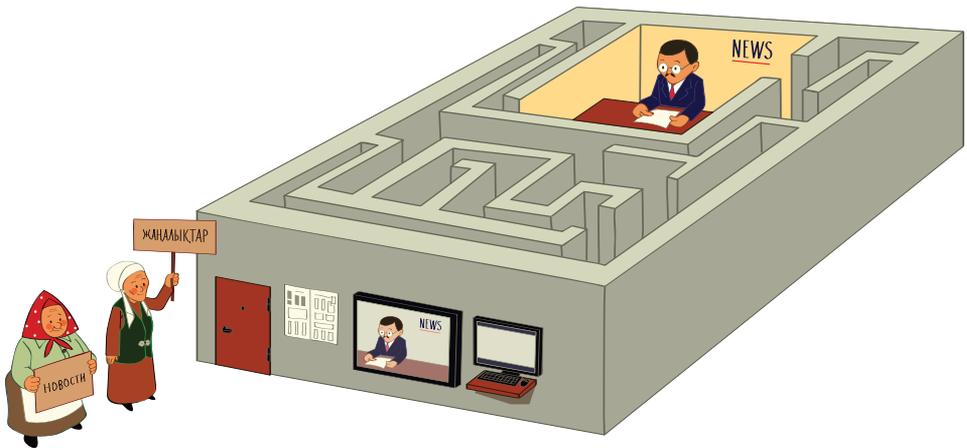
1. Посмотрите ролик, снятый журналистами «Настоящего времени» по ссылке <https://youtu.be/VImBE5z3L7Y>

Обсудите с учителем следующие вопросы:

- Как искусство связано с производством фейков и фейковых новостей?
 - Воспринимаем ли мы прошлое таким, каким оно было на самом деле?
 - Можем ли мы вообще говорить о том, какими были «на самом деле» события прошлого?
2. Объединитесь в группы по три-четыре человека и снимите ролик, в котором один из вас будет читать стихотворение. Наложите на ролик музыку и покажите в классе. Обсудите разницу восприятия роликов с музыкой и без неё.

ГЛАВА 4

ИНФОРМАЦИЯ. ИСТОЧНИКИ ИНФОРМАЦИИ



Информация и ее признаки

Слово «информация» мы слышим каждый день. Но большинство обывателей выступает в роли простых пользователей, отождествляя информацию со знакомыми действиями, связанными с ней.

Что же такое информация?

Новости, которые мы слышим, знания, которые черпаем из книг и учебников (независимо от носителя), кино и видео, фото, которое делается на смартфон, сообщения в мессенджерах, мейлах и т.д. – все это информация.

Но как описать саму информацию? Любой предмет или явление представляется нам по тем или иным деталям, штрихам, признакам. Давайте опишем самый простой предмет, например, яблоко. Что о нем можно сказать? Яблоко круглое, иногда продолговатое, красное, зеленое или желтое, сочное или мясистое, вкусное или нет, летнего или осеннего урожая, мягкое или твердое, растет на дереве, в нем много «железа», имеет гладкую кожуру и т.д.

Мы описали признаки яблока, по которым четко можем сказать, что это именно яблоко, а не другой фрукт. По аналогии попробуем обозначить признаки информации.

Они могут быть следующие:

- актуальная, важная;
- правдивая и неправдивая;
- научная, новостная, бытовая;
- быстро передается и создается;
- доступная и недоступная;
- интересная и неинтересная;
- игровая и серьезная;
- забывается, записывается, хранится, удаляется, теряется;
- подделывается, искажается;
- воздействует на людей, вызывает разные эмоции;
- бывает в виде звука, картинки;
- и т.д.

Как видим, на первый взгляд, признаков очень много. Признаки яблока можно объединить в своеобразные группы: по вкусу, по цвету, по качеству и т.д. И мы можем систематизировать эти признаки и сформулировать семь главных признаков информации — *ценность, влияние, гибкость, репродуктивность, логичность, интерактивность, проверяемость*.

Признак	Описание
Ценность	Касается непосредственно вашей жизни. То есть, данная информация именно для вас имеет определенную ценность
Влияние	Побуждает к действиям. Может влиять как на одного человека, так и на большое количество
Гибкость	Под воздействием аргументов или других обстоятельств – например, научных открытий, которые опровергают или уточняют уже имеющиеся данные, информация изменяется, или «изгибается»
Репродуктивность	Информация может бесконечно копироваться, изменяться, дополняться, восстанавливаться
Логистичность	Как бы ни изменялись средства передачи информации (жест, картинка, речь, письмо) и технологии передачи (радио, ТВ, Интернет) информация приспосабливается к разным каналам и способам передачи
Интерактивность (масштабируемость)	Информация может существовать в разных формах и масштабах. Суть текста объемом в несколько страниц можно передать в нескольких слайдах или коротком видео
Проверяемость	Информацию можно уточнить, проверить, опровергнуть, показать, что она правдива или наоборот – лжива, доказательна или необоснована

Искажение признаков информации и его последствия

Ни для кого не является секретом или открытием, что информацию сегодня используют очень часто не только для информирования, создания новых знаний, позитивных продуктов, но и в негативных целях. Более того, сегодня в обиход вошли такие понятия, как информационная война, информационная атака, пропаганда, манипуляция, фейк – понятия, связанные с использованием информации, но несущие негативный смысл, преследующие далеко не позитивные цели.



УПРАЖНЕНИЕ 1

Злоупотребление информацией

Назовите примеры негативного использования информации (не вдаваясь в детализацию, определите, что это за вид злоупотребления информацией). Зафиксируйте примеры в тетрадах, на доске или флипчарте.

Вышеуказанные понятия – от информационной войны до фейка – несут негативный смысл. Фейк – это плохо, манипуляция – это плохо. Все это искажение, искривление, игра информацией, говорим мы, обобщая данные отрицательные явления. Но информация становится неправильной или негативной не просто так – изменяются в негативную сторону ее признаки. И уже они придают сообщениям, новостям, публичным заявлениям негативный окрас.

Разберем пример

У нас есть очень интересная и редкая книга. Она находится, к примеру, в библиотеке. Чтобы ее прочитать, люди записываются в очередь на месяцы вперед. Но в один момент кто-то умудрился сделать фотокопию этой книги и выложил ее, к примеру, в группу в одну из соцсетей. К чему это приведет? В библиотеку никто не пойдет, не будет записываться в очередь на прочтение на месяц вперед, а просто откроет ноутбук и прочитает тогда, когда будет удобно.

Но через какое-то время 10 человек, решили: о, а я тоже могу написать что-то подобное – к примеру, аналогичную историю, но чуть с другими героями, чуть с другими деталями. Через месяц в сети появилось 10 других подобных историй, которые все решили прочитать – кто из-за интереса к жанру, кто чтобы сравнить, а кто потому что все читают и все об этом говорят.

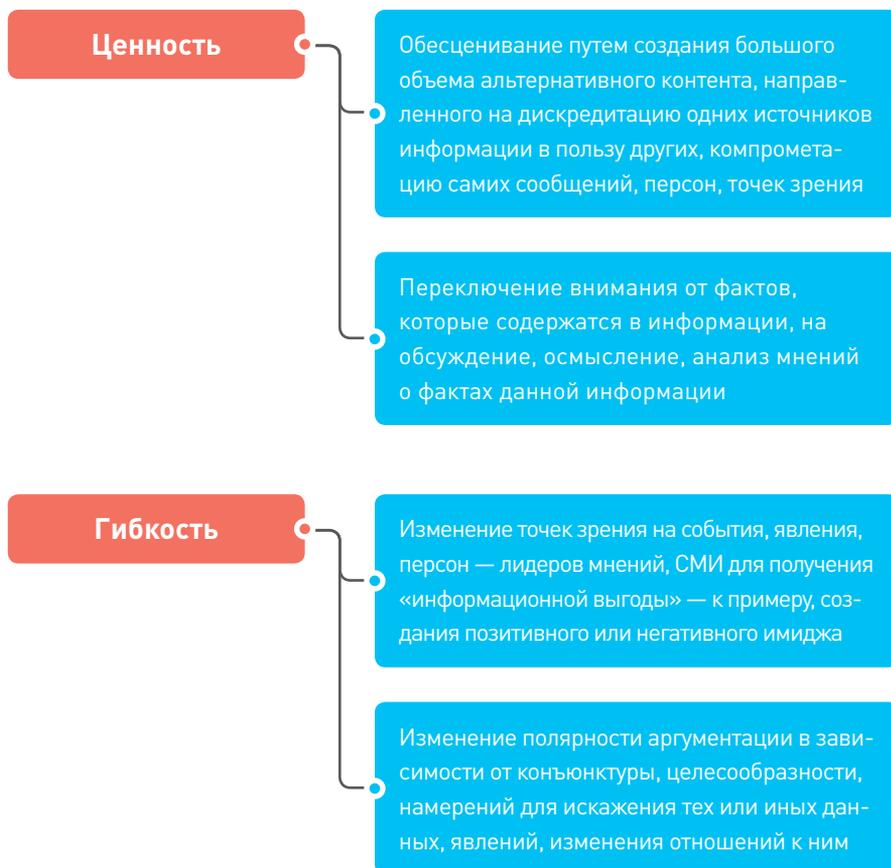
Чтобы поделиться впечатлениями, читатели создали несколько групп, где стали обсуждать новые книги. Кто-то был доволен, кто-то нет. А 15 человек сказали, что они напишут свои версии историй, так как предыдущие 10 их не устраивают. Прошло два месяца и появилось 15 новых версий 10 историй второй волны.

Вопрос: что стало с той самой первой книгой? Внимание к ней обесценено появлением ее новых версий, аналогов новых версий, доступностью как ее самой, так и «клонов», созданием вокруг интереса к обсуждению героев и обстоятельств со слов тех, кто читал, нежели к самостоятельному чтению.

Вспомним, что одно из ключевых свойств информации есть ее **ЦЕННОСТЬ**. На данном примере можно увидеть механизм обесценивания информации. То есть, воздействуя на один из признаков информации, мы меняем смысл / значение / акценты самой информации.

Негативное воздействие может происходить на любое из свойств информации, чтобы добиться ее «искажения / искривления» в нужном формате, векторе, направлении. Все зависит от целей, которые ставит перед собой тот, кто решает это сделать.

Схема использования свойств информации для придания негативного смысла самой информации



Влиятельность

Создание информационного шума — отвлечение внимания от главной новости / события путем создания потока псевдоинтересных сообщений, не имеющих ценности для пользователя

Системный вброс деструктивных альтернатив того или иного важного сообщения, которые подрывают доверие к фактическим данным и понятиям, заставляют реагировать в рамках нужной модели поведения

Побуждают к запрограммированным действиям (часто негативным) путем системного наполнения потока информационных сообщений призывами, пропагандой, обещаниями, угрозами

Репродуктивность

Системная генерация новых информационных сообщений, создание регулярных информационных волн, что сводит к угрожающему минимуму возможность критического анализа событий, их последствий, формирует искаженное представление о событиях, явлениях, персонах

Логичность

Создание новых каналов и технических возможностей транспортировки информации для массового охвата потенциальной аудитории с целью воздействия на нее

Интерактивность

Минимизация объемов сообщений, упрощение формата сообщений, уменьшение объемов анализируемых фактов в сообщении, усиление воздействия на эмоциональную часть восприятия информации (к примеру, через визуализацию)

Проверяемость

Уменьшение возможностей проверки данных, формирование такого отношения к информации, которое не побуждает к самостоятельной проверке данных, укрепление доверия к мнению о факте, а не к самому факту



Домашнее задание

Заведите личный медиадневник для исследования персонального медиаполя. В течение 10 дней фиксируйте в дневнике следующие данные:

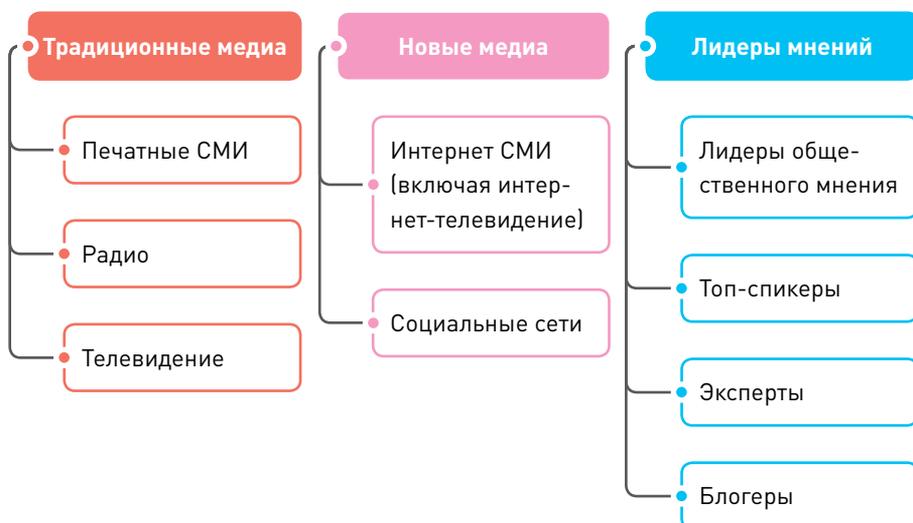
- сколько новостей вы услышали за день (записывайте даже те, о которых сможете вспомнить только отрывочные факты);
- сколько новостей вы просмотрели/прочитали самостоятельно (учитываются и просмотры только по заголовкам);
- сколько новостей вы прочитали полностью;
- распределите новости по следующим каналам получения:
 - а) телевидение
 - б) интернет-медиа
 - в) печатные медиа
 - г) радио
 - д) через ленту новостей в смартфоне
 - е) в пересказе от кого-то.

Через 10 дней резюмируйте собранные данные, представьте свое медиаполе и обсудите его с одноклассниками и учителем.

Современные источники информации и их признаки

Если мы говорим об информации не как о знаниях, а рассматриваем ее в разрезе информирования нас о событиях, интересных явлениях, наших увлечениях и хобби, каких-то изменениях или анонсировании чего-либо, то современный мир дает нам широкую возможность выбрать удобный для нас источник. И независимо от возраста, географии, персональных пристрастий, образованности, технической подкованности мы можем найти именно то, что будет удовлетворять наши потребности в получении информации.

Современные источники информации можно условно разделить на три группы:



Деление действительно условное, так как грань между источниками достаточно узкая и очень часто один источник является симбиозом или продуктом другого.

Как видим, третья группа фактически является продуктом (а часто и наполнением) второй группы (возможно, за исключением топ-спикеров и экспертов, которые присутствуют и в первой группе как ретрансляторы информации).

Если данные источники информации объединены в группы, то, вероятно, у них есть какие-то общие черты, признаки, свойства, а между источниками разных групп, соответственно, различия. Для того, чтобы было в этом

легче разобраться, стоит оценить и описать указанные группы по общим критериям, к примеру, популярность, охват аудитории, достоверность/доверие, доступность/мобильность, возможность участия пользователя.

Что такое «информационная деревня»

Анализ современных источников информации и их признаков показал, что наряду с рядом позитивных сторон – доступностью, удобством, мобильностью и т.д. – они имеют (особенно те, что относятся к категории новых медиа) и негативные стороны. Как минимум, явно прослеживается одна из них – низкая степень достоверности / проверяемости и, как следствие, доверия к информации.

Еще один фактор, который может быть использован в негативном аспекте, – практическая полная доступность для любого пользователя. Мы говорили, что современные медиа имеют широчайший охват аудитории, они мобильные и гибкие – изобретаются все новые и новые каналы и формы транспортировки информации. К примеру, если еще 6-7 лет назад на пике были текстовые блоги, то на рубеже 2013-2014 гг. их вытеснили видео-блоги. Если на заре появления Telegram это был мессенджер для коммуникаций, то сейчас в нем появился информационный функционал – Telegram-канал. Ещё вчера в Instagram мы только делились фото, а теперь используем его и для переписки.

Поэтому не быть в информационном поле сегодня практически невозможно – логистика информации такова, что, как вода, проникает в любую щель, где есть лазейка доступа.

Почему же мы подразумеваем некую скрытую угрозу при этом, ведь, на первый взгляд, все делается для удобства пользователя? Но так ли это? Можем ли мы как пользователи иметь гарантии получения достоверной информации в удобной форме?

Возможность получения нами как пользователями достоверной информации в удобной и понятной форме зависит как от нас самих, так и от медиа, который ретранслируют ее.

Почему? Когда мы изучали группы современных медиа, то констатировали, что их порядка 10 только основных. Второй момент – охват и объем информации, которой они заполняют информационное поле, – огромный. Мы имеем возможность знать о событиях, удаленных от нас на тысячи километров, пользоваться ресурсами и данными, находящимися на другом конце света. Это создает так называемый парадокс «информационной деревни».



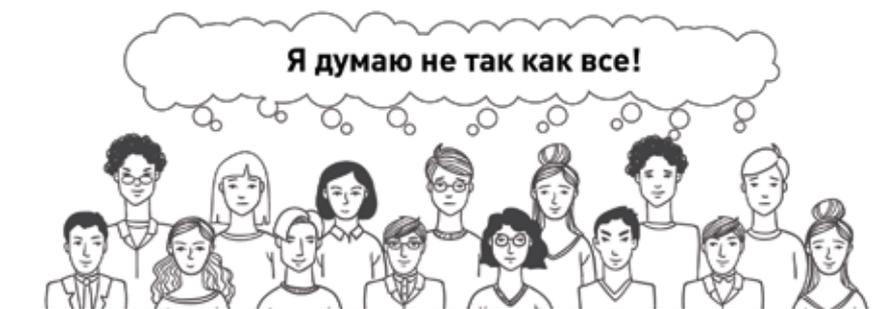
Разминка

Попробуйте вспомнить и записать, какие последние новости за неделю вы можете назвать о событиях: 1) в мире, 2) в стране, 3) в вашем городе. Различается ли количество новостей?

Современные технологии и сегодняшнее информационное поле позволяют нам быть в курсе сотен событий, которые происходят не только рядом с нами, но и на другой стороне света. Мы знаем о недавних ураганах в Австралии, о забастовках фермеров в Испании, об извержении вулкана в Исландии, о нарядах звезд на фестивале в Каннах. Мы читаем и слышим каждый день о том, что происходит в разных уголках страны, о событиях в городе.

У пользователя информации складывается впечатление, что он знает все и обо всем, что ему доступны любые сведения и данные, что он разбирается в политике, экономике, бизнесе, медицине, моде, искусстве, высоких технологиях, кулинарии и т.д.

На самом деле обычный пользователь обладает очень тонким слоем информации. Она не глубока, не детализирована, подчас является искаженной, так как является не первоисточником, а, к примеру, эмоциональным рассказом очевидца, трактовкой события экспертом, точкой зрения лидера мнений, пересказом новости другим пользователем. Складывая представление о событии или явлении из такого лоскутного одеяла обрывков информации, каждый пользователь решает, что он обладает уникальным мнением. К сожалению, это не так. Реальная ситуация показана на следующем рисунке:



Она демонстрирует принцип информированности жителей «информационной деревни», которыми, по большому счету, являемся мы с вами.

Обилие информации практически исключает возможность ее перепроверки, приверженность тем или иным медиа, лидерам мнений, бло-

герам – формирует стереотип, что раз эти источники так «профессионально» рассуждают о событии, значит, они подают нам достоверную информацию. В результате мы формируем свое мнение из далеко не точных, а главное неполных данных.

Механизм искажения информации (принцип каскадности информирования)

Ранее мы говорили о сложности получения достоверной информации, так как тому способствуют ряд причин – стереотипы, трудность проверки, обилие мнений о событии, большой поток самих новостей и т.д. Еще один важный момент, который влияет на степень достоверности получаемой пользователем информации, – это время, или период ее «свежести».

И тут интересен следующий парадокс — открывая, к примеру, смартфон, мы видим новость и воспринимаем ее как «свежую», новую. Почему? Потому что срабатывает простой психологический механизм – все что я вижу впервые (впервые за последний час, за день, просто утром), – для меня является «новым». Уже после может сработать механизм критического мышления: а посмотрю-ка я на дату публикации новости, а может, это поздняя перепубликация одного ресурса с другого. Но не всегда данный механизм включается. В тоже время очень часто сегодняшние медиа на волне интереса к какой-то теме публикуют новости о событии или какое-то заявление, давность которого исчисляется месяцами. Причем выдается такая новость как свежая – убираются любые маркеры временной идентификации, соответствующим образом корректируется контекст.

Но и это лишь один из механизмов искажения информации.

Каким же образом происходит так, что мы как пользователи, как правило, оперируем искаженной информацией и на основе ее составляем свое мнение о событии и его фактах? Разгадка кроется в понятии «каскадности» поступления информации в информационное поле.

Итак, представим себе, что произошло достаточно громкое и масштабное событие. Кто включается первый в информировании нас о нем? Как правило это:

- официальное сообщение соответствующих учреждений или органов;
- заявления или комментарии официальных или уполномоченных лиц;
- сообщения ведущих, топовых СМИ – как правило TV и интернет-МЕДИА.

Эти сообщения достаточно оперативны (если система информирования работает в рамках цивилизованных правил), лаконичны, не содержат много деталей, но достаточно информативны, чтобы сориенти-

ровать пользователя в том, что это за событие, каковы его последствия. Это – «**первый каскад информирования**».

Далее в информирование включаются те каналы и источники, что не успели поучаствовать в «разделе пирога» в первом каскаде. Причин этому может быть много, как объективных, так и субъективных – попросту не успели, не хватает ресурсов для оперативности, специфика работы и т.д. **Вторым каскад информирования** заполняют:

- заявления, комментарии заинтересованных лиц (официальных и неофициальных);
- комментарии, заявления топ-персон, экспертов, лидеров мнений, узко-профильных специалистов, иногда – очевидцев, участников событий;
- сообщения в СМИ «второго эшелона», радио, печатных медиа.

К информированию при **третьем каскаде** подключаются:

- сообщения в соцсетях;
- сообщения в СМИ «третьего эшелона» (как правило, это копирайт, иногда искаженный и неточный с топ-медиа);
- персональные заявления журналистов, блогеров;
- комментарии к комментариям;
- откровенно фейковые сообщения, созданные для придания событию сенсационности, остроты.

Не так сложно увидеть, что от каскада к каскаду достоверность фактов о событии снижается, так как очень большую роль начинают играть не факты события, а мнения, суждения, трактовки, вариации на тему, рассуждения, заявления о нем (часто с высокой степенью эмоциональности). В результате наблюдается следующая тенденция в достоверности информации:





ДОМАШНЕЕ ЗАДАНИЕ

Поиск искаженной информации

Найдите в трех разных медиа новость по одной и той же теме и сделайте сравнение того, как подается информация в каждом из них. А именно:

- громкость / яркость заголовка;
- кто / что указаны как первоисточник информации;
- точность передачи информации;

- использованы ли дополнительные данные;
- искажены ли данные.

Представьте свой анализ новостей, указывая плюсы и недочеты подачи информации в одних медиа по отношению к другим.

Факторы влияния на информацию: шум, цунами, троллинг и их угрозы

Говоря о моменте выбора той или иной информации, мы часто сталкиваемся с «изобилием» этой самой информации. Помним термин «информационная деревня»? Главная характеристика его – очень большой объем сообщений о событиях широчайшего диапазона тем и географии.

Но даже если мы возьмем какое-либо местное событие, то все равно столкнемся с несколькими или множеством сообщений о нем. Более того, начав изучать факты одной новости, мы подчас сталкиваемся с ситуацией, что нас накрывает «волна» следующего события и обилие трактовок его фактов. Оставив в стороне первое событие и переключив внимание на второе нас может удивить то, как же много «говорят и пишут» о данном событии (вспоминаем каскадность информирования). В этом потоке мнений, суждений, трактовок мы можем вообще потерять изначальный смысл реальных фактов события.

Описанная схема сегодня является объективной реальностью. Ее проявления имеют уже устоявшиеся названия. А именно:

- информационный шум;
- информационные волны (или цунами);
- информационный троллинг.

Информационный шум

Информация стремится к нам отовсюду, из разных источников, каждую минуту. И часто мы не различаем источники информации, а из-за огромного количества схожего контента не различаем источники, из которых мы его получаем. Мы читаем новости в Фейсбуке или в Инстаграме. Часто мы разглядываем все подряд, листая ленту сообщений. В такой ситуации мы можем просто «устать» и прекратить проли-

ствывание на 20-25-м сообщении, а вот как раз 26-е может быть для нас наиболее нужным, чем все предыдущие.

Но даже выбирая отдельную новость для прочтения (бегло или от «А до Я»), нередко нам трудно понять ее суть, разобраться в ее фактах, отделить факты от мнений и рассуждений, уловить главную идею. В этом и кроется угроза **«информационного шума»** – создания вокруг события потока из множества сообщений о нем, которые содержат в меньшей степени факты, а в большей – трактовки, мнения, альтернативные версии, комментарии к альтернативным версиям, опровержения версий (или отдельных фактов), симбиоз реальных фактов события и вымышленных, фейковых.

В этом кроются системные угрозы для нас как пользователей информации. А именно:



Информационные волны

Обилие ярких, громких новостей о событиях, которые заполняют информационное пространство за короткий промежуток времени, называется **«информационными волнами»**.

Информационные волны могут быть следствием реальной ситуации, когда действительно происходит много громких событий в течении нескольких дней, недели. Но чаще всего это искусственное явление. Как правило, информационные волны создаются группой медиа для привлечение внимания к какой-то теме или же наоборот – для отвлечения от события, явления, персоны (если речь идет о скандале, к примеру). Нарастание волны впоследствии поддерживают и обычные СМИ, так как не хотят остаться в стороне от освещения топового события.

В результате пользователь, еще не до конца разобравшись в одной серьезной теме, получает информационный удар следующей или нескольких. И так может повторяться ежедневно. Угрозы в такой ситуации кроются в следующем:



Информационный троллинг

Понятие троллинг пришло в информационное пространство из сленга социальных сетей. В простой доступной интерпретации это – забалтывание какой-то темы, словесное подшучивание над кем-то или чем-то. В инфопо-

ле троллинг имеет подобное определение — системная, целенаправленная «загрузка» медиапространства громкими, но бессодержательными информационными проявлениями по теме события, которые отвлекают внимание, но базируются на речах знаковых персон, ссылаются на псевдопризнанные источники, несут больше эмоциональную нагрузку, чем фактологическую.

Угрозы, которые кроются в информационном троллинге, следующие:



Теперь вы знаете, как устроено поле новостей и что мы живём в большой “информационной деревне”. Пора разобраться, как не попасться на удочку манипуляторам.



Домашнее задание

1. Запишите от 7 до 10 шагов и действий, которые нужно предпринять, чтобы максимально обезопасить себя от недостоверных новостей, которые влияют на наше мнение и представление о событии. Обсудите свои мнения в классе.

2. Подготовьте в небольших группах «правильную новость». На основе проведенных вами исследований новостей напишите «правильную новость». Важный момент: в новости должны найти свое применение не менее трёх признаков информации, которые мы изучали в начале главы. Главная задача – избежать тех недочетов в новостях, которые были выявлены вами ранее при анализе новостей. Объем новости – не более 2000 знаков.

ГЛАВА 5

ФОРМАЛЬНАЯ ЛОГИКА: КУРС МОЛОДОГО БОЙЦА



Вы уже сталкивались со словом «манипуляция» и «манипулирование». Мы сталкиваемся с ними ежедневно — в общении с родными, друзьями, учителями, посторонними людьми, через интернет и СМИ, рекламу, даже в играх. Разберёмся, откуда оно произошло и как с манипуляциями бороться.

Виды манипуляций и как с ними бороться

Manus по-латыни «рука», а manipula — «горсть». Так в Древнем Риме называлась основная тактическая единица легиона, небольшой отряд. Манипулярная тактика заключалась в правильном построении манипул, их чередовании на поле боя (от новичков до ветеранов — когда и кто должен был вступить в бой), очередности вступления в бой и, если необходимо — отступления, и так далее. То есть, это искусство управления людьми с какой-то целью, изначально — с военной. Нас, как эту «горсть» людей (манипулу), бросают на определённый участок «войны», в которой мы ничего не понимаем: зачем она, кому нужна, кому выгодна и почему мы должны находиться там и «умирать» за чьи-то интересы.

В жизни мы чаще всего сталкиваемся с психологическими манипуляциями, когда нас пытаются заставить делать что-то не по своей воле (испытывать комплекс вины, делать чужую работу, уважать кого-то «по умолчанию», и так далее).



Манипуляция — это всегда навязывание (скрытыми приемами, иногда насильственными) не своего мнения, а так как мы не успели или не захотели об этом подумать, нам дали готовое решение.

Так ли это плохо?

Манипуляция не всегда зло. То есть взрослые в общении с детьми, учителя в общении с учениками, генералы в общении с солдатами, правительство в общении с народом пытаются часто сделать все быстрее, донести какое-то решение или мысль, которые были до этого обдуманы целыми поколениями или специальными институтами. Им просто лень объяснять либо они считают, что объяснять — долго.

Однако как отделить злонамеренные манипуляции от позитивных? Как самому управлять собственной жизнью, не полагаясь на мнение окружающих?

Выход для любого думающего человека – подключить критическое мышление.



Критическое мышление – это способность человека ставить под сомнение поступающую информацию, даже собственные убеждения.

Это основа всего прогресса человечества, научного мышления. То есть мы должны перепроверять всю информацию и даже собственные убеждения, сложившиеся под воздействием этой информации.

Что нам в этом поможет? Формальная логика!

Формальная логика – это правильная последовательность суждений. Весь человеческий опыт передается только через речь, даже цифры, как бы ни убеждали математики и программисты – это иначе зашифрованная речь. А у речи есть формы. То есть мы строим предложение по определенным формулам, например, если в конце предложения поставим вопросительный знак, значит, это вопрос, если точку – это утверждение. Или если мы обращаемся к конкретному человеку, мы сразу определяем его статус в речи: либо родственный «папа, мама, дядя» и т.д., либо социальный «господин президент», «уважаемый», «эй ты!» ... Это все – формы речи.



Формы речи изучаются и определяются **логикой** — наукой о законах мышления и его формах.

Последовательность суждений тоже имеет смысл. Чтобы сделать правильный вывод, нужно руководствоваться четырьмя законами формальной логики, которые приведем ниже. Они не придуманы кем-то на самом деле, они были сформулированы из человеческого опыта. Форма – важнейшая часть мышления. Мы должны научиться определять формально что правда, а что манипуляция, то есть ложь (даже если «во благо»). Это азы критического мышления.



УПРАЖНЕНИЕ 1

Проверка логики

Попробуйте определить, правильно ли формально построены следующие утверждения:

1. Все кырымки имеют хвосты.
Рыкымбл тоже имеет хвост.
Значит, рыкымбл – кырымка.

2. Кыртымка чистит зубы по утрам – это гигиена.
Гигиена помогает бороться с заболеваниями.
Чистка зубов по утрам помогает кыртымке бороться с заболеваниями.
3. Кыртымка сказала, что против зла.
Я тоже против зла,
Значит, я за кыртымку!

История манипуляций и борьбы с ними

Более 2500 лет назад в Древней Греции активно распространились школы софистики. Там давали уроки начинающим политикам: как при помощи ораторского искусства добиваться своих целей. От философов софисты отличались тем, что главным признавали достижение практической цели.

То есть формула «цель оправдывает средства» еще оттуда.

Аристотель (384-322 гг. до н.э.) решил положить конец одурачиванию народа (по крайней мере, попытался — мы и сейчас попадаемся на те же самые уловки, что были известны еще 2500 лет назад). Он создал научную базу формальной логики, которую называл «Аналитика».

Итак, четыре основных закона логики

Три из них сформулировал еще Аристотель:

Закон тождества



«...иметь не одно значение — значит, не иметь ни одного значения», писал по этому поводу Аристотель в своей «Метафизике».

То есть каждая мысль и каждый термин в процессе рассуждения должны иметь одно и то же значение. Подмена понятия в ходе рассуждения — это классическая логическая ошибка (или уловка).

Например:

*Рыкымбл хороший человек, скромный и любит ездить на велосипеде.
Из него получится хороший аким города!*

Здесь мы видим, как в первой части утверждения говорится о личных качествах человека, а вывод делается о его профессиональных качествах, что далеко не тождественно.

Или:

Кыртымка – человек.

Кыртымка в то же время робот.

Кыртымка не может быть одновременно человеком и роботом, это взаимоисключающие понятия. Она либо человек, либо робот.

Закон противоречия



Два противоречащих друг другу суждения не могут быть одновременно истинными. По крайней мере одно из них ложно.

Например:

Кыртымки – неопасные существа.

Некоторые из кыртымок могут убить.

Из этого следует, что кыртымки совсем не безопасные существа, даже если большинство из них безопасны.

Это встречается сплошь и рядом – ложные обобщения.

Закон исключённого третьего



Два противоречащих друг другу суждения не могут быть одновременно оба истинными или оба ложными. Третьего не дано.

Противоречащими называют такие два суждения, в одном из которых что-либо утверждается о предмете, а в другом то же самое об этом же предмете отрицается.

Например:

Кыртымки ничего не соображают в кухне!

Кыртымки, готовящие борщ, великолепны!

Либо кыртымки ничего не смыслят в кухне, либо кыртымки могут готовить блюда.

Закон достаточного основания

Это особенный закон формальной логики, потому что он... неформальный.

Он был добавлен в формальную логику спустя две тысячи лет её существования в XVIII веке выдающимся немецким ученым Вильгельмом Лейбницем.



«Всякая правильная мысль должна быть обусловлена другими мыслями, истинность которых доказана» (Готфрид Вильгельм Лейбниц, «Монадология»).

Почему это произошло, почему в формальную логику вторгся закон неформальный? Потому что к этому времени был накоплен большой багаж знаний, книг, в которых были высказаны многие мнения, и люди путались, считая книжное мнение за единственно правильное. Но там было много ошибочных суждений, просто мнений, которые читатели воспринимали за истину в последней инстанции.

Нарушение этого логического закона мы видим ежедневно.

Например:

Доказано, что есть хлеб вредно!

Многие люди на подобные утверждения «ведутся». Однако: кем доказано, когда, почему, как? Ответов не приводится.

И нам нужно получить на это ответы, прежде чем верить источнику.



Домашнее задание

Разберите, нарушениями какого закона логики являются следующие утверждения. Обсудите ваши варианты с учителем.

1. Я познакомился с кырымкой, нормальная девушка, а, с другой стороны, — нечестная.
2. Я всегда выступаю за законность, поэтому обругал человека, выбросившего окурок мимо урны.

Классификация логических уловок (ошибок)

В принципе, логическая ошибка и логическая уловка — это одно и то же, просто ошибка допускается несознательно, а уловка специально вводится в речь. Они строятся на противоречии четырем основным законам формальной логики.

Ignoratio elenchi, или «подмена тезиса»

В переводе с латыни — «невежественное опровержение», попытка отвлечь оппонента, представив «аргумент», не имеющий отношения к первоначальной теме обсуждения. В принципе то, что известно и «сетевым аналитикам», говорящим: «Нас от чего-то отвлекают». Только вот *ignoratio elenchi* — это не конспирология, а вполне конкретная логическая ошибка, которая прямо противоречит первому закону фор-

мальной логики, закону тождества («...иметь не одно значение — значит, не иметь ни одного значения»).

Уловка в том, чтобы построить своё «доказательство» на том, что оппонент сделал какое-то слабое или неверное утверждение. Благодаря этому у аудитории и часто даже у самого оппонента создаётся ощущение, будто он действительно сделал такое утверждение. Наиболее часто встречающийся пример:

«Вот вы сказали, что вы недовольны качеством укладки дорог, вы недовольны частой сменой бордюров – вы вечно всем недовольны. Это очень плохо и неконструктивно».

Легко увидеть, что вывод «вечно всем недовольны» строится как раз на подмене понятия, ведь оппонент был всего лишь недоволен дорогами и бордюрами. Следовательно, все дальнейшие рассуждения о вредности пессимизма, о необходимости самому что-то изменить в жизни — это продолжение удачно ввёрнутой логической уловки и никакого отношения к логике и реальности не имеют.

Кстати, *ignoratio elenchi* – это совсем не обязательно негатив, но обязательно манипуляция. С «позитивным» примером легко можно встретиться каждый день в рекламе. Нам рассказывают о разных прекрасных товарах, благодаря покупке которых якобы можно сэкономить (потратив деньги), или подталкивают к покупке, подменяя тезис о реальном качестве товара «чучелом» в виде терминов «престижный», «модный», «всемирно известный бренд» и т.д.

Предвосхищение основания

Вторая по распространенности логическая уловка – это *restitutio in integrum* — «предвосхищение основания», которая преследуют нас ежедневно из всех каналов коммуникаций.

Эта логическая уловка строится на нарушении четвёртого закона логики – достаточного основания.

Поскольку она не формальная (то есть нельзя определить ошибку просто по неправильному построению логической цепочки), определить её сложнее. И именно эта уловка чаще всего применяется в социальных сетях. Когда для обоснования своих выводов относительно какого-то предмета, человека или явления применяется аргумент, который вызывает сомнения и сам нуждается в доказательстве.

Ярким примером использования этой уловки стало название диска Элвиса Пресли, вышедшего в 1959 г. «50 миллионов фанов Элвиса не могут ошибаться».

Конечно, они могут ошибаться! В мире живёт 7,7 миллиардов человек, мнение 50 миллионов – это не достаточное основание для принятия их точки зрения как всеобъемлющей.

Разновидности *petitio principii*

Argumentum ad hominem

В переводе с латинского означает «аргумент к человеку» или, ближе по смыслу, «атака на человека», или в просторечье – «переход на личности».

Это одна из самых бесхитростных уловок — переход от обсуждения предмета спора к обсуждению личности, в этом споре участвующей. Её очень легко разоблачить, но, тем не менее, она используется регулярно и с большим успехом.

Главное правило: важно не КТО говорит, а ЧТО он говорит.

Пример:

Кырымка сказала, что Рыкымбл пилит бюджет.

Но кырымка сама осуждена за коррупционные преступления.

Следовательно, верить Кырымке нельзя.

Вывод: можно верить, а можно не верить – не имеет значения личность кырымки, имеют значение факты, приведенные ею.

Аргумент к скромности

Другая версия «предвосхищения основания» — уловка **argumentum ad verecundiam**, что переводится как «аргумент к скромности», но означает, наоборот, «апелляция к авторитету».

Имеется в виду, что человек должен проявить скромность и признать, что мнение авторитета важнее, чем его личное, и даже важнее аргументов и фактов. Это когда вам навязывают какое-то суждение, и единственным доводом является то, что какой-то авторитетный человек уже принял это суждение за верное.

Этот приём любят использовать в рекламе, где различные селебрити «продают» еду, напитки, технику и т.д. Более того, часто производители рекламы идут на прямой подлог и используют мнимых авторитетов: многочисленные «ассоциации стоматологов», «терапевтов», «финансистов» и т.д. на самом деле созданы только для рекламы конкретного товара. Но главная ошибка кроется не просто в ссылке на мнение авторитета, а в вере, что его мнение всегда безошибочно. Однако футболист не является специалистом по чипсам,

боксер – специалистом по банкам, самые лучшие экономисты многократно ошибались, а фальшивые стоматологи преследуют только цель продать вам подороже самую обычную зубную пасту, но в новой упаковке.

Встречаются и другие вариации уловки *petitio principii*.

Argumentum ad antiquitatem – «апелляция к традиции»

Примеры манипуляций: «Так считается издавна», «Так делали на протяжении веков» и прочее.

При этом за века изменились условия существования человека, шагнула вперёд наука, трансформировались нравственные нормы общества. Если «раньше всегда» муж бил жену, это не означает, что сейчас он этим не нарушает уголовный кодекс. И если раньше попадание земли в рану обычно заканчивалось смертью, то сейчас можно принять антибиотики, а не заказывать похороны.

Argumentum ad ignorantiam – «апелляция к незнанию»

В данной уловке отсутствие доказательств подаётся как доказательство обратного. Чаще всего этой уловкой пользуются всевозможные шарлатаны: «Никто не доказал, что магия не действует, значит, она действует!»

Argumentum ad nauseam – «аргумент к тошноте»

Проще говоря — повторение тезиса до тех пор, пока оппонент не устанет его опровергать. Наверняка вы замечали такое поведение в комментариях к спорным постам в соцсетях.

Argumentum ad misericordiam – «апелляция к милосердию»

«Если вы продолжите спорить со мной, мне будет очень плохо». Предполагается, что человек из жалости к оппоненту должен принять его точку зрения или перестать переубеждать аудиторию, введённую оппонентом в заблуждение.

Argumentum ad baculum – «палочный аргумент»

Это даже сложно назвать аргументом в обычном значении этого слова. Оппонента просто заставляют согласиться с чужим мнением: «Если вы не согласитесь, произойдёт что-то плохое».

Мы можем столкнуться с этим в банках, например, когда начинаем спорить по трактовке какого-то пункта договора, а нам говорят: «Или вы соглашаетесь с нами, или мы не выдадим вам кредит».

Non sequitur – «не следует»

Довольно частая ошибка, когда на основании какого-то суждения, пусть даже верного, в итоге приходят к заключению, которое совсем не следует из него. С советских времён нам знакомо идеологическое клише – изначально ложное суждение «Кто не с нами, тот против нас!», вытекающее из нарушения четвертого закона логики – достаточного основания. Ведь для утверждения «он против нас» требуется больше доказательств, кроме того, что «он не с нами». Этот «он» может быть вообще ни с кем и ни против кого. Практически вся идеологическая машина работает, используя именно эту уловку. «Они критикуют наше правительство, значит, они не хотят счастья нашему народу!», «Они сопротивляются нашей агрессии, значит, они хотят поставить нас на колени!» и т.д. Хотя не только одно не следует из другого, но и предполагается гораздо больше вариантов, чем один-два озвученных. Шуточный пример этой уловки: «Сегодня он играет джаз, а завтра родину продаст». Никакой связи между джазом и предательством на самом деле нет, но эта конструкция в разных вариациях используется манипуляторами с успехом и сегодня.

Idem per idem – «то же посредством того же», или circulus vitiosus – «порочный круг»

Суть этой уловки в том, что аргумент доказывается с опорой на тезис, который входит в сам аргумент. «Этого не может быть, потому что этого не может быть никогда» (А.П. Чехов, «Письмо к учёному соседу»).

В наших условиях в основном этим грешат чиновники, затрудняющиеся сформулировать свои мысли или стремясь скрыть, что они на самом деле думают или делают (или не думают и не делают). «Мы за экологию, потому что мы – управление экологии!», «Задача правоохранительных органов – в охране правопорядка» и т.д. и т.п.

Fallacia fictae universalitatis – «ложное обобщение»

Когда на основании знаний о каких-то отдельных явлениях или представителях какой-то категории людей (или животных) делают вывод о целом.

Эта ошибка лежит в основе любой ненависти: от национальной «все представители этой национальности грубы и глупы» до классовой «все богатые – воры». На основе этой уловки были построены самые страшные политические режимы в истории: от германского нацизма до камбоджийского режима красных кхмеров.

В быту это также распространено и приводит к возникновению различных устойчивых стереотипов. О мужчинах (все мужчины такие-то), о женщинах, о представителях различных профессий.



Всё это – ложные обобщения. *Post hoc, ergo propter hoc* – «после» не значит «вследствие». С латыни этот термин переводится буквально «после этого, значит по причине этого».

Теперь вы вооружены инструментами логического анализа. Применяйте их всякий раз, когда вам покажется, что вами хотят манипулировать.



Домашнее задание

Определите, к какой логической уловке относятся эти утверждения:

1. Рыкымбл не дает нам денег.
Мы страдаем.
Рыкымбл плохой.
2. Кырымка из Кыртымии.
Кырымка постоянно выбрасывает мусор у подъезда.
Все из Кыртымии – такие же свиньи, как кырымка.
3. Вы пишете это, потому что просто не знаете, кто правит миром.

ГЛАВА 6

МЕДИА И РЕКЛАМА



В разных источниках можно встретить различные определения, что такое реклама. У каждого уже есть определенное представление о рекламе и опыт, как она влияет на каждого из нас. В этом разделе введем общее для нас понятие рекламы и того, как анализировать её влияние.

Реклама и медиа

Само слово «реклама» имеет латинское происхождение *reclamare* и в переводе означает «утверждать, выкрикивать». Есть другое мнение, что происходит оно от французского слова *reclame*, что переводится как «привлекать к себе внимание».

«Толковый словарь Ожегова» дает нам следующее определение:



Реклама — это оповещение различными способами для создания широкой известности, привлечения потребителей, зрителей.

В рамках нашего курса примем следующее определение:



Реклама — это информация, распространяемая различными способами с применением различных технических средств, адресованная широкому кругу лиц с целью привлечения внимания к объекту рекламирования.

Но откуда все начиналось?

Человечество торгует тысячи лет, примерно столько же существует реклама. Первые наскальные рисунки, содержащие информацию о месте охоты и о ее результатах, являются первыми признаками рекламы. Также желание выделиться среди себе подобных, украшая свою внешность самыми разнообразными способами, можно считать современной имиджевой рекламой.

В Древней Греции и Древнем Риме торговцы налаживали связи со своими покупателями посредством прямых словесных обращений. Места продажи оглашались громкими и повторяющимися криками продавцов. Самый старый рекламный текст был найден в Древнем Египте, в городе Мемфис: «Я Рино с Крита, по повелению богов толкую сны».

А современная реклама в том виде, в котором мы ее знаем, берет начало от изобретения первого печатного станка Иоганном Гуттенбергом в 1450 г. Данное открытие ознаменовало качественно иной этап развития маркетинговых технологий.

Первой официальной печатной рекламой считается объявление в английской газете в 1625 г. о награде тому, кто сообщит сведения об угнанных лошадях.

Первыми примерами социальной рекламы считаются работы Джеймса Флегга 1917 г. «Ты нужен Американской армии!», следом появились подобные плакаты в Советском Союзе «Ты записался добровольцем?».



Исследователи отмечают, что основателем печатной рекламы в Европе был французский врач Теофраст Рендо, который открыл в Париже справочную контору, печатавшую объявления во французской газете LaGazette. В 1890 г. было создано первое рекламное агентство в Филадельфии «Айер и сын».

По сей день реклама развивается параллельно с научно-техническим прогрессом. Сегодня это не только бизнес, а широкое явление, которое оказывает влияние на многие сферы человека:

- **Социальную** (достижение общественно полезных целей, информирование общества о различных инновационных достижениях, анализ и сравнение различных изделий, формирование эстетических представлений)
- **Нравственно-правовую** (продвижение этических и правовых норм)
- **Духовную** (формирование патриотизма или же манипуляция общественным сознанием)

- **Политическую** (агитационные материалы, формирование имиджа политика или политической партии)
- **Идеологическую** (фактор, влияющий на становление и формирование мировоззрения человека)
- **Психологическую** (воздействует на желания и мечты покупателя, не вызывая к его разуму)
- **Коммуникативную** (функция коммуникации между рекламодателем и рекламополучателем, поскольку перед рекламой поставлена задача донести необходимое сообщение до потребителей товаров и услуг)
- **Образовательную** (в процессе просмотра рекламы, а также внедрения новых технологий товаров и услуг, человек может почерпнуть для себя информацию абсолютно из всех сфер жизни (от причин появления налёта на плитке в ванной комнате до последних инновационных разработок в компьютерной технике)
- **Экономическую** (стимулирование потребителей к приобретению товаров и обеспечение экономической целесообразности производственно-сбытовой деятельности предприятий)
- **Эстетическую (культурную)** (во многих рекламных роликах очень качественно подобраны цвета, звуки, которые могут повлиять на человека, вызвав в нём желание реализовать рекламное предложение или хотя бы обратить на него более пристальное внимание).

Именно поэтому важно разбираться в том, как на нас действует реклама. Это не только инструмент сбыта товара или услуг, но и средство формирования нравственных установок, ценностных ориентаций, социальных норм, правил и стилей поведения. Несмотря на то, что у каждой страны есть особенности в разработке и подаче рекламы, она остается универсальным инструментом передачи информации. Она понятна людям разных национальностей и вероисповеданий.

Виды визуальных материалов

Реклама многолика: она может предстать пред нами как в виде кандидата на пост президента страны, так и в виде сюрприза в шоколадной конфете. Но всё же ее можно квалифицировать, разбить на несколько видов, каждому из которых присуща своя специфика. В зависимости от назначения рекламы выделяются разновидности. С различными видами визуальных материалов вы ежедневно сталкиваетесь на улице, просматривая сайты, телевизионные каналы или даже дома.



Коммерческая реклама – это информация о товарах и различных видах услуг с целью их реализации, создания спроса на них. Иногда это еще и распространение сведений о лице, организации, произведении литературы и искусства для его популяризации.



Социальная реклама – это когда посредством рекламы обществу хотят объяснить какие-то проблемные моменты общественного устройства. Например, вред ранних браков для здоровья граждан, равные возможности для детей с особенностями (больных аутизмом, например), лиц с ограниченными возможностями здоровья, чтобы создавать им условия для того, чтобы они не сидели дома, а имели возможность выходить на улицу, посещать развлекательные центры, кинотеатры.



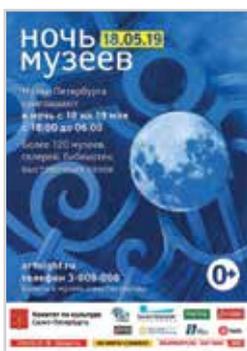
Агитация – устная и печатная деятельность в обществе, имеющая целью распространение каких-нибудь идей для политического воспитания людей и привлечения их к активной общественно-политической жизни. Это работа с избирателями, митинги, шествия; наглядная агитация включает плакаты и листовки, наружная агитация – баннеры, уличные щиты, уличные мониторы.



Политическая агитация – это тоже вид рекламы. Ее мы с вами видим во время выборов процессов. Когда сообщение на плакате призывает голосовать за того или иного кандидата, отдать свой голос определенной партии или выбрать депутатов различного уровня.



Пропаганда – это вид агитации. Когда информация навязывает нам определенное мнение. Пропаганда является одним из основных инструментов воздействия на общественное мнение. Она активно используется государством, политиками и партиями.



Информирование – объявление о том, что что-то происходит или произойдет. То есть, когда информация сообщается для того, чтобы тот, кто ее прочитал, просто знал о мероприятии или событии.



PR-кампания – ряд мероприятий, проводимых для организации коммерческой, политической или социальной кампании. Например, розыгрыш лотереи среди покупателей определенного магазина.



УПРАЖНЕНИЕ 1

Какой из вас рекламный специалист?

ШАГ 1: Еще раз посмотрите на картинки выше и прочитайте текст о разных видах визуальных материалов. Разделитесь на три группы. Каждая группа получает набор карточек. Обсудите и подпишите, к какому виду сообщения относится каждый постер.

1. _____



2. _____



3. _____



4. _____



5. _____



6. _____



7. _____



8. _____



9. _____



10. _____



11. _____



12. _____



ШАГ 3: Зачитайте свои ответы. Сверьте с правильными ответами.

ШАГ 4: Каждая группа должна придумать рекламу по трем видам (можно нарисовать постер, подготовить сценку, снять ролик на телефон или сделать что-то другое). Можно пофантазировать и придумать любой сюжет, который вы считаете нужным. Предмет (товар или услугу) рекламы можете выбрать самостоятельно.

1 группа: социальная реклама

2 группа: коммерческая реклама

3 группа: информирование.

ШАГ 5: Презентация групповых заданий.



Домашнее задание

Прочитайте закон РК о рекламе. Обсудите с учителем, какие требования предъявляются к рекламе в Казахстане, что можно, а что нельзя рекламировать.

Функции рекламы

Согласно Уильяму Уэллсу (William Wells), исследователю рекламы, она выполняет 7 основных функций. Функции основываются на том, что может получить рекламодатель от своей рекламы или почему он решает использовать рекламу:

1. Создаёт осведомленность о товарах и брендах.
2. Формирует имидж бренда.
3. Информировует о товаре и бренде.
4. Убеждает людей.
5. Создаёт стимулы к совершению действий.
6. Обеспечивает напоминание.
7. Подкрепляет прошлый опыт покупок.

Реклама, как и любое другое явление медиа, подразумевает создание послания и отправки его группе людей в расчете на то, что они отреагируют на рекламу определенным образом. Мы каждый день встречаем огромное количество рекламных обращений, которое видим по телевизору, слышим по радио, читаем в газетах и журналах, встречаем

в интернете и на билбордах. Реклама, хотим мы этого или нет, влияет на человека, на его поступки, выбор, стиль жизни. Можно сказать, реклама манипулирует человеком. Она влияет на общество, а общество, в свою очередь, влияет на развитие рекламы.

Вы уже изучили основные виды манипуляций, работая с главой о формальной логике. Пришло время разобраться с тем, как манипуляции используются в рекламе.

Манипулятивный уровень с использованием рекламных технологий может организовываться огромным количеством способов.

Первый способ связан, прежде всего, с информационным потоком.

Например:

- опустить часть информации или исказить ее;
- обобщить информацию до неузнаваемости;
- выдумать ложную информацию;
- задать вопрос и не дать возможности ответить;
- сослаться на авторитеты;
- метафоры, юмор, шутки могут также использоваться как средство манипулирования.

Кандидат психологических наук Сергей Леонидович Братченко (1956-2015) выделяет пять видов манипулирования:

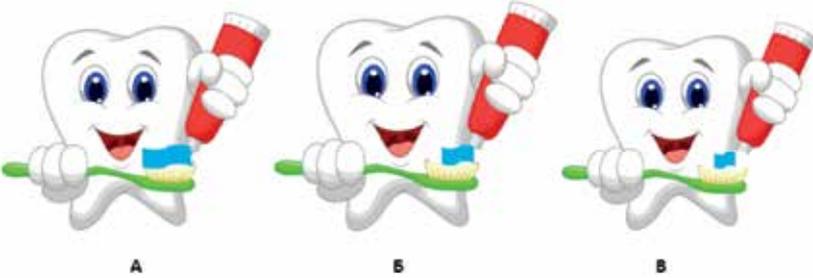
1. манипулирование потребностями (использование желаний, влечений, интересов);
2. «духовное» манипулирование (формирование у человека определенных идеалов и ценностей);
3. интеллектуальное манипулирование (навязывание человеку мнений, точек зрения);
4. манипулирование чувствами (использование эмоций);
5. символическое манипулирование (формирование устойчивой реакции человека на определенные символы).



УПРАЖНЕНИЕ 2

Манипуляция в рекламе

1. Посмотрите на картинку. Индивидуально ответьте на вопрос, сколько зубной пасты вы выдавливаете на зубную щетку? Почему?
2. Разделитесь на три группы, на А, Б и В, как на картинке, то есть кто сколько выдавил пасты.



3. Ответьте на вопросы:
 — Почему вы используете столько зубной пасты? Обоснуйте свой ответ.
 — Знаете ли вы, сколько пасты рекомендуют стоматологи использовать для чистки зубов?

4. Приведите из жизни примеры влияния рекламы на человека.

Приёмы и стереотипы в рекламе

В рекламе используют разнообразные психологические приемы, чтобы задеть потребителя за живое. Реклама пытается связать наши потребности с продуктом. В ней скрыто послание о том, что покупка нового товара не только принесет пользу и будет приятной, но и что купив тот или иной продукт, мы сами станем лучше. Давайте рассмотрим приемы, которые используются в рекламе.

- **Информационный** — даёт информацию о товаре или об услуге, разъясняет, для чего предназначен товар или услуга. Для этого типа рекламы хорошо подходят газеты и журналы. Чаще всего используется метод обращения или советы – сберечь деньги или получить более качественный товар или услугу. Ощущение того, что вы делаете выгодную покупку, — мощное средство мотивации, когда вы решаете что-то приобрести.
- **Эмоциональный** — очень часто реклама воздействует на эмоциональную составляющую наших установок. Влияние на эмоции — это действенный способ влиять на наши убеждения и в конечном итоге на наше поведение. Например, очень много рекламных роликов обращены к нашей любви, семье, друзьям, хорошим временам и чувствам, с которыми они связаны. Реклама говорит: купите это товар или услуги, подарите близким и сделайте приятное, купите тур, путевку и съездите

с семьей на отдых. Определенные культурные символы в рекламе вызывают у зрителей теплые чувства, и эти чувства переносятся на рекламные товары. Бабушка, которая печет в тандыре свежий хлеб, мальчик с собакой, мама, готовящая завтрак для всей семьи, семья за новогодним столом — все это примеры таких символов. Эти символы часто появляются в рекламе всех видов.

- **Патриотический** — в рекламе распространен призыв к национальной гордости. Такие обращения часто попадают в рекламу в период проведения Олимпийских игр, различных соревнований Кубка мира или Азиатских игр.
- **Пробуждение страха** создает в воображении угрозу или страх перед тем, что может случиться с человеком, если он не приобретет тот или иной продукт. Например, если: «Вы хотите жить долго, купите такую воду», «Вы же не хотите, чтобы ваш ребенок отстал по математике из-за того, что вы не купите ему компьютер». Это сильное воздействие на чувство вины или страха, которое есть у каждого отца или матери. А теперь посмотрим на психологическую установку в рекламе.

Стереотипы, которые используются в рекламе:

- Дефицит — всегда хорош и ценен. Прекрасного не может быть много. Лучше, когда товар существует в строго ограниченном количестве.
- Дорогой товар — значит, хороший товар.
- Традиционное добротное и достойно по покупке. Некоторые производители пишут на упаковках дату основания компании, указывая и XIX век, и более ранние периоды.
- Авторитету всегда доверяют. Образ человека в белом халате действует безотказно в рекламе не только лекарств, но и зубной пасты или жевательной резинки. Также в рекламе применяются «географические» и «именные» принципы. Например, покупатель думает, что лучшие часы — это «швейцарские» или лучший костюм Hugo Boss.
- Раз все так делают — значит, это правильно.

Какие еще манипуляционные инструменты есть в рекламе?

Существует множество методов манипуляции массовым сознанием. Один из методов — дробление и локализация. Например, самый интересный материал журнала разделен на несколько частей, которые разбросаны по всему номеру. Таким образом, читатель должен пролистать весь журнал, в том числе и рекламные вкладки.

Еще один метод манипулирования, особенно в политической рекламе, когда тщательно подобранные слухи, разбавленные не связанными

между собой и малозначительными кусочками правды, выдаются за аргументированный и глубокий анализ ситуации.

Главная конечная цель рекламного воздействия — вынудить массового покупателя совершить покупку.

Обобщение

Подведем итог нашему занятию.



Домашнее задание

Прочитайте самостоятельно про рекламные тексты и напишите рекламный текст, применяя следующую форму построения текстов:

1. Заголовок
2. Слоган
3. Текст
4. Эхо-фраза

ГЛАВА 7

КИБЕРБЕЗОПАСНОСТЬ



Всеобщая цифровизация несёт не только огромное количество благ и удобств, но и множество дополнительных угроз, число которых постоянно повышается. В этой главе мы поговорим о том, каковы угрозы интернета и социальных сетей, как защитить свой аккаунт в соцсетях, как избежать проблем в интернете и сохранить в нём своё личное пространство.

Безопасность в социальных сетях

Угрозы интернета и социальных сетей

Пожалуй, среди вас почти нет людей, кто не имел аккаунт в социальных сетях и мессенджерах (если есть — вы уникальный и счастливый человек, которому угрожает гораздо меньше проблем, чем остальным!). Социальные сети позволяют нам многое: читать новости, общаться с друзьями, делиться новостями, найти сообщество по интересам или даже создать его самому. Мы чаще всего не задумываемся о безопасности, пока что-то не случится с нами или нашими друзьями. Давайте задумаемся о возможных проблемах заранее, чтобы избежать их в будущем.



УПРАЖНЕНИЕ 1

Как много у вас соцсетей

Посчитайте, сколькими социальными сетями и мессенджерами вы лично пользуетесь.

Какие проблемы возможны в социальных сетях?

Взлом аккаунта

Вы проснулись утром, привычно взяли в руки смартфон, запустили приложение, а оно вдруг просит у вас пароль. Вы пробуете зайти в свой аккаунт с компьютера – то же самое. Что случилось? Вас взломали.

Все может быть иначе. Ваш лучший друг вдруг спрашивает вас в личном сообщении: «Зачем тебе потребовались деньги?». «Какие деньги?» — удивляетесь вы. Оказывается, за последний час вы отправили несколько десятков сообщений своим друзьям с просьбой перевести деньги. Вы также обещали через неделю вернуть всю сумму. Кто от-

правил эти сообщения? Вы это были или не вы? Что случилось? Ответ простой: вас взломали.

Вы можете возразить, сказав: «Да кому нужно меня взламывать? Я не известный человек, да и денег у меня нет». Но могут быть и другие сценарии. Например, вы — администратор сообщества в социальной сети, и буквально за пару минут после взлома вашего аккаунта вы можете его потерять. А если это не ваше сообщество, а большой организации, где вы подрабатывали SMM-менеджером? Последствия будут печальные: на восстановление доступа к группе уйдет несколько дней, а ваша репутация будет испорчена.

Мошенничество

Представьте, что вам пишет администратор известного вам сообщества и сообщает, что вы выиграли в розыгрыше. Подождите радоваться, это может быть обманом. Также вы можете получить сообщение со ссылкой на видео с вашим участием или предложение стать участником проекта — вариантов заманить беспечного пользователя соцсетей очень много. А результат один — вас обманывают, получая от вас деньги или информацию. Вы не заметите, как продиктуете мошеннику номер вашей банковской карты или щелкните на ссылку, по которой в ваш компьютер проникнет вирус-троян.

Кража личной информации

«Я никому не нужен» или «мне нечего скрывать» — это слабая и пассивная позиция. Чаще всего за ней прячутся пользователи сети, которые не могут или не хотят разобраться в вопросах безопасности. В чем уязвимость этой позиции? У каждого человека есть информация, которую не хочется публиковать в общем доступе. Переписка, фотографии, видео, личные записи — много всего.

Беспечные пользователи соцсетей хранят в своих фотоальбомах сканы документов и даже паспорта (на всякий случай), записывают в заметки пароли к своим аккаунтам, отсылают друзьям фотографии, которые не стали бы публиковать на стене. Представьте, что кто-то получил доступ ко всему этому. Это может обернуться для вас ударом по репутации в случае публикации фотографии и переписки. Вы можете стать жертвой шантажа, вымогательства. Ваши средства с банковской карты могут исчезнуть, а паспорт «всплывет» в оформленном на вас кредите.

Кибербуллинг

Все начинается неожиданно: вы как обычно публикуете пост, получаете лайки и комментарии от друзей, и вдруг появляется незнакомый

человек (точнее, аккаунт), который начинает оставлять издевательские сообщения, высмеивать вас, комментировать каждое ваше действие или переходить на личности (писать о ваших особенностях, фигуре, имени, увлечениях – о чем угодно). Он будет язвить в ваш адрес в ответ на любое ваше сообщение. Это может продолжаться довольно долго и не только в комментариях к посту или фотографии, но и в личных сообщениях. На языке интернета это называется «троллить». Но в жесткой форме шутки переходят в травлю и преследование (буллинг), а это уже преступление против личности.

В тяжелых случаях в буллинге могут участвовать несколько человек, тогда жертве сложнее «спрятаться», она постоянно под ударом. Приходится удалять аккаунт или менять имя в социальной сети.

Ниже мы подробнее поговорим об угрозах в интернете и рассмотрим варианты, как их предотвратить или решить.

Как защитить свой аккаунт в соцсетях

Уровень первый. Создаем надежный пароль

Каждый аккаунт в интернете может иметь по крайней мере два уровня защиты. Первый уровень – это пароль. Любой пользователь интернета, который знает ваше имя в социальной сети или электронную почту, может попытаться зайти в ваш аккаунт.

Вообще-то, это противозаконно в любой стране, но, с другой стороны, такая открытая возможность привлекает злоумышленников и скользящих школьников.

Итак, чтобы войти в ваш аккаунт, достаточно указать имя (электронную почту, номер телефона) и пароль. От сложности пароля зависит, удачным будет взлом или нет.

Взлом аккаунта может происходить по разным сценариям, самый распространенный из них – подбор пароля. В этом случае мошенник с помощью специальной программы (реже вручную) и словаря слов автоматически подбирает пароль к аккаунту, отправляя множество вариантов паролей в секунду. Разумеется, в этом случае пароли, которые используются чаще всего из-за неграмотности или недостатка фантазии, будут найдены довольно быстро.

Каждый год Британский Национальный центр кибербезопасности публикует списки самых популярных и в то же время бесполезных паролей, известных взломщикам по всему миру. Так, в 2019 г. лидерами рейтинга популярности стали пароли «123456», «123456789» и

«qwerty». Даже не думайте их использовать! Любой, даже начинающий хакер взламывает ваш аккаунт за секунды.

Топ-10 самых популярных паролей 2019 г.:

- | | | |
|-------------|------------|-------------|
| - 123456 | - 111111 | - password1 |
| - 123456789 | - 12345678 | - 12345 |
| - qwerty | - abc123 | |
| - password | - 1234567 | |

Практическая работа: Создаём пароль, устойчивый ко взлому

У нас есть несколько вариантов.

Будем создавать пароли и проверять их на стойкость с помощью сервиса How Secure Is My Password? (howsecureismypassword.net). Будьте осторожны! Не рекомендуется проверять в этом сервисе свой реальный пароль или использовать пароль, введенный в сервис ранее. Используйте пароли, похожие на те, которые вы ввели в поле сервиса.

Еще один сервис для проверки паролей – Strength Test (<http://rumkin.com/tools/password/passchk.php>). Он подсчитывает степень энтропии (степень предсказуемости появления какого-либо символа). Пароли с энтропией более 36 бит считаются достаточно защищенными.

Вы также можете попробовать сервис для проверки паролей Password Check от Kaspersky <https://password.kaspersky.com/ru>

Классический вариант

В классическом варианте ваш пароль должен состоять из более чем восьми символов. Среди символов должны быть строчные и ПРОПИСНЫЕ буквы на латинице, цифры и спецсимволы (!@#-_%& и другие). В некоторых сервисах в пароле можно использовать пробел – это еще более усложняет жизнь взломщикам.

Вы можете придумать пароль самостоятельно. Возьмите слово, которое вы запомните. Например, *dolphin* (дельфин).

Этот пароль будет мгновенно взломан, да и в нем всего семь символов, так что можно добавить к нему *my*: *my dolphin* (мой дельфин). Этот пароль будет взломан за одну неделю.

- Заменяем некоторые буквы на цифры и спецсимволы: *8yd#lph1n*
- Добавим прописную букву: *8yD#lph1n*
- Завершим создание пароля спецсимволами: *8y!_D#lph1n*. На взлом этого пароля уйдет 400 лет. Это хороший результат.

Теперь запишите пароль в блокнот и храните дома в надежном месте. Наберите его на клавиатуре несколько раз, чтобы запомнить. Раз-

умеется, запомнить разные пароли к нескольким сервисам сложно, и ниже мы расскажем, как это можно сделать.

Создание пароля с помощью списка слов

Метод Diceware предполагает создание пароля из нескольких случайно подобранных слов. Это исключает возможность угадывания продолжения пароля по первому слову.

Представьте, что ваш пароль начинается на «Я помню чудное». Что дальше? Мгновение? Это цитата из Пушкина. А что последует после «Как приручить»? Дракона, правда ведь? Мы предсказуемы, и хакеры это знают. Поэтому все цитаты, названия фильмов, пословицы и поговорки в чистом виде использовать не стоит.

Для создания пароля по методу Diceware вам нужно скачать специальный словарь слов (есть словари для разных языков; общее количество слов — 7776). Вы можете найти в интернете несколько вариантов таких словарей. Не стоит бояться их использовать. Да, словари опубликованы в публичном доступе, но слова, которые вы используете, и их порядок будут известны только вам.

Итак, вам нужен словарь и игральный кубик. Каждое слово имеет свой код. Например, «11111 абажур». Вам нужно бросить кубик пять раз, а потом найти слово, соответствующее этому коду. Например, за пять бросков кубика у меня выпало 16231. Это слово «вече».

Для хорошего пароля рекомендуется пять слов. Бросьте кубик 25 раз, запишите коды и найдите слова.

У меня получилось пять слов: «вече», «хлам», «озноб», «борщ», «железо». Если написать их подряд на латинице, получится *dtxt[kfvjpyj,,jho;tktpj* Отличный пароль! В нем есть строчные буквы и спецсимволы, он довольно длинный. Для его расшифровки потребуются 84 квинтильона (84 с 18 нулями) лет! Из-за своей непредсказуемости он подойдет даже для защиты финансовой информации.

Запомнить такой пароль будет немного легче, чем пароль из классического варианта. Слова «вече», «хлам», «озноб», «борщ», «железо» нужно связать в любую фразу, чтобы связать между собой. Скажем,



Это важно!

Главное правило работы с паролями: не использовать один пароль для нескольких сервисов. В этом случае вас могут взломать во всех социальных сетях и мессенджерах, причем довольно быстро. Создавайте каждый раз уникальный пароль, используя наши рекомендации.

«Собрались на вече, убрали хлам, почувствовали озноб, съели борщ и пошли поднимать железо». Могут быть и смешные варианты, главное, чтобы они запомнились.

Метод парольной фразы

Этот вариант удобен тем, что созданный пароль легче запомнить. Правда, есть риск сделать его предсказуемым, как описывалось выше. Давайте попробуем.

Итак, выберите короткую фразу, которую вы запомните. Это может быть цитата из 3-4 слов, любимая фраза вашей бабушки или срока из учебника. Выбирайте тщательно, ведь эта фраза будет с вами надолго.

Например, я выберу фразу «Что наша жизнь? Игра!» из оперы «Пиковая дама». Наберу ее на латинице без пробелов: *Xnjyfif;bpym&Buhf!* Знак вопроса в английской раскладке превратился в знак &, а восклицательный знак остался. Надежность пароля высокая, но он длинноват для дальнейшего использования.

Перефразирую: «Наша жизнь – игра!», получится *Yfif;bpym-buhf!* Для расшифровки этого пароля потребуется 82 миллиарда лет. Хороший пароль и запоминается легко.

Но нам нельзя использовать его в разных сервисах. Не придумывать же новый!

Метод парольной фразы предлагает нам решение: вы используете основной пароль (сложный, придуманный на основе фразы), а потом для каждого сервиса добавляете к нему символы.

Например, у меня получился пароль *Yfif;bpym-buhf!*

- Для ВКонтакте я буду использовать его вариант *Yfif;bpym-buhf!VK* или *Yfif;bpym-buhf!DR* (DR – это «VK» в английской раскладке).
- Для почты я использую вариант *Yfif;bpym-buhf!gjxnf* (gjxnf – это почта) или *Yfif;bpym-buhf!vskj* (vskj – мыло).
- Для Инстаграма – *Yfif;bpym-buhf!ajnr* (ajnr – фотки).

Иными словами, я буду писать в английской раскладке «Наша жизнь—игра!» и добавлять в конце или в начале символы, связанные с конкретным сервисом. Надежность пароля при этом очень высока. Скажем, указанный выше пароль для инстаграма можно взломать (если вы не читали эту книгу или не подсмотрели его часть) только за 33 секстильона (33 с 21 нулями) лет.

Советы по использованию пароля

- Не стоит использовать пароли на основе последовательностей на клавиатуре (например, *QWERTYUIOP* или *1QAZZWSX*). Их очень просто подобрать.

- Не используйте дату вашего рождения, кличку домашнего животного, свои увлечения, имена родных и друзей при составлении паролей. Хакеры часто пользуются «социальной инженерией» – узнают все о человеке, которого пытаются взломать. Потом все собранные данные служат основой для подбора пароля.
- По той же причине не используйте имена популярных артистов и спортсменов, названия брендов и фильмов.
- Не стоит хранить пароль в аккаунте социальной сети, а также на стикере, закрепленном на мониторе. Лучше хранить этот листочек в книге или папке в столе.

Уровень второй. Защита с подтверждением

Для надежной защиты аккаунта нам нужно установить второй рубеж защиты. Мы можем настроить свой аккаунт так, чтобы после ввода правильного пароля дополнительно требовалось ввести специальный код. Это называется двухфакторная аутентификация.

Это второй уровень защиты. Если даже злоумышленники подберут/узнают ваш пароль, они не смогут войти в ваш аккаунт, так как не смогут пройти аутентификацию.

Вы можете получить код для подтверждения входа разными способами: в смс на ваш телефон, с помощью специального приложения, в виде списка резервных кодов и др.

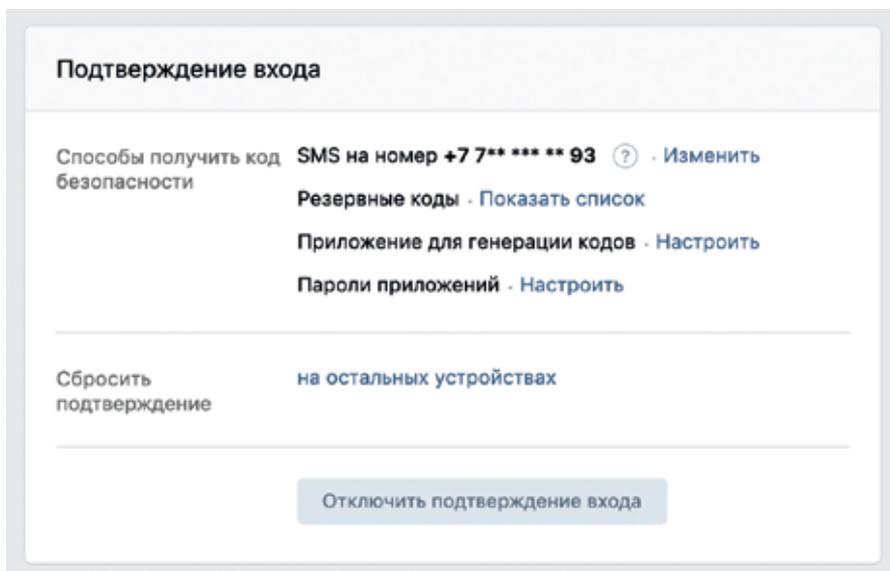
На момент создания книги двухфакторную аутентификацию поддерживают социальные сети ВКонтакте, Instagram, Facebook, «Одноклассники», мессенджеры Telegram, WhatsApp (6-значный pin-код при входе со смартфона), почтовые сервисы Gmail, Mail.ru, Yandex. Вы можете проверить, поддерживает ли сервис дополнительный уровень безопасности, поискать в справке сервиса или в поисковой системе.

Рассмотрим на примере ВКонтакте. Откройте социальную сеть на компьютере. Щелкните на свою фотографию в правом верхнем углу экрана, откройте настройки, затем раздел «Безопасность». Самый первый пункт – «Подтверждение входа». Укажите свой номер телефона, и вы защитите свой аккаунт почти на 100%.



Это важно!

Самый простой способ защититься: включить подтверждение входа с помощью кода в смс. Как правило, эта настройка включается в настройках безопасности сервиса.



Настройки безопасности вКонтакте

На примере вКонтакте рассмотрим другие варианты двухфакторной аутентификации.

Резервные коды позволяют подтверждать вход, когда у вас нет доступа к телефону, например, в путешествии. Каждым кодом можно воспользоваться только один раз. Распечатайте их, уберите в надежное место и используйте, когда потребуются коды для подтверждения входа.

Приложения для генерации кодов позволяют получать коды даже без подключения к сети и сотовой связи. Воспользуйтесь любым приложением для генерации кодов двухэтапной аутентификации. Например, Google Authenticator для iPhone, Android. Для работы с приложением щелкните по ссылке «Настроить».

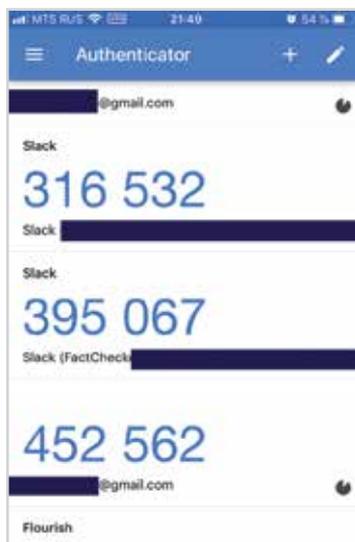
Подтверждение входа на сегодняшний день является самым доступным и надежным способом защиты аккаунта. Взломы аккаунтов стали бы крайне редким явлением, если бы пользователи интернета включили эту настройку в своих аккаунтах.

Самый частый вопрос, который задают о двухфакторной аутентификации: «Мне нужно будет каждый раз вводить этот код, когда я захожу в соцсеть?». Пользователи представляют себе этот трудоемкий процесс: ввод пароля, потом ожидание кода по смс...

Нет, ничего такого не будет. Вспомните, как обычно вы входите в соцсеть, мессенджер или почту? Вы просто щелкаете на закладку

в браузере или запускаете приложение. Так будет и с двухфакторной аутентификацией, и код вам понадобится только в самый первый раз для подтверждения. Потом вы на какое-то время вообще забудете о кодах и паролях (надеюсь, не навсегда).

Но при этом ваш аккаунт будет надежно защищен, и если какой-нибудь взломщик подберет пароль к вашему аккаунту (надеюсь, нет, ведь вы помните правила создания пароля), он столкнется с проблемой: ему потребуется код. А этот код только у вас (через смс, приложение или в распечатанном виде в сейфе). Так и закончится неудачный взлом, а вы будете спокойны.



Скриншот приложения Google Authenticator

Опасности входа в аккаунт на чужом компьютере

Завершим разговор о безопасности аккаунтов важным дополнением. Иногда нам приходится открывать личный аккаунт (социальной почты, почту) на компьютере в библиотеке, интернет-кафе. Школьники и учителя регулярно делают это в школе, в компьютерном классе, например. Давайте рассмотрим эту ситуацию с точки зрения безопасности.

Итак, для начала определим, что плохого может произойти? Вы вошли в соцсеть, почту, потом закрыли вкладку/браузер, может, даже выключили компьютер. Но знайте, что ваше имя и пароль для входа с большой долей вероятности сохранятся в браузере, и следующий пользователь этого компьютера сможет без проблем открыть ваш аккаунт, а значит, заглянуть в переписку, посмотреть личную информацию. Хотели бы вы этого? Наверняка, нет. Давайте разберемся, как защититься.

Сохранение паролей в современных браузерах настроено автоматически для удобства пользователей. Правда, в общественном месте эту функцию удобством не назовешь, её стоит отключать. Но что делать, если она включена? Быть внимательным. Когда вы вводите пароль, браузер вас спросит: сохранить ли его для дальнейшего использования. Твердо жмите «Нет». Это и есть решение против первой технологии.

Со второй технологией сложнее. Cookie – это данные, которые сайт хранит на компьютере, чтобы нам было удобно работать с этим сайтом. Так сайт «запоминает» нас и не требует пароль при каждом входе, определяет время последнего нашего входа и многое другое.

Когда вы входите в свой аккаунт на чужом компьютере, сайт сохраняет cookie с вашими данными на этом компьютере. Ваш аккаунт будет открыт, пока вы или кто-то другой не нажмет кнопку «Выход». Но даже в этом случае ваш аккаунт появится на странице входа в сервис, ожидая ввода пароля. Такие вот они прилипчивые, эти cookie.



Это важно!

Против нас на чужом компьютере работают две технологии: сохранение паролей в браузере и cookie.

Казалось бы, всё для удобства пользователей. Так оно и есть, если речь идет о домашнем компьютере. Но если компьютер общественный? Не хотелось бы оставлять свои данные и уж тем более открытый аккаунт. Что делать?

Стараться не входить в свои аккаунты на чужих компьютерах. Вы можете переслать сообщение, опубликовать файл в облачном сервисе, создать совместный документ – есть много способов сделать информацию доступной всем, не открывая свой аккаунт.

Но если вам всё-таки нужно открыть свой аккаунт, следуйте этой инструкции:

1. Переведите браузер в приватный режим (Firefox, Opera), режим инкогнито (Chrome). В этом режиме не будет сохраняться история просмотров, файлы cookie и данные сайтов, сведения, которые вы отправляете через формы авторизации (логин и пароль).
2. Откройте нужный вам сайт, укажите логин и пароль. Введите код (у вас ведь уже включена двухфакторная аутентификация?).
3. После работы в аккаунте нажмите на кнопку «Выход».
4. Закройте браузер.

Для надёжности не мешало бы потом сменить пароль, но это уже зависит от вашей тревожности и степени доверия тому месту, где вы пользовались компьютером.

Если всё перечисленное выше вам кажется сложным, то, по крайней мере, будьте внимательны и ставьте галочку в чек-бокс «Чужой компьютер» при вводе имени и пароля (такие есть во ВКонтакте и Mail.ru) – это сделает ваш вход на чужом компьютере безопаснее.

ГЛАВА 8

КОНФИДЕНЦИАЛЬНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ



Никому не хотелось бы рассказывать публично о своих секретах, все имеют право на тайну переписки, любой из нас будет против использования наших фотографий и текстов без разрешения – эти постулаты обычной жизни переключались в цифровой мир. Но есть существенная разница. В Сети за нами постоянно следят, причём как легально, так и нелегально.

Все мы ежедневно тратим несколько часов в день на интернет и социальные сети. Мы сами оставляем там свой «цифровой след»: открываем сайты и заходим в приложения, листаем фотографии, смотрим видео, ставим лайки, пишем комментарии, публикуем тексты, фотографии. Всё это рассказывает о нас больше, чем мы хотели бы. Иногда мы даже не догадываемся, что может быть известно злоумышленнику, собирающему наши «цифровые следы», или о каком нашем действии в интернете мы потом пожалеем.

Источники проблем

Давайте рассмотрим подробнее, кто доставляет нам проблемы в интернете и какие наши слабые места использует.

Источник проблем	Цель	Способы достижения цели
<i>Рекламодатели</i>	Деньги	Рекламные сообщения, предложения товаров и услуг, акции
<i>Цифровые преступники</i>		
<i>Мошенничество</i>	Деньги, материальные ценности, аккаунты	Рекламные сообщения, предложения товаров и услуг, акции, выгодные предложения
<i>Компьютерные вирусы</i>	ПК, смартфон, аккаунты	Отправка вредоносных файлов, ссылок на сайты

Источник проблем	Цель	Способы достижения цели
<i>Вовлечение в противоправную деятельность</i>	Личность, психика	Сообщения, чаты, закрытые сообщества
<i>Кибербуллинг</i>	Личность, психика	Сообщения, чаты, комментарии в аккаунте жертвы, закрытые сообщества
<i>Грабители</i>	Деньги, материальные ценности	Мониторинг публикаций в аккаунтах (ценности в доме, отъезд), геометки
<i>Правоохранительные органы*</i>	Предотвращение распространения экстремистских и противозаконных материалов	Мониторинг публикаций в аккаунтах, комментариев и отметок «Нравится»

**В зависимости от законодательства страны*

Рекламодатели

Мы видим рекламу повсюду, во всех каналах коммуникации. Цель рекламы – продать аудитории товар или услугу, то есть, в конечном счете, реклама нацелена на деньги пользователей. Реклама всегда будет яркой, громкой, будет сообщать об уникальном торговом предложении.

Если не углубляться в теорию бизнес-моделей, можно кратко сформулировать главный подход интернет-сервисов: «Либо вы покупаете [подписку на сервис], либо вас продают [рекламодателю]». Следуя этому подходу, можно понять, почему так много рекламы на сайтах с бесплатным доступом и ощутить разницу при использовании оплаты. Например, подписка YouTube Premium позволяет пользователю смотреть видео без рекламы на всех поддерживаемых устройствах.

В целом реклама создает мощный информационный шум в интернете в виде рекламных постов в соцсетях, баннеров на сайтах, коротких роликов перед началом видео. Пользователи сети, конечно, быстро

адаптируются, и исследователи уже давно отмечают у них «иммунитет» от рекламы, например, «баннерную слепоту» – способность не замечать рекламу на сайтах.

При этом постепенно реклама становится всё более агрессивной, и мы все чаще получаем личные сообщения или письма с рекламным содержанием. Разумеется, чаще всего эта реклама приходит без нашего согласия. Это явление называется «спам», и в некоторых странах отправителя можно привлечь к ответственности. Если получится его найти.

Как устоять перед натиском рекламы и не читать бесконечные рекламные сообщения?

1. По возможности ограничьте вероятность незнакомым людям отправлять вам сообщения в социальной сети и мессенджере (зависит от интернет-сервиса).
2. В социальной сети закройте возможность писать на вашей стене (даже друзьям, ведь если их аккаунт будет взломан, то злоумышленник может опубликовать что-то на вашей стене). Обычно бывает достаточно комментирования.
3. Удаляйте сообщения рекламного характера, на которые вы не давали согласия, помечайте их как спам, жалуйтесь на них службе поддержки, блокируйте отправителей.
4. Старайтесь не указывать в интернете адрес основной электронной почты и номер телефона.
5. Зарегистрируйте отдельный адрес электронной почты для регистрации на сервисах.
6. Во всех ненужных рассылках от сайтов и сервисов ищите в письме ссылку «Отписаться от рассылки» и отписывайтесь.
7. Смело отмечайте как спам сообщения в почте, социальных сетях и мессенджерах. Современные сервисы используют машинное обучение и мощные фильтры спама, так что вы этим поможете себе и другим.

Мы рассмотрели только самые простые рекомендации. Современные рекламодатели идут дальше и анализируют намного больше информации о нас, пользователях интернета.

Так, например, вы должны точно понимать, что все наши действия в интернете фиксируются. Да-да, каждый раз, когда вы открываете со смартфона или компьютера сайт, этот факт фиксируется сразу в нескольких базах данных: как минимум, у провайдера связи (того, кто предоставил вам интернет) и у владельца сайта. Что они знают? Ваш

IP-адрес в сети, модель устройства, его настройки, могут знать историю вашего просмотра сайтов, количество открытых страниц, время на сайте и глубину просмотра каждой страницы. Это неполный перечень возможностей современных систем интернет-аналитики. В результате анализа сервис аналитики определяет ваш возраст и пол, может определить ваши аккаунты в социальных сетях, а затем – электронную почту и телефон, если вы их опубликовали там.

Понимание того, что в интернете фиксируются все наши шаги, должно сделать вас осторожнее и внимательнее. Вы должны точно понимать, к чему приведут самые обычные, на первый взгляд, действия.

Действие	Результат	Способ защиты
Запрос в поисковой системе (Яндекс, Google)	Появление баннерной и контекстной рекламы на тему запроса	<i>Используйте поисковую систему без отслеживания DuckDuckGo</i>
Открытие рекламного сайта	Появление баннерной рекламы на тему сайта, рекламных постов в соцсетях и даже личных сообщений	<i>Используйте приватный режим (Firefox, Opera), режим инкогнито (Chrome). Установите специальное дополнение для браузера (AdBlock, uBlock, Privacy Badger или любое другое)</i>
Отправка адреса эл. почты или (что хуже) номера телефона на сайте (для регистрации, получения бесплатного контента)	Получение спама по эл. почте, в личных сообщениях, рекламных смс и звонков	<i>Нигде не указывайте основной адрес эл. почты и номер телефона</i>

Как обезопасить себя от цифровых преступников

Ниже мы выделили основные группы цифровых преступников. Одним из них нужны наши деньги, другим важно изменить наше психи-

ческое состояние. Все они опасны, и стоит подумать, как защититься от них.

Мошенничество

«Вы получили перевод», «Вы выиграли в лотерею», «Мой дядя оставил вам завещание», «Последний день распродажи со скидкой 99%» – эти и похожие сообщения получают пользователи интернета ежедневно. Почта, социальные сети, сайты, смс-мошенники могут использовать все возможные каналы распространения, чтобы заманить в свои сети наивных пользователей.

Что объединяет подобные сообщения от мошенников? Какие можно выделить признаки сообщения от мошенников?

- Обещание быстрой и легкой выгоды (получения товара, денег, услуги).
- Ограничение во времени (нужно действовать скорее, чтобы не было возможности обдумать).
- Ограничение предложения (остался последний товар, последний день).

Сообщения мошенников похожи на агрессивную рекламу. Они могут быть яркими, «кричащими», вызывающими эмоции и действия. Но всё может закончиться очень печально: вы переводите деньги и ничего не получаете взамен.

Другая категория мошенников может маскироваться под добросовестных бизнесменов. Вы обнаружите у них солидный сайт или хорошо оформленное сообщество в соцсети. Всё сделано красиво и «по-настоящему», чтобы покупатели поверили. Держите ухо востро! Не стоит переводить деньги до получения товара или услуги, всегда ищите или спрашивайте о варианте оплаты после получения. Предоплату нужно делать только на проверенных сайтах и приложениях. Например, на некоторых сайтах (Aliexpress, Ebay) применяется защита покупателя. Если вы не получили товар или у вас есть претензии к нему, вы можете вернуть свои деньги.

Есть мошенники, специализирующиеся на обмане с банковскими картами или переводами. Если у вас уже есть банковская карта, вы можете получить сообщение о переводе или зачислении средств на вашу карту или счет телефона. Разумеется, ни перевода, ни зачисления не было. Мошенник после этого свяжется с вами и предложит решить «проблему». Он попросит у вас сообщить номер карты и CVV-код на обороте, после чего вы лишитесь всех денег. Помните о том, что никто (даже работники банка) не могут спрашивать ваш CVV-код. А проблемы с ошибочными переводами можно решить в отделении банка или у оператора связи, но никак не с вашим участием.

Отдельно стоит выделить мошенников, отправляющих ложные письма от сервисов и банков (фишинг). Эти письма вызывают доверие: в них есть логотип компании, фирменные цвета, к вам могут обратиться по имени. Поверив содержанию письма, вы можете ввести на открывшемся сайте логин и пароль, потеряв навсегда доступ к аккаунту. А если мошенник создаст копию сайта вашего банка? Вы навсегда потеряете все свои деньги.

Как защититься от подобных мошенников?

1. Следуйте всем рекомендациям из предыдущего параграфа (о защите от рекламы), так как мошенники используют те же уловки. Удаляйте сообщения мошенников, помечайте их как спам, жалуйтесь на них службе поддержки, блокируйте отправителей.
2. Критически относитесь ко всем неожиданным и выгодным предложениям. Помните о трех признаках сообщений мошенников. Не действуйте сгоряча, подумайте о последствиях, спросите совета у близких, поищите информацию о продавце (сайте, сервисе) в интернете.
3. Проверяйте отправителей писем. Реальные компании указывают полное имя отправителя, а адрес эл. почты содержит название компании. Например, вряд ли реальному банку или магазину будет принадлежать адрес эл. почты cimba.pimba@yahoo.com.
4. Не указывайте нигде в интернете, по почте и в смс номер вашей карты, имя владельца, дату окончания действия и CVV-код. Разумеется, это относится и к банковским картам ваших родителей. Помните, что платить онлайн можно только со старшими!
5. Для платежей через интернет откройте виртуальную карту (это возможно сегодня во многих банках). Перечисляйте на неё средства только перед переводом.
6. Не покупайте ничего в интернете со 100% предоплатой. Ищите варианты с оплатой при получении. Если вы всё-таки платите заранее, убедитесь в надёжности сайта.
7. Не верьте объявлениям в социальных сетях. Настаивайте на личной встрече, ничего не высылайте и не переводите первым. Лучше потерять время или заплатить больше в обычном магазине, чем потерять всё.

Компьютерные вирусы

Целью злоумышленников, распространяющих компьютерные вирусы, как правило, является личная информация о пользователях (файлы ком-

пьютера; информация, отправленная в интернет, включая пароли и данные карт), получение доступа к аккаунтам в интернете, блокировка компьютера с дальнейшим шантажом, включение компьютера в сеть для атак сайтов (ботнет) и другие. Иногда вирусы распространяются ради развлечения.

Как защититься от вирусов?

1. Установить на компьютер антивирус. Есть масса бесплатных антивирусов достаточно хорошего качества, например Avast.
2. Настроить «Защитник Windows», если вы пользуетесь этой операционной системой. Стоит отметить, что операционные системы Macintosh и Linux менее подвержены воздействию вирусов.
3. Нельзя открывать ссылки в письмах, сообщениях и смс без проверки. Особенно это касается писем от незнакомых людей, но и сообщениям от друзей доверять не стоит. Что произойдет? Вы получаете письмо со ссылкой, щелкаете по ней и открываете сайт с вредоносным кодом, заражая свой компьютер или смартфон. Сообщения могут быть самые привлекательные: обещание чего-то интересного или важного. Злоумышленники могут маскироваться под правоохранительные органы или бизнес, предлагая перейти по ссылке на сайт. Стоит дважды проверить, прежде чем открывать ссылку. Другой вариант: вы получаете сообщение от друга: «Привет! Смотри, какое о тебе сняли видео!», ниже – ссылка. Как только вы переходите по ней, вирус заражает ваш компьютер или аккаунт (от вас сотнями уходят вирусные сообщения). Ссылки можно проверить в разных сервисах проверки ссылок на вирусы. Например, в онлайн-сканере Dr.Web для проверки подозрительных ссылок <https://vms.drweb.ru/online>.
4. По той же причине нельзя скачивать и открывать файлы из писем и сообщений, особенно от незнакомых отправителей. Вам приходит письмо с фотографией, файлом Word или видео, и вы открываете файл, активируя вирус.

Вовлечение в противоправную деятельность

Но не только деньги и материальные ценности интересуют злоумышленников. Некоторым из них хочется получить власть над вашей личностью, чтобы управлять вами. Спустя время жертвы жалеют о том, что отправились к ним на встречу или занялись экстремистской деятельностью. Иногда, к сожалению, главной целью подобных преступников является доведение до самоубийства. Как избежать печальных последствий?

1. Максимально защитите себя от внимания незнакомых людей. Не добавляйте в друзья тех, кого вы плохо знаете. Если человек старше вас, лучше спросить совета у взрослых. Есть такой подход к добавлению в друзья: напишите обобщённый портрет того, кого добавляете в друзья. Например, это люди, которых вы знаете лично, либо те, чьи публикации вам интересно и полезно читать, люди известные, разделяющие ваши взгляды и интересы. Добавляйте в друзья таких людей.
2. Проверяйте аккаунты людей, которые вам написали сообщение, комментарий, поставили лайк или пытаются добавиться в друзья. Возможно, это фейковый аккаунт. Как его определить?
 - Проверьте фото на аватаре. Если там нет портрета или это фото принадлежит другому человеку, у вас есть основания думать, что это фейковый аккаунт.
 - Если возможно, посмотрите список друзей. Если у вас есть общие друзья, вы можете спросить у них об этом человеке.
 - Посмотрите, о чём и как часто были публикации. Отсутствие постов или большое количество репостов дают основания думать, что это фейковый аккаунт.
 - Обратите внимание на активность друзей пользователя на странице. Если активности нет или она очень слабая – это тоже может быть признаком фейка. Имейте в виду, что фейк может «дружить» с другими фейками, так что друзей фейка тоже стоит проверить.
 - Отсутствие данных в разделе «личная информация» может быть признаком фейка.
 - Один из способов разоблачения фейка – это прямые вопросы. Но стоит понимать, что общение с злоумышленником, который наверняка обладает навыками убеждения, может закончиться не в вашу пользу. Не рекомендуется общаться с незнакомцами в интернете, даже для того, чтобы «вывести их на чистую воду».
 - Закрытый аккаунт незнакомца также не стоит добавлять в друзья.
3. Ограничьте возможность незнакомым людям отправлять вам сообщения в социальной сети и мессенджере (зависит от интернет-сервиса).
4. В социальной сети закройте возможность писать на вашей стене.
5. Ещё одна уловка для злоумышленников – это тематические сообщества в социальной сети и чаты в мессенджерах. Современный

интернет дал нам возможность находить единомышленников в разных увлечениях. Чем бы мы не интересовались: от спорта до кино – мы найдем в сети тех, кто поддержит наш интерес, с кем будет интересно обсудить общие темы. В этом случае от общения в интернете мы получаем пользу и удовольствие.

При этом всегда стоит обращать внимание, когда разговор в сообществе или в чате уходит в сторону от главной темы. Злоумышленники иногда маскируются под обычных пользователей, приходят в тематические сообщества, участвуют в обсуждениях, знакомятся с участниками, а потом заводят разговоры о жизни. Вы должны помнить: любые беседы о вашей личной жизни, семье, ваших ценностях и мотивах могут быть неспроста. Часто преступники владеют навыками психолога, позволяющими разговорить и расположить к себе человека.

Каждый момент, общаясь с кем-то в интернете, вы должны себя спрашивать: а тот ли это человек, за которого себя выдаёт? Вы думаете, что это девушка или юноша, ваш сверстник, а на самом деле это может быть бородатый мужчина, который умело маскируется. Иногда в этом случае пользователи интернета решаются проверить, кто этот человек, назначая встречу в реальности. Нельзя этого делать, это тоже может быть ловушка.

Что же делать, скажете вы? И верить нельзя, и встречаться, чтобы проверить, тоже нельзя? Да, из соображений безопасности. Как показывает опыт, и общение «по душам» с незнакомцами онлайн, и встречи «чтобы проверить» могут привести к печальным последствиям. Главная защита – это полное ограничение общения с незнакомыми людьми в интернете, особенно на личные темы. Нужно отклонять предложения добавиться в друзья, ограничить незнакомцам возможность писать сообщения и комментарии.

Тролли (кибербуллинг)

Буллинг (от английского bullying – «запугивание», «издевательство», «травля») – это агрессивное преследование одного из членов коллектива (школьников и студентов) со стороны другого члена коллектива. Буллинг не всегда выражается в физическом нападении. Чаще происходит психологическое насилие в форме словесной травли (оскорбления, злые и непристойные шутки, насмешки и прочее), распространения слухов и сплетен, бойкота.

Важно сразу отметить, что травля во многих странах квалифицируется как правонарушение, поэтому мы поместили буллинг в раздел «Цифровые преступники». В любом случае жертва буллинга может получить помощь от старших (родителей, учителей, полиции). Главное – не молчать о проблеме.

Травля человека в интернете получила название «кибербуллинг». Благодаря технологиям буллинг в интернете стал более опасным благодаря трем дополнительным возможностям.

Угроза	Как защититься
<p>Круглосуточное вмешательство в личную жизнь. Агрессор может писать вам днём и ночью в социальных сетях или по смс.</p>	<p>Заблокировать агрессора, пометать его комментарии и публикации как спам.</p>
<p>Неограниченность аудитории, быстрота распространения информации. Сообщения могут быстро распространяться в сети, их может увидеть большая аудитория.</p>	<p>Блокировка сообщений в сообществах, жалоба на сообщения в службу поддержки (пункт «Пожаловаться» у публикаций есть во всех социальных сетях). Публичное признание факта травли в интернете может сыграть против агрессора. Напишите в своем аккаунте о том, что происходит – так вы получите поддержку от своих друзей и объясните им появление оскорбляющих вас публикаций и комментариев.</p>
<p>Анонимность преследователя. Агрессор может действовать анонимно, создав фейковый аккаунт.</p>	<p>Снова помогут блокировка агрессора и публичное признание факта травли. Лишение агрессора анонимности тоже может помочь, но не так сильно, как кажется.</p>
<p>Возможность использования личной информации. У каждого пользователя социальных сетей в аккаунте содержится много личных данных, фотографий, видео и публикаций, которые могут стать объектами насмешек.</p>	<p>Блокировка агрессора, ограничение доступа к фотографиям, видео и стене для тех, кто не является вашим другом. Если оскорбляющие вас публикации появляются в аккаунте агрессора, можно отправить жалобу на него. Если это происходит в сообществе, сообщите администратору или службе поддержки.</p>

Итак, агрессор может писать вам сообщения, комментировать ваши публикации, размещать о вас публикации у себя в аккаунте или в сообществе. Все эти действия можно заблокировать или отправить жалобу на них. Кроме этого, нужно сообщить о факте травли всем, включая взрослых.

Грабители

Это малозаметная группа злоумышленников, но они существуют и черпают информацию в том числе из социальных сетей. Пользователи сами рассказывают в своих аккаунтах о дорогих покупках, предметах роскоши, ценностях, без боязни публикуют интерьеры своего дома и детали жизни. Немудрено, что человек, задумавший кражу, может довольно быстро решиться на неё, глядя на публикации в аккаунте.

Особенно удобно будет организовать кражу, когда вы сообщите всем, что поехали всей семьей в отпуск. Вы радуетесь новым впечатлениям, а злоумышленник уже подбирает ключ к вашему замку. Он уже прочитал все посты о ваших украшениях и бытовой технике и ждет момента, когда сможет их забрать. Как только вы написали, что поехали на неделю на курорт, домушник отправляется к вам.

Конечно, вы можете делиться радостью от поездки с друзьями, но публикации об этом стоит делать только «для друзей». При этом нужно быть уверенным, что в списке друзей нет постороннего человека.

Не нужно хвастаться в социальных сетях и мессенджерах дорогими приобретениями, украшениями и прочим, что может привлечь внимание грабителей. Не стоит также писать в публичном доступе о времени вашего отсутствия, особенно если в вашем доме никто не остается.

Что знают правоохранительные органы

Правоохранительные органы в каждой стране занимаются мониторингом социальных сетей и мессенджеров для предотвращения распространения экстремистских и противозаконных материалов. Что это может быть? Довольно большой перечень: пропаганда насилия и нетерпимости (в том числе по национальному, религиозному признаку), призывы к насилию или свержению власти, пропаганда наркотических веществ, алкоголя и другое.

Кажется, что каждый воспитанный и законопослушный гражданин и так не будет публиковать ничего подобного. В чем угроза?

Дело в том, что пользователи интернета недостаточно осведомлены о том, какие материалы являются противозаконными или не понимают,

какие действия могут быть опасными для них с точки зрения закона. Рассмотрим по порядку:

Нельзя публиковать и репостить любые материалы:

- призывающие к осуществлению экстремистской деятельности,
- оправдывающие необходимость такой деятельности,
- публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство,
- оправдывающие практику совершения военных или иных преступлений,
- призывающие к насилию по отношению к этнической, социальной, расовой, национальной или религиозной группы,
- пропагандирующие наркотические и психотропные вещества,
- пропагандирующие суицид и провоцирующие его совершение,
- содержащие материалы порнографического характера,
- содержащие нецензурные слова и выражения,
- содержащие любую информацию противоправного характера.

Большой список, правда? И даже он не полный. Стоит помнить, что все наши действия в интернете фиксируются, это не анонимная среда. В онлайне не получится не соблюдать законы страны.

Обратите внимание, что публикация и репост для правоохранительных органов – одинаковое по значимости действие. Да, может быть, изначально пост был не ваш, но вы его распространяете. Значит, вы тоже виноваты.

Здесь есть один важный нюанс: не всегда суды и полиция учитывают, с каким комментарием вы делали репост публикации. Иногда суды и полиция привлекают к ответственности и тех, кто против незаконной деятельности. Возможно, вы хотели осудить насилие или потребителей наркотиков и сделали репост чьей-то записи. Ваше осуждение понятно, но сделав репост, вы распространили противозаконные идеи, призывы. Вопреки вашему замыслу кто-то, напротив, может принять их.

Будьте осторожны, не делайте репостов! Не помогайте злу распространяться. Можно написать об этом явлении свой пост, упомянув о том, что вы видели.

Во-первых, как уже написано выше, ваш комментарий суд или полиция могут расценить как поддержку. Во-вторых, комментарии и «лайки» повышают этот пост в рейтинге ленты социальной сети. Ваши действия будут



Это важно!

Не стоит комментировать публикации с противозаконным содержанием и уж тем более ставить им «лайк».

способствовать тому, чтобы этот пост увидели ещё больше людей. Зачем это делать?

Обращайте внимание на название сообщества, его «шапку», описание, просмотрите посты за последние две недели. Иногда безобидное, на первый взгляд, сообщество публикует раз в неделю публикации экстремистского содержания.

Выходите и отписывайтесь от таких групп сразу, как увидели подобный пост. Можно также отправить жалобу в службу поддержки.

Если ваш друг внезапно начал это делать, уточните, возможно, его аккаунт взломан, либо он связался с плохой компанией.



Это важно!

Не вступайте в сообщества и чаты, где публикуют противозаконные или сомнительные с точки зрения закона публикации.



Это важно!

Отписывайтесь от «друзей» в социальных сетях, которые публикуют противозаконный контент.

Практика. Как сохранить личное пространство в соцсетях

Мы подробно описали различные источники проблем пользователей интернета и рассмотрели варианты их предотвращения или решения. Как правило, многие советы сводились к правильной настройке аккаунта социальной сети: закрыть незнакомцам возможность писать сообщения, запретить делать публикации на вашей стене, закрыть возможность комментирования и т.д.

Давайте рассмотрим, как выглядит ваш аккаунт для окружающих и какие у него слабые места. Проведем эксперимент на примере социальной сети ВКонтакте или любой другой, которой пользуются большинство ваших одноклассников. Посмотрите на свой аккаунт глазами трёх пользователей интернета: вашего друга в соцсетях, незнакомого вам пользователя соцсети и совсем постороннего.

Для первой части эксперимента вам потребуется, например, смартфон вашего друга, который подписан на вас в соцсети. Пусть друг откроет ваш аккаунт в приложении и даст смартфон вам в руки. Для второй части вам понадобится найти человека, которого вы не добавляли в друзья в социальной сети. Для третьей части вам нужно временно выйти из своего аккаунта и открыть его в отдельной вкладке, не вводя имя и пароль. Так вас будут видеть все, кто не зарегистрирован в социальной сети.

Итак, посмотрите на свой аккаунт по очереди в трех вариантах и отметьте, что вы можете увидеть. Ставьте по баллу за каждый пункт.

1. Фотографии профиля.
2. Телефон, эл. почта.
3. Фотографии, на которых вы отмечены.
4. Список ваших друзей.
5. Список ваших групп.
6. Ваши отметки и/или фотографии на карте.
7. Ваши фотоальбомы.
8. Публикации на стене.

Если в первой части эксперимента («взгляд друга») вы насчитали 8 баллов – это значит, вы доверяете своим друзьям.

Задумайтесь только о том, все ли пользователи вКонтакте, которых соцсеть называет друзьями, действительно являются вашими друзьями. Вы действительно готовы каждому из списка «друзей» вКонтакте доверить информацию из списка выше?

Во второй части («взгляд пользователя соцсети») будет плохо, если вы наберете от 4 до 8 баллов. Лучшие – не более 4 баллов.

Особенно чувствительная информация из списка – контактная (телефон, эл. почта), отметки на карте и фотографии, на которых вы отмечены. Плохо, если она доступна тем, кто не является вашим другом в соцсети.

Почему? Если любой пользователь соцсети видит ваши контакты, вас могут внести в базу для спам-рассылки или рекламных звонков, смс. Отметки на карте – это подробный рассказ о вашей жизни, работе, отдыхе. Зачем этим делиться с незнакомцами? Фотографии, на которых вы отмечены, часто не контролируются вами. Вы можете следить за своими фотоальбомами, но ваши друзья будут публиковать фото с вечеринки, которые вы не хотели бы показать незнакомым людям. Представьте, что ваш аккаунт смотрит ваш будущий работодатель (такая практика уже существует). Это как раз «взгляд пользователя соцсети». Что вы хотели бы ему показать, а что нет?

В настройках вКонтакте предусмотрена возможность посмотреть на аккаунт так, как его видят другие пользователи сети. Откройте настройки, затем раздел «Приватность» и найдите ссылку в нижней части страницы. Вы также можете открыть свой профиль и дописать в адресной строке в конце адреса «?as=-1». Например, https://vk.com/id***?as=-1. Так вашу страницу видит незнакомый вам пользователь.

В третьей части эксперимента («взгляд со стороны») в идеале вы должны получить 0-3 балла. Очень плохо, если от 4 до 8. Всем, кто не зарегистрирован в соцсети, вообще ничего не должно быть доступно в вашем аккаунте. Может быть, только ваше имя и фотография профиля.

Сегодня во многих соцсетях есть возможность закрывать профиль от всех, кроме друзей. На наш взгляд, это оптимальная настройка безопасности для большинства пользователей до 18 лет.

Если же вы оставляете профиль открытым, внимательно проверьте настройки доступа к информации в вашем профиле. Эти настройки есть в каждой социальной сети.



Домашнее задание

Мы собрали для вас информацию о настройках приватности в социальных сетях в одну таблицу ниже. Внимательно рассмотрите возможности каждой сети. Определите, насколько вы защищены. Включите настройки приватности в вашем аккаунте.

Настройки приватности социальных сетей, август 2019*

Настройки				
Включение закрытого аккаунта (только для друзей)				
Расширенные настройки доступности информации аккаунта (группы, контент, геометки, друзья)				
Публикация сетевого статуса				
Возможность другим пользователям делиться историями				
Расширенные настройки историй (просмотр, ответы, реакции)				

Настройки				
Настройки доступа к публикациям в отдельности	⊖	*** ⊕	⊖	⊕
Возможность другим пользователям публиковать сообщения на странице	⊖	⊕	⊖	⊕
Настройки доступа к фотографиям (просмотр, репост)	⊖	⊖	⊕	⊕
Контроль отметок в публикациях	⊕	⊕	⊕	⊕
Контроль автоматической отметки на фото	⊖	⊖	⊕	⊕
Контроль комментариев	⊕	⊕	⊕	⊕
Отключение возможности отправлять сообщения	⊖	⊕	⊕	**** ⊖
Контроль доступности аккаунта для поисковых систем	⊖	⊕	⊕	⊕
Поиск по номеру телефона	⊖	⊕	⊖	⊕

**Данные приводятся на август 2019 года. Версии настроек могут отличаться от времени и региона. Социальная сеть может изменить настройки, убрать или добавить новые.*

***Платная возможность*

****Только два варианта: открытая публикация и для друзей*

*****Автоматическая фильтрация для всех, кто не является другом в соцсети*

ГЛАВА 9

**ПРОВЕРКА НА ДОСТОВЕРНОСТЬ
ФОТО И ВИДЕО**



В этом разделе вы узнаете, как превратить свой ноутбук в инструмент современного Шерлока Холмса. И это совсем не преувеличение. Вы научитесь проверять достоверность фото- и видеоматериалов и познакомитесь с инструментами, которые помогут вам в несколько кликов понять, насколько достоверна визуальная информация, оказавшаяся на вашем экране.

С ростом количества дезинформации и фейков, которые попадают в наше инфополе, к счастью, растёт и число технических решений, которые помогают с фейками бороться. Может показаться, что проверка контента на достоверность — занятие долгое и неблагодарное, но на самом деле иногда достаточно одной-двух минут, чтобы убедиться в подлинности материала или его подмене.

Инструменты проверки фото и видео на достоверность



УПРАЖНЕНИЕ 1

Фейк или нет?

Посмотрите на это фото. Оно было опубликовано на более чем десяти крупных новостных сайтах с заголовком «Строители под Шымкентом обнаружили скелет динозаврика».



Каковы ваши предположения по поводу этого фото и подписи?

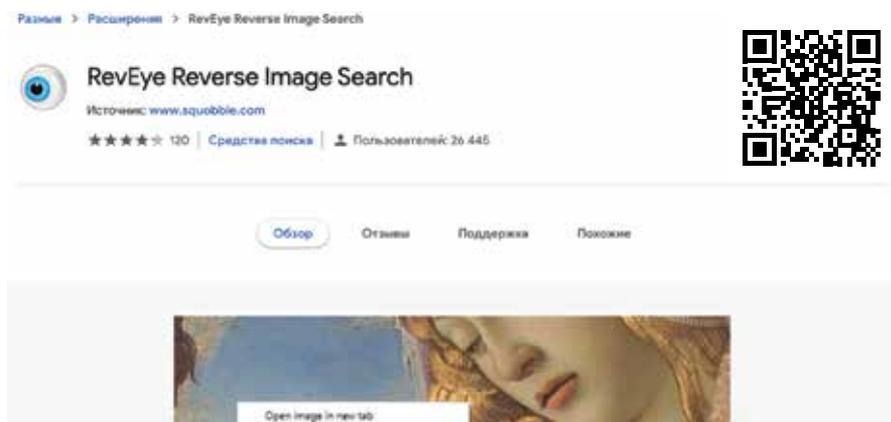
- а) это действительно скелет динозаврика;
- б) подпись не соответствует тому, что запечатлено на фото;
- в) это фото смонтировано в Photoshop или другой программе для обработки фото.

Кто производит фото- и видеофейки

Хотя из-за их количества может показаться, что фейки массово производятся с какой-то определённой целью группами людей или отдельными злоумышленниками, на деле это не так. В действительности большая часть фото- и видеофейков создаётся «на коленке» случайными пользователями, которые делают их от скуки или не предполагая какой-либо широкий охват. Скучающие где-нибудь в Алматы или Алгабасе Василий, Серик или Акбота видят фотографию, придумывают к ней забавную (по их мнению) подпись и выкладывают в своих аккаунтах в социальных сетях. А поскольку, как вы уже знаете, информация в наше время распространяется моментально и уровень критического мышления в обществе невысок, такие фейки легко расходятся в социальных сетях, а могут даже пробиться и на новостные сайты. Конечно, есть и те, кто производит фейки целенаправленно, чтобы посеять панику или ненависть, но таких «производителей» меньшинство.

Как вы уже поняли из анализа фото с «динозавриком», главная ваша сила это внимательность к деталям. Первое, что стоит сделать с присланным вам фото или видео, рассмотреть детали — возможно ли вообще такое в реальности и нет ли на фото признаков монтажа. В дополнение к этому есть ряд инструментов, которые помогут вам проверить, где впервые появилось фото и действительно ли на нём изображено то, что озвучено в подписи к фото.

Если вы пользуетесь браузером Chrome (а мы очень рекомендуем пользоваться именно им) или Firefox, то установите расширение RevEye (<https://tinyurl.com/yyvtaah3>).



Оно позволит вам в два клика проверить любую фотографию по всем поисковым машинам: Google, Yandex, Bing, TinEye и даже в китайском Baidu. Искусственный интеллект этих поисковых систем позволяет найти самое старое, самое большое или самое зафотошопленное изображение.

Все эти технологии поиска основаны на разработках Google. Самый простой способ проверить фото с вашего смартфона — сохранить картинку и загрузить её в Google Картинки (<https://www.google.com/imghp>).



Там вы можете выставить параметры поиска: искать ли самое большое изображение, точно совпадающее, или искать изображение, опубликованное в определённый период времени.

А как же Яндекс?

Стоит сказать, что поиск Яндекса по картинкам (совершенно аналогично устроенный на первый взгляд) может дать вам гораздо более точные результаты, особенно если вы ищете фото, на котором чётко видны лица людей. Алгоритмы искусственного интеллекта поисковой системы Яндекс позволяют даже найти социальные аккаунты незнакомого вам человека, случайно попавшего на фото (конечно, если он беспечно относится к конфиденциальности своего аккаунта). Поэтому, если вы не нашли ничего в одном поисковике — попробуйте другой. Иногда даже весьма непопулярный в Казахстане Bing может принести точные результаты.



Это важно!

- Перед тем как проверять изображение с помощью технических средств, рассмотрите его внимательно. Фейки чаще всего очень грубо смонтированы и следы монтажа видны невооружённым глазом — могут отсутствовать тени, наклон деревьев не соответствовать направлению ветра, части фотографии могут неестественным образом перекрывать друг друга, люди на фото могут быть одеты не по погоде и так далее. Ваша логика — ваш главный помощник!
- Важно читать подписи к фотографиям, поскольку у двух абсолютно идентичных изображений могут быть разные описания. Как мы уже говорили — это один из наиболее распространенных методов создания фейков.

- Если логика не помогла и вы начали поиск, то помните, что изображение, которое вы ищете, может состоять из двух скомпонованных частей, снятых в разное время и в разных местах. Вы можете обрезать изображение в любом графическом редакторе и искать каждую из его частей по отдельности. Это часто помогает при анализе смонтированного фото. Изображение также могут отзеркалить, поэтому попробуйте отзеркалить его обратно в графическом редакторе и заново провести поиск.
- Для анализа фото на предмет использования Photoshop и монтажа можно использовать сайт Forensically, который покажет вам, как определить врезки на фото.

Казахстанский кейс

Давайте рассмотрим фейк, проанализированный казахстанским фактчекинговым сайтом Factcheck.kz.

Портал «Новости Усть-Каменогорска и ВКО» 19 июля 2017 г. сообщил, что жители Восточно-Казахстанской области стали получать через Whatsapp фото градин и овец, якобы убитых ими, с текстом, утверждающим, что это произошло именно в их местности.

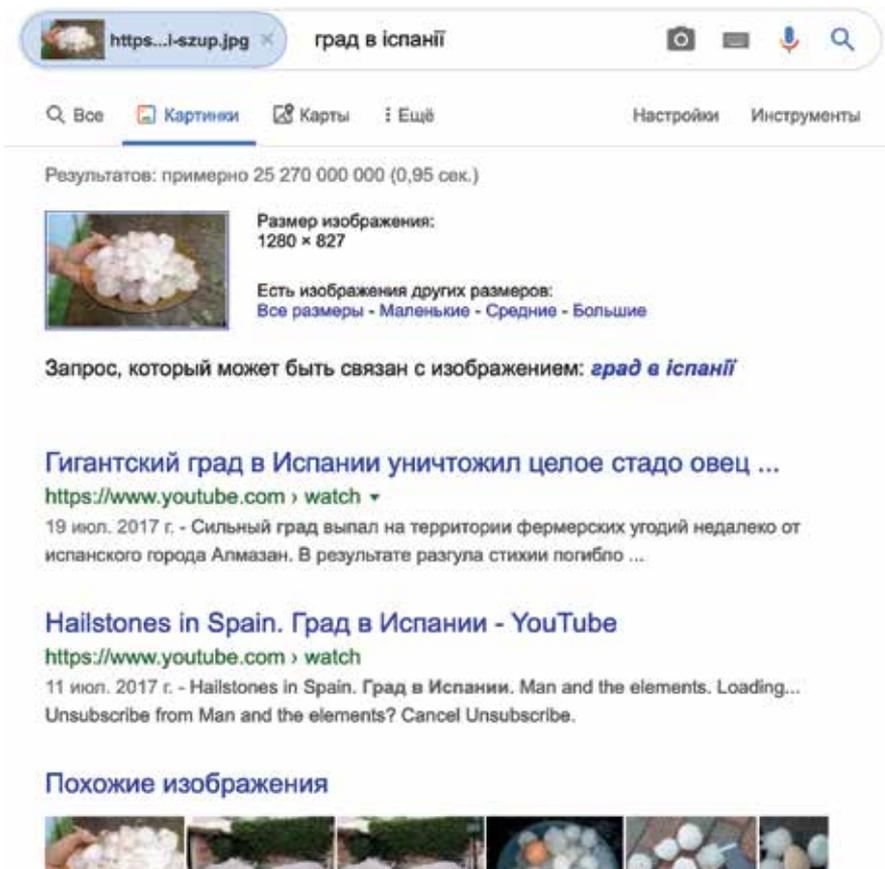
Жителям ВКО присылают фейковую новость о «граде в Георгиевке»

Область 19 июля 2017, 16:01 6386 Поделиться ▾



Мы можем проверить это фото с помощью *Google Image Search*.

Как мы видим на скриншоте ниже, фото градин иллюстрирует событие, произошедшее также в июле, но 18 числа в Испании, где выпал необычайно крупный град.



The screenshot shows a Google Image Search interface. At the top, there is a search bar with the URL 'https...i-szup.jpg' and the search term 'град в іспанії'. Below the search bar, there are navigation options: 'Все', 'Картинки', 'Карты', and 'Ещё'. To the right, there are links for 'Настройки' and 'Инструменты'. The search results section shows 'Результатов: примерно 25 270 000 000 (0,95 сек.)'. The first result is an image of a hand holding a large amount of hailstones. To the right of the image, it says 'Размер изображения: 1280 x 827' and 'Есть изображения других размеров: Все размеры - Маленькие - Средние - Большие'. Below the image, there is a suggestion: 'Запрос, который может быть связан с изображением: град в іспанії'. There are two search results listed below, both from YouTube. The first is titled 'Гигантский град в Испании уничтожил целое стадо овец ...' with a link to 'https://www.youtube.com > watch' and a description: '19 июл. 2017 г. - Сильный град выпал на территории фермерских угодий недалеко от испанского города Алмазан. В результате разгула стихии погибли ...'. The second is titled 'Hailstones in Spain. Град в Испании - YouTube' with a link to 'https://www.youtube.com > watch' and a description: '11 июл. 2017 г. - Hailstones in Spain. Град в Испании. Man and the elements. Loading... Unsubscribe from Man and the elements? Cancel Unsubscribe.'. At the bottom, there is a section titled 'Похожие изображения' with a row of six small thumbnail images showing various scenes of hail.

Другое фото — то, что с погибшими овцами — использовалось еще раньше, мы можем найти его на агрегаторе изображений *imgur* через поисковый сервис *TinEye**. Оно датируется 2015 г. (!). С помощью плагина *RevEye* вы сможете проверить практически любое фото в два-три клика мыши.

* Следует учитывать, что *TinEye* анализирует фото медленнее, чем гиганты вроде *Google* и *Яндекс*. Однако, если фото использовалось несколько раз ранее, это один из самых удобных и надёжных способов проверки.



87 results

Searched over 38.1 billion images in 0.8 seconds

Using TinEye is private. We do not save your search images. TinEye is free to use for non-commercial purposes. For business solutions, learn about our technology.

Sort by oldest

Filter by domain/collection

< 1 of 9 >



imgur.com

[a/aFjfx](#) - First found on Oct 22, 2015

Filename: [NB7yS61.jpg](#) (432 x 720, 59.8 KB)



reddit.com

[r/WTF/comments/3ptnzn/nasa_says_south...](#) - First found on Nov 29, 2015

[r/WTF/related/3ptnzn/nasa_says_south...](#) - First found on Jun 04, 2016

[view all 3 matches](#)

Filename: [NB7yS61.jpg](#) (480 x 270, 33.0 KB)

Пример смонтированного фото



Фейковое фото известного гитариста Джими Хендрикса с аккордеоном



Оригинальное фото



УПРАЖНЕНИЕ 1 Анализ фото



- а) Проанализируйте фотомонтаж Джими Хендрикса с аккордеоном. Расскажите, какие признаки указывают на то, что это фейк?
- б) Попробуйте проверить фото по ссылке <https://imgur.com/s7aMEw8> с помощью инструмента RevEye. Из каких фотографий смонтирован этот фейк?



Домашнее задание

Посмотрите обучающие ролики по работе с

1. Google Image Search и RevEye (<https://youtu.be/rb6pKCWCKqE>)
2. Forensically (https://youtu.be/XRCq8CJrl_s)

Обсудите инструменты с учителем.



Проверка видео

Итак, вам прислали ссылку на видео или вы увидели его в соцсети. Прежде чем отправлять его своим контактам, делать репост или оставлять комментарий, проверьте, не вводят ли вас в заблуждение.

Логично ли то, что происходит на видео

Это первый вопрос, который стоит себе задать. Алгоритм тот же, что и с фото — соответствует ли то, что происходит на видео, подписи к нему? Не пытаются ли с помощью подписи манипулировать вами (см. раздел «логические уловки» в главе о формальной логике). Уже на этом этапе довольно часто можно с большой вероятностью определить, фейк это или нет.

Как проверить видео на оригинальность

Подобное могли выложить в интернете ранее, вполне возможно в ином контексте и с иной подписью. Проверить это можно сделав скриншот заглавного кадра видео и проверив его с помощью Google Image Search или TinEye, которые, как вы уже знаете, ищут в базе схожие изображения.

Но есть и более технологичный способ, даже два.

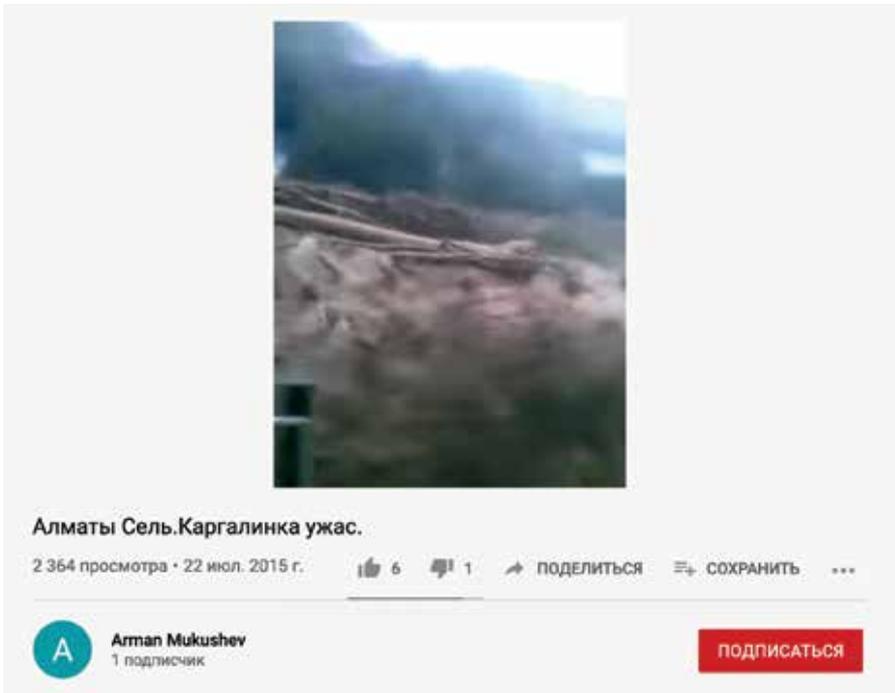
Первый — инструмент, разработанный организацией Amnesty International — Youtube Data Viewer (<https://citizenevidence.amnestyusa.org>). Вам нужно скопировать в него ссылку на ролик и он сгенерирует отдельные кадры (которые посчитает ключевыми) из ролика и найдёт их в Google Image Search. В результатах поиска вы получите список ссылок с аналогичными или схожими видео. Таким образом можно будет сравнить даты заливки видео на сервис.



Казахстанский кейс от Factcheck.kz

Сошедший 23 июля 2015 г. сель в Наурызбайском районе Алматы стал поводом к массовому распространению видео в мессенджерах и социальных сетях. На видео бурные потоки сносили все на своем пути, и у многих видео вызвало панику.

Чтобы проверить это видео, для начала следует найти похожее видео (желательно без логотипа) через поиск Youtube. Так будет проще найти оригинал.



Копируем ссылку на видео и вставляем её на странице сервиса Youtube Data Viewer, который генерирует нам несколько ключевых кадров из видео со ссылками на Google Image Search.

Youtube DataViewer

Алматы Сель.Каргалинка ужас.
Сход селя

Video ID: PW2exBDbo88
Upload Date (YYYY/MM/DD): 2015-07-23
Upload Time (UTC): 05:38:57 (convert to local time)

Thumbnails:



[reverse image search](#)



Все Картинки Карты Ещё Настройки Инструменты

Результатов: примерно 25 270 000 000 (0,70 сек.)



Размер изображения:
120 x 90

Изображения других размеров не найдены.

Запрос, который может быть связан с изображением: **платина алматы чапай**

Сель сошел в Наурызбайском районе Алматы - события ...

<https://tengrinews.kz> > Происшествия > События ▾

23 июл. 2015 г. - Сель сошел в Наурызбайском районе Алматы, передает корреспондент

Перейдите по ссылкам и обратите внимание на миниатюры видео и даты их публикации во второй строке описания.

В потоке ссылок о селе в Казахстане мы видим ссылку на материал о селе в Карачаево-Черкесском районе России, граничащим с Краснодарским краем, который прошел там тремя неделями ранее, а именно 2 июля 2015 г. Проверяем, писали ли о стихии другие издания.



Все Картинки Видео Новости Карты Ещё Настройки Инструменты

На всех языках ▾ 1 мая 2015 г. – 1 авг. 2015 г. ▾ Все результаты ▾ Сбросить настройки

Видео



В Карачаево-Черкесии ликвидируют последствия ...



ВИДЕО: в Карачаево-Черкесии сносит поселок



Непогода стала причиной подтопления в двух районах ...

И выясняем, что селё на видео сошёл в Карачаево-Черкессии в 2015 г. Оригинал видео найден. Вердикт — фейк.

Если вам недостаточно такого поиска, завязанного на поисковик Google, или вам кажется долгим сам путь поиска, попробуйте протестировать второй инструмент под названием InVid — <https://www.invid-project.eu>.

Установив в свой браузер это расширение, вы так же, как в случае с RevEye и фото, в два клика сможете проверить любое видео в любой социальной сети и получить из него ключевые кадры, по которым можно произвести детальный поиск.



Это важно!

Если видео или фото фейковое, вы с большой вероятностью найдёте источник на первой же странице поиска. Однако, если вы не нашли его — не поленитесь заглянуть на вторую или третью страницы. Именно там могут оказаться доказательства подмены и фальсификации.



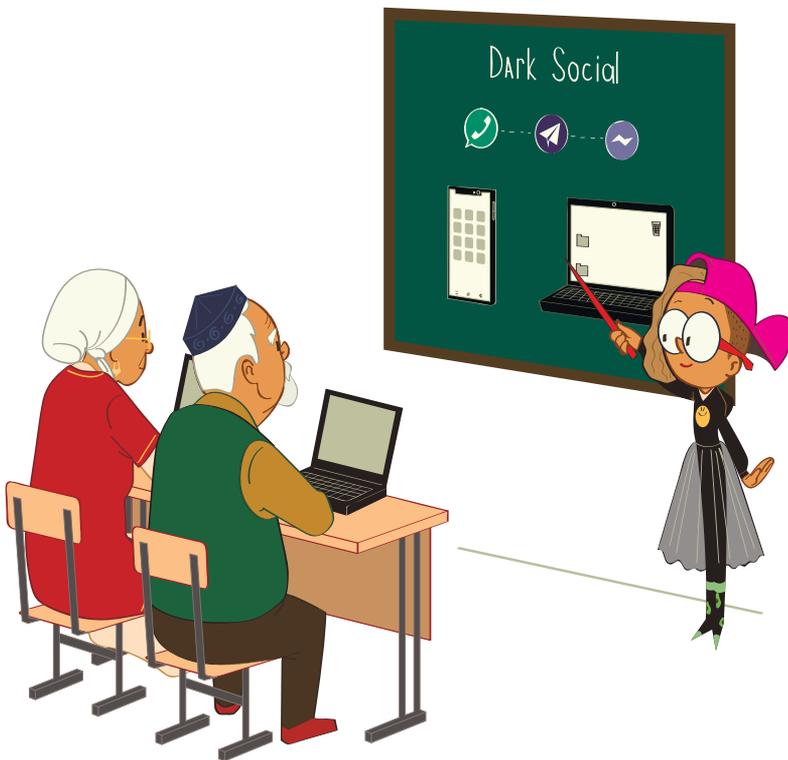
Домашнее задание

1. Изучите инструкцию по использованию сервиса YouTube Data Viewer <https://youtu.be/Q1vonStaf5Q>.
2. Попробуйте с помощью этого инструмента обнаружить оригинал вот этого видео, на котором злоумышленники якобы похищают ребёнка <https://www.youtube.com/watch?v=AEUdiEDsm5I>.
3. Обсудите, насколько этичны действия создателей ролика.



ГЛАВА 10

“ТЕМНЫЕ” СОЦИАЛЬНЫЕ МЕДИА



Несмотря на мрачное название — dark social, или «тёмные медиа» — это не что-то неизвестное, а то, с чем мы все имеем дело каждый день. В первую очередь это наши сообщения в мессенджерах.

Что такое Dark Social

Понятие «тёмных» социальных медиа сравнительно новое, пришедшее в русский язык калькой с английского dark social, хотя первым таким каналом является переписка в обычной электронной почте. «Тёмными» каналами их называют из-за непрозрачности. Всё, что мы делаем на своих страницах в соцсетях, публично или доступно более-менее ограниченному кругу лиц. Переписка же — дело частное, конфиденциальное, и получить к ней доступ могут только хакеры (как от них защититься, мы говорили во время изучения основ кибербезопасности) или правоохранительные органы по решению суда. Для удобства будем называть такие медиа «дарксоциал»

Почему Dark Social так важны

Доля трафика ссылок в дарксоциал в последние три года — от 60 до 90% всего интернет-трафика в мире.



И именно через мессенджеры распространяется огромное количество фейков, дезинформации и опасных манипуляций. В Индии и Мексике известны случаи убийств, произошедших из-за массовых фейковых рассылок о похищении детей.

Пожалуй, дарксошиал — это самый сложный материал для проверки, ведь в данный момент легальных способов проверки источника распространения информации в мессенджерах не существует. Большинство создателей мессенджеров стоят перед дилеммой «анонимность или прозрачность». То есть, предоставлять ли ваши данные третьей стороне (например — спецслужбам) или же следовать мировой тенденции к максимальной защите персональных данных. Этим пользуются как журналисты-расследователи, так и злоумышленники.



Это интересно!

Порой фейковые рассылки появляются благодаря не злоумышленникам или скачающим пользователям, а из-за вполне законопослушных граждан и даже служителей правопорядка.

Так, фейк о «новом опасном наркотике под названием Дарт Вейдер» появился из-за поста от полиции Эксетера (город в английском графстве Девоншир) в twitter. В благих целях полиция сообщила ложные сведения о составе распространяющихся в клубах Англии опасных наркотических веществ (напомним, все наркотики опасны), но в итоге родилась фейковая рассылка, успевшая за год обойти полмира и затронуть в том числе Казахстан (<https://factcheck.kz/glavnoe-en/lozh-novyj-opasnejshij-narkotik-stanovitsya-populyarnym-sredi-shkolnikov-v-almaty>). Вместо того, чтобы противодействовать распространению наркотиков, полиция наоборот привлекла к ним дополнительное внимание из-за того, что посеяла панику среди родителей в Британии, а после ещё в ряде стран по всему миру.



Как проверять рассылки в мессенджерах

Тексты

Здесь вам в первую очередь пригодятся знания, почерпнутые из главы о формальной логике. Рассылки в мессенджерах довольно часто

используют манипуляции, описанные в этой главе. Всякий раз, когда рассылка вызывает у вас гнев или другие яркие эмоции, задумайтесь, не хотят ли вас использовать для дальнейшего распространения недостоверной информации.

При всей кажущейся сложности вам на помощь придёт обычный поиск в Google или Яндексe. Дело в том, что большинство текстовых фейковых рассылок — так называемые «зомби-фейки». Они уже распространялись ранее, возможно, на других языках, но мировое сообщество фактчекеров с вероятностью в 90% уже проверяло их. Скопируйте одно или два предложения и попробуйте проверить их на совпадения в поисковых системах. С большой вероятностью первая же страница поиска подскажет вам источник сообщения и укажет на его (не)достоверность.

Аудио

Если вам прислали аудиосообщение — проведите те же манипуляции: загуглите несколько фраз из сообщения. С большой вероятностью вы обнаружите первоисточник или же материал от фактчекеров, в котором сообщение было подробно разобрано.

Видео

С видео придётся повозиться, но вам помогут инструменты, описанные в предыдущей главе. Есть два основных варианта:

- Вы можете загрузить ролик на YouTube и затем скопировать ссылку на него и проверить через YouTube Data Viewer.
- Можете загрузить ролик на сайте InVid, разбить его на кадры и проверить по ключевым изображениям.



Это важно!

На что стоит обратить внимание в рассылке (алгоритм проверки)

- Насколько грамотно написано сообщение? Часто фейки пишутся «на коленке» со множеством ошибок и не перепроверяются после.
- Во многих мессенджерах сообщение, пересланное вам от третьего пользователя, помечается особым образом. Если вам пришло сомнительное сообщение от близкого человека, посмотрите, он ли его написал на самом деле.
- Никогда не открывайте ссылки на ресурсы, с которыми вы незнакомы. Для проверки можно вбить название ресурса (не саму ссылку!) в Google и посмотреть, что про него знает поисковик.

Также можно пойти по олдскульному пути, сделав скриншот ключевого кадра и проверив его через сервисы поиска картинок. Если этот вариант вам кажется удобнее — используйте его!



ПРАКТИЧЕСКОЕ ЗАДАНИЕ

Попробуйте прямо сейчас проверить достоверность этой рассылки с помощью поиска:

«Facebook может использовать ваши фотографии <...> Это может быть использовано в судебных делах в судебном процессе против вас. Все, что вы когда-либо опубликовали, становится общедоступным с сегодняшнего дня. Даже сообщения, которые были удалены, или фотографии запрещены».

Как видите, действия, которые необходимо предпринять для проверки информации, не сложны и алгоритмичны, особенно, если всякий раз получая сомнительную рассылку, задумываться и приучить себя критически подходить к любому сообщению из непроверенного источника.

Теперь вы готовы к проверке практически любой информации. Но не забывайте: главное ваше оружие — это ваши внимательность и критическое мышление. Никакое цифровое решение не сможет их заменить, только помочь и облегчить поиск первоисточника информации.



Домашнее задание

1. Посчитайте, сколько разных программ для обмена сообщениями установлено на ваших мобильных устройствах или компьютерах (считаются также чаты внутри браузерных версий социальных сетей), и ответьте на вопросы:
 - как часто вы ими пользуетесь;
 - переписываетесь ли вы с одними и теми же людьми в разных мессенджерах?
2. Если у вас три и более мессенджеров, проанализируйте, какую именно информацию и от кого вы получаете через них:
 - достоверную, новостную, проверенную, непроверенную, слухи, розыгрыши?
 - от семьи, друзей, одноклассников, незнакомых людей?

3. Устройте дискуссию на тему: сколько программ для передачи сообщений действительно необходимо для того, чтобы оставаться на связи с близкими и получать достоверную информацию. Может быть, достаточно просто кнопочного телефона? А может, для каждого из круга общения необходим отдельный мессенджер?

Глоссарий

Автоматизированный фактчекинг (англ. automated fact-checking) — специальные алгоритмы, позволяющие автоматически собирать, распознавать, сортировать и выводить необходимую информацию в интернете и медиа, на основании которой делается фактчекинг. Построен на машинном обучении, Python и др. языках программирования.

Алгоритм — ряд математических инструкций или правил, с помощью которых можно решить задачу (Кембриджский словарь).

Архивирование данных — сохранение информации в интернете на специальные сервисы (archive.org, archive.today) для истории, будущих исследований и широкой публики. Сохранять информацию могут как поисковые роботы, так и все желающие.

Бот — компьютерная программа, выполняющая автоматические действия, в частности в интернете. Боты могут быть как полезными, так и вредоносными: к примеру, поисковый бот ищет новые страницы в интернете, чтобы включить их в выдачу поисковика, в то время как другие рассылают вирусы, спам или оставляют комментарии на сайтах (Technopedia).

Верификация — проверка материала на достоверность, сверка любых данных до их публикации или иного распространения.

Видеофейк — умышленно искаженное видео. Как распознать видеофейки и какие они бывают, можно прочитать по ссылке.

Визуализация информации — визуальное представление абстрактных данных или информации, например, в виде инфографики, географических карт, карты концептов. Используется в научных исследованиях, журналистике, анализе финансовых данных и т.д.

Вирусный контент — контент, распространяемый в интернете, большей частью за счёт социальных сетей, резко набирающий популярность.

Вычислительная журналистика (англ. computational journalism) — применение вычислительных методов в журналистике

для сбора, организации и распространения новостной информации. Вычислительная журналистика использует приемы искусственного интеллекта, анализа контента, визуализации, персонализации и рекомендательных систем.

Газетная утка — то же, что и фейк. Точное происхождение фразы не установлено, но ходят легенды, что некий брюссельский журналист Роберт Корнелиссен, живший еще во время Наполеона, написал статью о небывалой прожорливости уток, которые поедали своих сородичей. Другая легенда гласит, что немецкие редакторы помечали непроверенную информацию аббериавитурой NT, что при беглом прочтении читается также, как и «утка» на немецком — Ente.

Геолокация — определение месторасположения пользователя с помощью интернета или мобильного телефона (Кембриджский словарь).

Гиперпартизанский сайт — сайт, чей контент категорично отражает взгляды только одной из политических партий.

Гражданская журналистика — вид журналистики, в котором активное участие при создании, анализе и распространении медиа принимают рядовые граждане, профессионально не работающие в медиасфере.

Групповое подкрепление (англ. communal reinforcement) — ситуация, при которой высказывание становится убеждением вне зависимости от того, является ли оно реальным фактом или нет. Групповое подкрепление происходит внутри социальной группы, члены которой многократно повторяют это убеждение (The Sceptic's Dictionary).

Дата-журналистика — направление в журналистике, в основе которого лежит обработка данных и их использование для создания журналистского материала. Данные могут служить как инструментом для раскрытия определенной журналистской истории, так и ее источником.

Дебанкинг/Развенчание — с англ. debunking — разоблачить слух, неправду, миф.

Дезинформация — специально распространяемая неверная информация. Не путать с misinformation.

«Желтая» журналистика — журналистика низшего сорта, отдающая предпочтение громким и сенсационным новостям без какого-либо фактчека (см. ниже Фактчек). Термин появился в разгар битвы между двумя американскими медиамагнатами Джозефом Пулитцером и Уильямом Рэндольфом Херстом в конце XX века. New York World, принадлежащий Пулитцеру, печатал в то время комикс «The Yellow Kid».

Зомби-фейк — фейковая новость, всплывающая время от времени в интернете и других медиа, даже после выполненного фактчека.

Индекс свободы прессы — ежегодный рейтинг от организации «Репортеры без границ». Учитываются следующие параметры в СМИ: плюрализм мнений, самоцензура, независимость, законодательство и др.

Интернет-троль — интернет-пользователь, цель которого разжечь спор и вовлечь в него как можно большее количество людей (Guardian).

Инфлюэнсер, или лидер мнений — влияет на мнения и поведение людей с помощью социальных сетей (Кембриджский словарь).

Информационная война — борьба нескольких сторон с применением информационных технологий для сбора данных о противнике, а также кибератак, манипуляции, пропаганды и других коммуникационных средств для создания негативного образа соперников.

Информационное загрязнение — загрязнение информационных ресурсов неполной, противоречивой, малоценной или не относящейся к делу информацией.

Информационная перегрузка — ситуация, при которой человек получает настолько много информации, что не может ясно ее воспринять (Кембриджский словарь).

Информационный пузырь (на англ. filter bubble) — явление, присущее в частности социальным сетям, при котором человек не имеет доступа к информации, противоречащей его взглядам и вкусам, получая таким образом однобокую картину мира. Причинами являются персонализированный поиск и веб-алгоритмы, которые основываются на локации пользователя, его предыдущих запросах и в целом поведении в интернете.

Информационный шум — информационная нагрузка, которая возникает в результате перенасыщения информацией, вследствие которой человек теряет способность адекватно воспринимать информацию.

Искусственный интеллект — способность компьютера или робота, управляемого через компьютер, выполнять задания, которые обычно делает или присущи человеку, например, обучение на прошлых ошибках, нахождение причин и умение делать выводы. Компьютеры, оборудованные подобным программным обеспечением, обыгрывают людей в шахматы и го, а также могут писать фейковые новости.

Кликбейт — контент в интернете, главная цель которого — количество просмотров. Для привлечения внимания используют «желтые» заголовки.

Критическое мышление — рациональный, объективный анализ фактов.

Кодекс фактчекеров — разработан IFCN, Международной фактчекерской сетью (см. IFCN). Основные принципы включают в себя беспристрастную подачу информации, прозрачность источников, прозрачность финансирования, методологии и добавление при необходимости объективных корректировок. Организации, вступающие в IFCN, должны соответствовать принципам Кодекса фактчекеров.

Конспирологические теории строятся также и вокруг мультимиллионера и филантропа Джорджа Сороса. О некоторых из них мы писали ранее. Источник изображения: Wikipedia Теория заговора/ Конспирологические теории — объяснение какого-либо факта путем причастности к нему государственной, тайной организации или известных лиц. Часто противоречит всемирно известным фактам. Известный пример — «плоская» Земля.

Кэширование страниц — сохранение страниц любого сайта поисковиками. Таким образом можно просмотреть историю изменений контента. В Google найти кэш сайта можно, нажав на стрелку возле ссылки на страницу сайта в поисковой выдаче.

Македония — известна как главный поставщик сайтов с фейковыми новостями, особенно популярных в период избирательной

президентской кампании в США 2015–2016 гг. Македонские «фермы» фейков действуют по одной схеме: они копируют контент у американских гиперпартизанских сайтов или друг у друга, добавляют или усиливают «желтые» заголовки и раскидывают ссылки на получившиеся статьи по социальным сетям в группы правого толка с помощью личных и фейковых профайлов. Сайты этих «ферм» подключены к Google Ad-Sense или схожим сервисам, поэтому за каждый переход на сайт и показ рекламы владельцы этих сайтов получают деньги.

Манипуляция — способ управления читателем (потребителем контента) путем искажения фактов, создания и продвижения «выгодной» информации.

Машинное обучение — раздел искусственного интеллекта, посвященный созданию алгоритмов, которые обучают самих себя и умеют делать прогнозы. В фактчекинге машинное обучение используют для выявления фейковых новостей (O'Reilly).

Медиаграмотность — умение анализировать и оценивать различные виды и жанры медиа на предмет нахождения пропаганды, манипуляции, цензуры и других видов искажения информации.

Мессенджер — приложение, позволяющее пользователям обмениваться друг с другом сообщениями. Функции мессенджера есть в приложениях Whatsapp, Telegram, Wechat, Snapchat и т.п. В распространении фейковых новостей мессенджеры играют одну из ключевых ролей, поскольку отследить первоисточник в них невозможно.

Мистификация (на англ. — hoax) — намеренно распространяемая ложная информация, не приносящая какого-либо вреда. К ней относятся слухи, городские легенды, псевдонаука, розыгрыши.

Мнение — точка зрения, суждение, не обязательно обоснованное на фактах. Не путать с фактом.

Открытые данные (англ. open data) — данные, к которым каждый может получить доступ, воспользоваться и поделиться ими (Open Definition). Примерами открытых данных могут считаться сайты Комитета статистики РК, Мажилиса и Сената или Открытого Правительства.

Первоисточник — самый первый, то есть оригинальный источник, где появились новость, факт, мнение. Из-за структуры социальных сетей, сайтов и плагиата найти первоисточник зачастую сложно. Но возможно, прибегнув к помощи поисковиков.

Популизм — политика, апеллирующая к широким массам и обещающая им скорое и легкое решение острых социальных проблем (словарь Ожегова-Шведовой).

Постправда — слово 2016 г. по версии Оксфордского словаря. Обозначает явление, при котором общественное мнение формируется личными убеждениями людей и их эмоциями, нежели объективными факторами. PolitiFact присваивает вердикт «Pants On Fire» откровенно лживым утверждениям.

Правдомер — измерительная шкала фактчекинговых вердиктов. Обычно включает в себя «Правду», «Полуправду», «Ложь». Есть и другие дополнительные вариации — factcheck.kz также дает вердикты «Манипуляция» и «Без вердикта»; американский фактчекинговый сайт PolitiFact — «Почти правда», «Почти ложь», «Pants on fire»; мексиканский Animal Politico — «Подлежит обсуждению», «Невозможно проверить», «Вводящий в заблуждение», «Смешно». Washington Post и вовсе раздает вердикты в виде Пиноккио.

Пранк — намеренный розыгрыш.

Предмет фактчекинга — собственно, что проверяют фактчекеры. Этим являются утверждения политиков, чиновников или других публичных лиц, содержащие факты, данные и цифры. Те заявления, что касаются планов, то есть по сути являются обещаниями изменить что-либо в какой-либо сфере, относятся к разряду Promise tracking.

Пропаганда — по словарю Ожегова-Шведовой, распространение в обществе и разъяснение определенных воззрений, идей, знаний, учения, агитация. Однако, следует помнить, что словарь Ожегова создавался в СССР, где пропаганда была одним из инструментов работы партии, а искажение информации или частичная ее подача является одним из инструментов пропаганды. Поэтому мы используем современное определение пропаганды из Оксфордского и Кембриджского словаря: «Пропаганда — информация, идеи, мнения

или изображения, часто дающие только часть аргументации или искажающие её, которые транслируются, публикуются или иным образом распространяются с намерением повлиять на мнение людей».

Псевдонаука — убеждения или методики, которые ошибочно принимают как основанные на научных методах (Оксфордский словарь). Примеры: астрология, феномен «плоской» Земли, фен-шуй, гомеопатия, акупунктура, нейролингвистическое программирование, уфология.

Расследовательская журналистика — согласно Оксфордскому словарю, цель данного вида журналистики состоит в обнародовании информации, представляющей большой интерес для публики, которую, тем не менее, от нее скрывают. Часть инструментов, использующихся в фактчекинге, применяют и в расследовательской журналистике — открытые источники, инструменты для анализа и верификации.

Редакционная политика — описывает многоуровневый комплекс принципов и предписаний (преимущественно формальных), лежащих в основе организации работы редакции. Р.п., к примеру, может ограничивать выражение мнений авторов на их открытых страницах в соцсетях.

Слух, сплетня — сообщение о чьей-либо личной жизни, которое может быть неверным (Кембриджский словарь).

Социальная сеть — сайт или компьютерная программа, позволяющая пользователям делиться или обмениваться информацией с помощью компьютера или мобильного телефона (Кембриджский словарь). Примеры — Facebook, Instagram, Youtube, TikTok, Tinder, Reddit, Twitter, Pinterest. В распространении фейковых новостей социальные сети играют ключевую роль наравне с мессенджерами.

Факт — реальное событие, явление, существование которого можно проверить с помощью открытых источников. В фейковых новостях нередко путают факт с мнением.

Фактоид — опубликованное официальное сообщение, которое становится «истинным» в результате самого факта его обнародования, т.е. недостоверное, ложное сообщение, которое благодаря

определенным обстоятельствам приобретает достоверную форму и обнаружится как достоверное (ист. «Фактчекинг как тренд журналистских расследований: возможности и перспективы», А. Гороховский, 2017).

Фактчекинг (англ. fact-check) — дословно проверка фактов. С помощью методов фактчекинга проверяют заявления публичных персон, резонансные утверждения в социальных сетях и мессенджерах в формате текста, фото и видео.

Фейк — умышленно искаженные новость, факт, данные, информация. Существуют как текстовые фейки, так и видео, фото-, аудиофейки (см. Фотофейк, Видеофейк).

Фейковый аккаунт — аккаунт в социальных сетях, созданный и ведущийся не от имени реального человека. Фейковые аккаунты зачастую воруют контент у других пользователей. Могут использоваться для распространения фейковых новостей.

Фейковые новости (Fake news) — слово 2017 г. по версии словаря Коллинза. Он же предлагает следующее значение — ложная информация, зачастую сенсационная, распространяемая под видом новостной журналистики. Широкая дискуссия о фейковых новостях и их последствиях набрала обороты во время президентских выборов в США в 2016 г.

Фотофейк — умышленно искаженное изображение.

Эхо-камера (англ. echo chamber) — ситуация, при которой повторяются или распространяются одни и те же мнения, поэтому люди не сталкиваются с противоположными им взглядами (Dictionary.com).

Для заметок

Для заметок

МЕДИА И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ

Учебное пособие для 9-11 классов

Издание для апробации

Павел Владимирович Банников

Олександр Гороховський

Таша Соколова

Иван Михайлович Печищев

Дайнюс Радзявичус

Айчурек Усупбаева

Дмитрий Павлович Шишкин

Менеджер проекта	А. О. Кошкина
Координатор проекта	С. Е. Цой
Редактор	П. В. Банников
Корректор	С. Х. Амирова
Дизайнер	А. М. Нәзір
Иллюстратор	М. Ж. Дильманов

Подписано в печать 21.10.2019. Формат 70x100 1/16.
Бумага офсетная. Гарнитура Times. Печать цифровая.
Усл.печ.л. 12,5 Тираж 50 экз. Заказ № 295.10.19

Издано ОФ «Международный центр журналистики «MediaNet»

050040, г. Алматы, ул. Тимирязева, 156, офис 10.

Тел.: 8(727)292-20-46

Email: medianet.smm@gmail.com

Website: www.medianet.kz

Отпечатано в ТОО «Дом печати «Баспагер»

Тел.: +7 727 2222 000

+7 727 2222 202



МЕДИА И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ

9-11 КЛАСС