

УЧЕБНОЕ ПОСОБИЕ

МЕДИА И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ

для учащихся 9–11(12) классов общеобразовательной школы



Медиа и информационная грамотность. Учебное пособие для учащихся 9–11(12) классов. / П. Банников, Т. Соколова, О. Гороховський, И. Печищев, Д. Радзявиčус, А. Усупбаева, Д. Шишкін. – Алматы: ОФ «Международный центр журналистики «MediaNet», 2021.

Данное учебное пособие стало возможным благодаря помощи американского народа, оказанной через Агентство США по международному развитию (USAID) и было подготовлено в рамках «Центральноазиатской программы MediaCAMP», реализуемой Internews при финансовой поддержке USAID. ОФ «Международный центр журналистики «MediaNet» несет ответственность за его содержание, которое не обязательно отражает позицию USAID или Правительства США, или Internews.

USAID является ведущим международным агентством развития и выступает катализатором достижения устойчивого развития. Деятельность USAID направлена на продвижение национальной безопасности США и экономического процветания. Она демонстрирует щедрость американского народа, способствует достижению самообеспеченности и жизнестойкости стран-бенефициаров.

© П. Банников, Т. Соколова, О. Гороховський,
И. Печищев, Д. Радзявиčус, А. Усупбаева, Д. Шишкін, 2021
© ОФ «Международный центр журналистики «MediaNet», 2021



*П. Банников, Т. Соколова, О. Горюховский,
И. Печищев, Д. Радзявицус, А. Усупбаева, Д. Шишкин*

МЕДИА И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ

УЧЕБНОЕ ПОСОБИЕ

для учащихся 9–11(12) классов
общеобразовательной школы

ОФ «Международный центр журналистики «MediaNet»
2021

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ



— Ключевые слова



— Новые термины



— Это интересно!



— Индивидуальная работа



— Парная работа



— Групповая работа



— Задание легкого уровня сложности



— Задание среднего уровня сложности



— Задание повышенной сложности

ист. — Источник

ВВЕДЕНИЕ	7
ГЛАВА 1. История медиа: как мы оказались в XXI веке 8	
Коммуникации человека — от жеста к письменности.....	10
История развития медиа.....	13
Эволюция средств преобразования информации	17
Развитие компьютеров и интернета	20
ГЛАВА 2. Медиаполе и медиаграмотность 22	
Типы медиа	24
Накопление знаний	27
Современные мифы: лжетеории и псевдонаука	30
Медиамир	32
Медиамир и медиаграмотность.....	33
ГЛАВА 3. Фейк и фантазия: чему мы верим и почему 38	
Вымысел в искусстве: кино, театр, тексты	40
Чем отличаются сказки для детей и для взрослых.....	41
Польза детских сказок	43
Фильмы ужасов и кинофантастика	42
Музыка и эмоциональные манипуляции в кино	43
Как с «Прибытия поезда» началась история кино	45
Слово против технологии.....	46
ГЛАВА 4. Информация. Источники информации 48	
Информация и ее признаки.....	50
Искажение признаков информации и его последствия.....	51
Современные источники информации и их признаки	56
Глобальное информационное пространство	57
Механизм искажения информации (принцип каскадности информирования)	59
Факторы влияния на информацию:	
шум, цунами, троллинг и их угрозы.....	63
Информационный шум.....	63
Информационные волны	64
Информационный троллинг	65

ГЛАВА 5. Формальная логика: курс молодого бойца	68
Виды манипуляций и как с ними бороться.....	70
История манипуляций и борьбы с ними	72
Классификация логических уловок (ошибок).....	74
Разновидности petitio principii	75
ГЛАВА 6. Медиа и реклама	82
Реклама и медиа.....	84
Виды визуальных материалов.....	87
Функции рекламы.....	91
Приемы и стереотипы в рекламе	93
ГЛАВА 7. Кибербезопасность	96
Безопасность в социальных сетях	98
Какие проблемы возможны в социальных сетях	98
Как защитить свой аккаунт в соцсетях	100
Уровень второй. Защита с подтверждением	104
Опасности входа в аккаунт на чужом компьютере	107
ГЛАВА 8. Конфиденциальность в социальных сетях	110
Источники проблем	112
Как обезопасить себя от цифровых преступников	115
Что знают правоохранительные органы	122
ГЛАВА 9. Проверка на достоверность фото и видео	128
Инструменты проверки фото и видео на достоверность.....	130
Кто производит фото- и видеофейки	130
Возможности Яндекс.Картинки	132
Проверка оригинальности	136
Казахстанский кейс от Factcheck.kz	136
Информационное оружие будущего	139
ГЛАВА 10. «Темные» социальные медиа	142
Что такое Dark Social.....	144
Как проверять рассылки в мессенджерах	146
ГЛОССАРИЙ	151

ВВЕДЕНИЕ

За последние десять лет мир кардинально изменился. На нас все большее влияние оказывает не сама физическая, ощутимая реальность, в которой мы живем и взаимодействуем друг с другом, а информационный фон вокруг. Факты отходят на второй план, на первый выходят мнения – причем не всегда обоснованные или хоть как-то связанные с реальностью. Партнер по онлайн-игре оказывается гораздо более ценным источником информации, чем сосед по дому.

В этом дивном новом мире мы каждую секунду подвергаемся информационной атаке. Она может просто испортить нам настроение или дезинформировать, а может привести к более печальным последствиям. Например, мы можем стать жертвой преступников или даже попасть под влияние экстремистов.

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

Перед вами первое экспериментальное учебное пособие по медиа и информационной грамотности в Казахстане. Авторы надеются, что оно поможет вам ориентироваться в современном информационном пространстве, отсекать лживую информацию и ее источники, а также повысить свою цифровую безопасность.

Кроме того, программы, описанные в книге, позволят вам сделать свой смартфон или ноутбук инструментом, превосходящим, возможно, весь арсенал современного детектива – если, конечно, не забывать про логические способности и критическое мышление. Они – самое главное. Вместе с вами мы разберемся в том, как устроен мир информации, и как вы сами можете проводить расследования, оберегать свое личное пространство и при необходимости защитить своих близких от информационных атак и обмана.

1

ГЛАВА

ИСТОРИЯ МЕДИА

КАК МЫ ОКАЗАЛИСЬ В XXI ВЕКЕ



КЛЮЧЕВЫЕ СЛОВА:

информация
коммуникация
медиа
медианоситель



Вы узнаете:

- какие способы коммуникации появились первыми,
- какую роль письменность сыграла в формировании государств,
- как развивались медианосители.

Вы научитесь:

- пользоваться разными формами коммуникаций,
- анализировать используемые вами носители информации,
- отличать медиа от массмедиа.

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. У последней – специфический статус, так как в настоящее время крайне сложно найти музыку как форму коммуникации. Она почти целиком превратилась в искусство, выйдя из сферы коммуникаций.



Жест – это самый ранний способ коммуникации, он появился 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». Появившаяся жестовая коммуникация присутствует у некоторых животных, которые охотятся в стае (в частности, у волков). Рисунок 1.1 демонстрирует элемент жестового языка, который сегодня – в сочетании с мимикой, движениями губ и корпуса – используется в культуре глухих и слабослышащих для коммуникации. Жест возник задолго до того, как в ходе эволюции человек научился говорить. Его голосовые связки и легкие были еще недостаточно развиты для коммуникации, но простейшие обозначения руками, понятные соплеменникам, он уже был способен производить.

К доисторическому периоду речевые органы человека развиваются настолько, что позволяют появиться речи. Она является еще одним естественным способом коммуникации. Это значит, что речь – достижение эволюции, природы, а не изобретение самого человека. Речь носит мультимодальный характер, то есть предусматривает сразу несколько уровней. Она, в частности, включает в себя не только содержание, но и интонацию, высоту, скорость. Речь является главным носителем информации.



Сегодня в мире насчитывается более 7 000 языков, однако их число стремительно сокращается. По данным ЮНЕСКО, каждые две недели в мире исчезает приблизительно один язык.

Рисунок 1.1. Элемент жестового языка

Одна из причин исчезновения языков – неравномерность их распространения. 2/3 живущих на Земле людей разговаривает на 40 самых распространенных языках, и лишь на оставшуюся треть приходятся все остальные. Язык считается умершим, когда умирает его последний носитель, поэтому языки без письменности подвержены этому риску сильнее.

Изображение появилось между 50 000 и 30 000 годами до нашей эры. Оно носило универсальный характер – например, символ, обозначающий солнце, одинаково легко могли понять носители любого языка. Изображение возникло тогда, когда родилась потребность в передаче и сохранении информации, не касающейся «здесь и сейчас».



Письменность – это самый молодой способ коммуникации. Первые письменные системы появились около 6 000 лет до нашей эры. Вначале они были достаточно примитивны: конкретный рисунок подразумевал конкретный объект. Каждый такой символ называется пиктограммой, а письменность – пиктографией. Такие письменные свидетельства сохранились 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. Так появляется идеограмма – письменность, кодирующая не материальные объекты, а их акустические элементы. Теперь каждый символ кодирует некое слово или часть слова. Например, символ, обозначающий слог «вол», теперь начинает использоваться в словах и «волынка», и «волна», и «волк».

Последней появляется силлабическая письменность. В ней идеографические знаки кодируют звуки слова один за другим. Она же называется алфавитным письмом. Самое древнее алфавитное письмо – греческое. Кодирование всех звуков слова подряд делает чтение и письмо автоматическим занятием. Платон и Аристотель отмечали крайнюю важность письменности, так как она позволяет сохранить речь и открывает простор для ее толкования или критики.

Письменность древних германцев, существовавшая с I–II по XII век, называлась рунической. Руны вырезались в основном на камне, металле, дереве и кости. Рунами также принято называть алфавиты некоторых других древних народов. Датский ученый Вильгельм Томсен древнюю тюркскую письменность тоже называл руной. Он, в частности, изучал один из самых заметных памятников древнетюркской письменности – каменную стелу Культегина (рисунок 1.2).



Рисунок 1.2. Каменная стела Культегина
(ист. — Betta 27/Public domain)

На берегу реки Или в Алматинской области есть урочище «Тамгалы-Тас» – еще один уникальный памятник искусства, истории и культуры. По словам археологов, здесь около 5 000 наскальных рисунков, которые сопровождаются тибетскими надписями. В 1875 году Чокан Валиханов сделал зарисовку местности.

После появления письменности новые способы коммуникации перестают появляться. Инновация отныне проявляется лишь в изменении способов доставки информации при помощи разнообразных носителей.



Задание 1.1

Покажите на ленте времени историю появления различных способов коммуникации. Поясните свой рисунок.



Задание 1.2

Не используя письмо, попробуйте в парах передать друг другу простые сообщения: «это мой дом», «на охоте я добыл оленя» или «приближаются враги». Придумайте ситуацию, в которой наиболее эффективной будет коммуникация с помощью музыки.

История развития медиа

Как уже говорилось выше, любой из способов коммуникации имеет целью передачу какой-либо информации. Вначале информация носила исключительно утилитарный и сиюминутный характер. Первобытный человек делился такой информацией: «этот фрукт вкусный и неядовитый», «этот зверь опасен, беги и прячься». В его языке было 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 происходящее в данный момент, но и события прошлого или будущего, а также гипотетические.

Стоит отметить, что вне зависимости от способа коммуникация 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, коммуникация между ними не состоится. Так же произойдет и в ситуации, если жесты в их культурах несут разную смысловую нагрузку (например, болгары для отрицания кивают головой, а для согласия – покачивают из стороны в сторону). Частично успешной будет коммуникация между носителями разных языков, если они смогут объясняться с помощью, например, английского языка.

Коммуникация играла важнейшую роль в формировании человеческого общества. Первобытные племена охотников и собирателей постепенно превращались в более крупные образования («вождества» или государства) с целью лучше координировать свои усилия. Экономические системы развивались параллельно с развитием специализации и необходимостью вести торговые отношения.

Способность общности укрупняться и развиваться зависела в первую очередь от умения ее членов соотносить себя с группой. Это было невозможным без наличия письменной культуры. При этом важную роль в развитии государств играли и формы коммуникации. Так Месопотамия представляла собой более локальное государство из-за того, что носители информации были крайне несовершенны и плохо транспортабельны. 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 уступал государствам, перешедшим на силлабическое письмо. Они достигли большего расцвета. Этую гипотезу – об «общественной зависимости от коммуникативной эффек-

тивности» – развивали канадский культуролог Маршалл Маклюэн и канадский экономист Гарольд Иннис.

Именно эти ученые ввели понятие «медиа». Маклюэн говорил: «Media is the message». Афоризм 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 из счетной книги, куда древнеегипетский торговец написал, что «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 для всех жителей страны, – массмедиа. Если перевести на современный лад, то сообщение, отправленное другу, относится к медиа, а сообщение, отправленное в школьный чат, – уже массмедиа. Однако с распространением интернета эти понятия стали синонимами.

Самым древним письменным документом являются Тэртерийские надписи – глиняные таблички, найденные на территории современной Румынии и датируемые в районе 5500 года до нашей эры. Их содержание предположительно носит хозяйствственный характер, следовательно они подпадают под категорию «медиа». Во всех только обретающих письменность культурах сначала под запись отправляются данные для хозяйствственно-экономических целей, и лишь потом – школьные, медицинские и юридические тексты.

Первым наиболее крупным и известным памятником массмедиа являются уже упомянутые таблички Хаммурапи, так как они были адресованы 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 пр. 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.

С возникновением рабовладельческих государств у правителей появляется необходимость получать свежую информацию о положении дел на подконтрольной им территории – так зарождается почтовая связь. Сначала почтовые сообщения носили преимущественно экономический и военный характер. Затем почтовые голуби и конные всадники заменили рабов-курьеров, которых богатые граждане Древнего Египта использовали для обмена сообщениями между собой.

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

Позднее в Древнем Риме появился прообраз газеты. Интересно, что и регулярные газеты, и единная почтовая система возникли в период правления одного человека – Гая Юлия Цезаря. Он обязал распространять отчеты о заседаниях сената, донесения полководцев и послания правителей соседних государств. Он же распорядился о создании единой государственной почтовой системы, которая позволила связать самые отдаленные уголки Римской Империи.

На просторах Великой степи также постоянно происходил обмен сообщениями. Людей, непосредственно участвовавших в передаче информации, называли «жаршы» (в переводе на русский – глашатай; сообщал самые важные официальные новости) или «хабаршы» (в переводе на русский – вестовой, гонец). Отдельное место в этой системе занимало сарафанное радио – үзынқұлақ, когда люди узнавали последние известия друг от друга. Габит Мусрепов в повести «В двадцать четыре часа» отмечал, что именно этот способ передачи информации зачастую работал безотказно – в условиях, когда телеграммы и поезда задерживаются, писал он, «новости из Москвы, Парижа, Лондона путешествуют по степи на лошадях и верблюдах».

Первая печатная газета появилась в Древнем Китае в VIII веке. «Столичный вестник» 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. В Европе в эти годы продолжали пользоваться исключительно рукописными массмедиа. Так продолжалось еще несколько столетий.

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 покрытых воском табличках. После правок и корректировок автора секретарь переносил утвержденный текст на бумагу. Копирование чаще всего также проводилось под диктовку. Только с развитием монастырской письменной культуры появились индивидуальные копировальщики текстов.

Первоначальной формой таких записей являлся свиток. Это крайне сложная форма организации текста, потому что написанное приходилось удерживать сразу с двух сторон. Это значительно осложняло работу сразу с несколькими свитками. Также существенным минусом свитка являлась невозможность сразу перейти к требуемому разделу текста.

На смену свитку пришел 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 переходить 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 достигла соответственно 100% и 96%.

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



Задание 1.3

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 другое? Обсудите свои ассоциации с одноклассниками.

Эволюция средств преобразования информации

До появления печатного станка газеты распространялись в форме индивидуальных оттисков. Все изменилось в 1450-х годах после того, как Иоганн Гуттенберг изобрел печатный пресс. Это позволило полностью отказаться от услуг переписчиков, стандартизировать форму и удешевить процесс.

Парадокс Гуттенберга: изобретение печатного станка инициировало новую информационную революцию и положило начало новой эре, однако с массовой коммуникацией, массовым книгопечатанием и массовым словом в жизнь общества пришел и массовый обман.

В XVI веке в речи появляется слово «газета». Оно произошло от названия мелкой венецианской монеты «газетты» – столько стоил листок с последними новостями. Можно сказать, что именно в Венеции появились 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.

Первой казахской газетой стала «Түркістан уәлаятының газеті». Она издавалась в Ташкенте с 1870 года, а с 1888 года выходила в Омске под названием «Дала уәлаятының газеті». Первый казахский журнал назывался «Айқап» и издавался в 1911–1915-е годы.

Параллельно с распространением газет набирало обороты и книгопечатание. Для бедных слоев населения, не умеющих читать, выпускали особый вид книг, где вся история рассказывалась с помощью картинок. Такая книга представляла собой по сути первый комикс.

Затем человек задался целью передавать информацию на расстояния. Вначале использовался метод семафора – приемопередаточные посты располагались на достаточном для прямой видимости расстоянии. Таким образом каждый пост передавал сигнал следующему. Француз Клод Шапп усовершенствовал этот метод, 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 поняли и торговцы – с помощью телеграфа они стали передавать котировки валют и сигналы о приходе в порт кораблей с товаром. Интересно, что слово «сеть» появилось именно в применении к линиям телеграфа, устроенным по принципу узлов связи.

Изобретение телеграфа радикальным образом изменило скорость коммуникации, а, значит, и скорость жизни. И во времена Юлия Цезаря, и на пороге XIX века письмо из Парижа в Марсель, если его не вез отдельный гонец, шло в среднем 15–20 дней. С изобретением же телеграфа новость стала доходить 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 алфавите. Однако это было крайне неудобно для передачи сообщений на разных 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 после изобретения телефона. 14 февраля 1876 года Грэм Белл (рисунок 1.3) получил патент на телефонный аппарат. 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 больше использовался для личных переговоров. Из исследования телефонных разговоров в 1909 году: 20% звонков – коммерческие заказы, еще 20% – звонки из дома на работу с распоряжениями, 15% – приглашения и 30% – просто «болтовня». С течением времени телефон все сильнее начинает выполнять функцию социализации.



Рисунок 1.3. Грэм Белл и изобретенный им телефон (ист. - Библиотека Конгресса США)

В 1920-х годах даже появляется такое понятие, как «телефонный визит», когда разговор по телефону заменил необходимость лично посещать родственников.

До XIX века человечество могло сохранять только письменную информацию. С изобретением фотографии и фонографов стало возможным хранить и визуальную, и аудиальную информацию. 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 «бессмысленным» использованием своих детищ.

Кино появилось во Франции в 1895 году у изобретателей братьев Люмьер. В отличие от Томаса Эдисона, параллельно работающего над 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 арендовывали помещения и показывали там выкупленные или снятые их же компаниями фильмы. Так появились киногиганты Парамаунт, Уорнер Бразерс, Метро Голливуд Майер (MGM), XXВек и RKO. Юниверсал, Коламбия и Юнайтед Артистс своих залов не имели, поэтому развивались намного медленнее.

В наши дни мы можем пойти в любой кинотеатр и посмотреть там фильмы, снятые всеми компаниями, а в начале XX века за просмотром каждого фильма требовалось идти в кинозал той компании, которая его сняла.

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

Что касается радио, выделить одного человека, который его изобрел, не представляется возможным. В странах бывшего СССР господствует теория, что радио изобрел Александр Попов. Европа, Америка и весь остальной мир считают первым в этом Гульельмо Маркони. И тот, и другой вариант являются упрощением, потому что и Томас Эдисон, и Никола Тесла, и даже Бенджамин Франклин совершили ряд открытий, создавших возможность передачи радиоволн. Интересно, что радиосвязь (а не телеграф в свое время) начали называть «беспроводной связью».

Как и в случае с радио, у телевизора нет одного установленного изобретателя. Над его созданием параллельно трудились ученые из разных стран. Владимир Зворыкин, эмигрировавший в Америку, смог собрать разные технологии и добиться наилучшей четкости изображения. И в США, и в СССР стали создаваться системы вещания, но первый регулярный телеканал появился в 1934 году в Германии. Берлинская Олимпиада 1936 года стала первым событием, с которого велась прямая трансляция. В 1950 году телевидение стало цветным, а в 1990-х годах появились технологии цифрового вещания.

Развитие компьютеров и интернета

Первая ЭВМ (электронно-вычислительная машина) появилась в 1945 году, хотя разработки велись еще с 30-х годов. Она называлась ЭНИАК и весила целых 30 тонн. Только в 70-е годы появились «микро»-ЭВМ размером всего-то с платяной шкаф. В 1976 году на рынке появился 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 году на рынок поступила другая 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 году появился первый планшет весом 680 грамм.

Разработка глобальной сети обмена данными началась в 1950-е годы. Прототип сети появился в 1969 году. Как и многие другие изобретения, вначале он был поставлен на военную и государственную службу. Благодаря исследователю Тому Бернерсу-Ли в 1984 году появилась открытая для всех желающих сеть. Она сделала возможными электронную почту, мгновенный обмен сообщениями, телефонную связь по интернет-протоколу, видеосвязь, а также Всемирную паутину с ее форумами, блогами, социальными сетями и интернет-магазинами.

В развитии Всемирной паутины выделяют пока три основных периода:

- В период Web 1.0 (90-е и начало 2000-х годов) 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. Основным местом общения были специальные разделенные

по темам форумы и чаты. В те годы скорость работы сети была значительно ниже сегодняшней. Порой интернет-трафик проходил по линиям телефонной связи, и было невозможно одновременно находиться в интернете и говорить с кем-то по телефону.

- С появлением высокоскоростного интернета наступила эпоха Web 2.0. Пользователи стали активно делиться картинками, музыкой, видео. Скачивание файла стало происходить быстро – без перегрузки линии. Сайты наполнялись во многом пользовательским контентом, появилась возможность комментирования, зарождаются и развиваются социальные сети и мессенджеры. В эпоху Web 2.0 количество информации в сети резко возросло, стало возможным найти все и обо всех. Вместе с тем стал очевидным новый вызов – в такой сети почти невозможно сохранить анонимность.
- Когда смартфоны с высокоскоростным интернетом стали доступными почти каждому пользователю и обеспечили его круглосуточное присутствие в сети, началась эпоха Web 3.0. Она характеризуется тем, что социальные сети почти полностью поглотили весь остальной интернет. В них теперь можно не только общаться, но и учиться, работать, смотреть фильмы, слушать музыку, заниматься творчеством и его продвижением. 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.

Итоги



«Кодекс Хаммурапи» в переводе Якобсона В.А. (Хрестоматия по истории Древнего Востока. Часть 1. – Москва: 1980. – С.152–177) и в частичной обработке Немировского А.А. содержит 61 645 знаков. Вес носителя составляет 4 тонны.

- а) Посчитайте, сколько бы весила ваша любимая книга.
- б) Узнайте у школьного библиотекаря, сколько приблизительно книг в библиотеке. Посчитайте, сколько бы весила такая библиотека, если средний вес каждой книги равнялся бы весу вашей любимой книги.



* Интернет больше не является инновацией, он уже наша повседневность. А какую инновацию вы хотели бы получить в ближайшие 10 лет в области коммуникации и информации? А в других областях? Составьте ваш прогноз технологического развития до 2030 года.

2

ГЛАВА

МЕДИАПОЛЕ И МЕДИАГРАМОТНОСТЬ



КЛЮЧЕВЫЕ СЛОВА:

мультимедиа

наука

миф

медиаграмотность



Вы узнаете:

- по какой закономерности развиваются технологии в современном мире,
- как человечество накапливало знания,
- что лежит в основе медиаграмотности, и в чем ее необходимость.

Вы научитесь:

- распознавать современные мифы и лжетеории,
- отличать медиасферу от медиаполя,
- определять фейки, сплетни и пранки в медиапространстве.

Типы медиа

В современном мире понятия «медиа» и «массмедиа» почти не имеют различий. Более того, появилось новое слово «мультимедиа». Это технология, когда контент передается с помощью сразу нескольких средств – компьютерная графика, музыка, звук, брендированные товары, книги и пр. (рисунок 2.1).



Рисунок 2.1. Каналы мультимедиа

В развитии технологий существует такая закономерность – сначала 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 развиваются инновацию и наполняют ее множеством функций), затем она закрепляется в повседневности (все, кто хочет получить доступ к технологии, имеют такую возможность). Как только технология закрепляется, она перестает значительно меняться и прогрессировать, освобождая научное и творческое пространство для будущих инноваций.

Рассмотрим этот цикл 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, когда в коммуникационном пространстве освободилось место инновации, 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. В начале для взаимодействия «человек – компьютер» использовалась письменность – с помощью клавиатуры пользователь вводил определенные текстовые команды. Следом появился графический интерфейс – теперь большинство операций с компьютером осуществляется 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 Siri или Алису найти что-то в интернете, засечь 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 (рисунок 2.2).

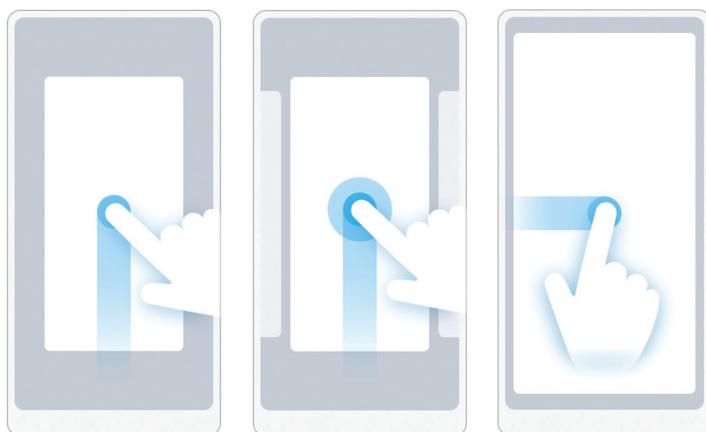


Рисунок 2.2. Управление смартфоном с помощью жестов



Задание 2.1

Подумайте, какие жесты популярны в вашем общении, какую информацию они передают. Проиллюстрируйте их.



Задание 2.2

Прочтите список ниже. Как вы думаете, существуют ли уже такие технологии, или это пока возможно только в фантастических фильмах? Подтвердите свои предположения конкретными фактами.

- 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) принтер со специальными «ароматическими» картриджами позволяет пользователю на расстоянии понюхать любой предмет из каталога;
- 5) человеку можно пересадить целиком руку, ногу или голову, и пересаженная часть тела будет полностью функциональна;
- 6) появились программы голографической связи, целиком проецирующие 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 планеты 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), 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, способный 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.

Составьте презентацию с указанием гиперссылок на информацию, подтверждающую ваши ответы. По своему усмотрению вы можете создать видеоклип продолжительностью от 2 до 5 минут.

Накопление знаний

Как мы уже отметили, коммуникативные технологии развиваются по спирали: появляется что-то новое, активно совершенствуется, становится частью повседневности, освобождая место для очередной новинки. 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 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 очевидны. Открытия египетских, греческих и римских ученых позволили убедиться, что засуху можно победить человеческими силами 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 были разрушены и забыты. 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 объяснялась исключительно волей Божьей. Страшные эпидемии чумы и холеры опять же объяснялись гневом единого Бога. Земля уже стоит не на черепахе, но абсолютно плоская и сотворенная 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 позволившими 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, которая якобы находит закономерности между формой черепа и социальным поведением. Физиognомика предлагает по чертам лица полностью определять характер и наклонности человека. Графология ищет 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 привлечь 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 период (начало – середина XIX века) длился около 50–70 лет, поэтому есть надежда, что мы сумеем пройти эпоху мифов за 15–20 лет.

Помимо выделенной закономерности про накопление знаний и технологий человечеством в Таблице 2.1 приведем наблюдение в отношении места человека в каждой из обозначенных эпох.

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

Таблица 2.1. Возможности человека в ходе накопления человечеством знаний



Это интересно!

1 апреля 2017 года сайт azh.kz распространил информацию о том, что 20-летний житель Атырау Акылбек Копжасаров решил математическую задачу, которую ученые всего мира не могли решить много лет. Информационные порталы мгновенно переопубликовали сенсационную «новость». И несмотря на то, что сайт-первоисточник сразу же указал, что это первоапрельская шутка, сообщения о гениальном соотечественнике до сих пор размещены на некоторых казахстанских интернет-ресурсах. Чтобы убедиться в этом, достаточно вбить в поиск «Акылбек Копжасаров».

Современные мифы: лжетеории и псевдонаука

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.
- Гомеопатия – лжетеория, согласно которой «подобное излечивается по-подобным». В организм пациента вводят сильно разведенные препараты, которые якобы и у здорового пациента вызывают такое же заболевание.
- ВИЧ-диссидентство – лжетеория о том, что вирус иммунодефицита человека – выдумка, а СПИД вызывается неинфекционными факторами.
- Астрология – лжетеория, по которой положение небесных тел в момент рождения ребенка и в другие значимые моменты его жизни может влиять 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 вызывать аутизм и другие нежелательные особенности развития.
- Абсолютная вредность ГМО – лжетеория, утверждающая, что все продукты с генной модификацией несут опасность и вред для человеческого организма.



Задание 2.3

Найдите в казахстанских СМИ материалы или рекламные объявления об оказании услуг, доказывающих, что лженавуки живы и подобная информация востребована среди потребителей.



Задание 2.4

Рассмотрите скриншоты публикаций, одна из которых пропагандирует отказ от профилактического прививания детей (рисунок 2.3), а другая приводит слова министра здравоохранения Республики Казахстан,

отстаивающего противоположную точку зрения (рисунок 2.4). Выразите свое мнение по этому вопросу. Обсудите, какие мифы вокруг вакцинации распространены в вашем окружении (если необходимо, проведите мини-опрос).

АДРЕСАТ: ПРЕЗИДЕНТУ РК КАСЫМУ-ЖОМАРТУ ТОКАЕВУ СПИКЕРУ СЕНАТА ДАРИГЕ НАЗАРБАЕВОЙ СПИКЕРУ МАЖИЛИСА НУРЛАНУ НИГМАТУЛИНУ

ГРАЖДАНЕ КАЗАХСТАНА ПРОТИВ ОБЯЗАТЕЛЬНОЙ ВАКЦИНАЦИИ



Рисунок 2.3. Скриншот (ист. — Citizen.org)

За 10 лет в Казахстане не зарегистрировано ни одного летального случая от вакцины – Биртанов

Глава Минздрава призвал отделить эмоции от фактов

ТАМАРА ВАДЛЬ 08.05.2020, 18:41 9106



ФОТО ЖАНАРЫ КАРИМОВОЙ

Рисунок 2.4. Скриншот (ист. — Vlast.kz)

Медиамир

Современный человек живет полностью в медиамире. От влияния источников информации почти невозможно укрыться. Медиа – это не только чтение новостей или просматривание ленты социальных сетей. 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 все равно может откладываться у него в 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 медиасфера каждого школьника Алматы очень похожа между собой, но будут отличаться от медиасфер каждого городского школьного учителя. Вместе они (медиасфера школьников и учителей) имеют много общего, но сильно отличаются от медиасфер школьников и учителей США. В каждой медиасфере есть составляющая, которую мы сознательно не замечаем, и другая, которой мы активно пользуемся и за которой активно следим. Вторую называют медиаполем. А вот медиаполе у каждого ученика может быть свое, абсолютно не похожее на медиаполе сверстников. Например, ученик, интересующийся дизайном, будет отмечать для себя важным все, что его интересует, а ученик, увлекающийся музыкой, полностью проигнорирует медиаполе первого, зато составит свое, с отдельным вниманием к звукам.



Задание 2.5

Составьте свою персональную карту медиа. Зафиксируйте письменно все казахстанские 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 и медиаграмотность

Информацию принято делить на фиксированные категории (таблица 2.2).

	Журналистика	Энтертеймент	Промоушн	Пропаганда	Сырая информация
Цель	Информировать	Развлекать или вовлекать людей во время досуга в деятельность, в которой они пассивные участники	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
Методы	Верификация, независимость, ответственность	Стори-теллинг, перформанс, визуальное искусство и музыка	Оплаченнная реклама, PR, пресс-релизы, публичные заявления, постановочные события, спонсорство, продукт 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
Участники	Репортеры, фотографы, видеооператоры, редакторы, продюсеры	Писатели, актеры, художники, музыканты, дизайнеры	Рекламные агентства, публицисты, эксперты PR, официальные публичные лица	Политики и организации	Любой человек с доступом к интернету, фотооборудованию или иным любительским способом распространения информации
Результат	Усиление гражданской информированности	Отвлечение граждан от повседневной жизни. Изменение или критика социальных норм	Рост продаж продуктов или услуг, зарабатывание денег теми талантами, которые промоутируются	Помощь идеологическим группам в захвате и удержании власти и через влияние на публичное мнение и мотивацию действовать в удобном ключе	Самовыражение или любительское производство энтертейнмента, промоушена, защиты общественных интересов или пропаганды

Таблица 2.2. Журналистика и ее «соседи»

Подчеркнем, что из приведенной таблицы совсем не следует, что только журналистика – это хорошая и правильная информация. Полезной может быть информация в любой из категорий. Главное – отдавать себе отчет, с каким типом информации мы имеем дело, и чего на самом деле хочет от нас автор материала.



Задание 2.6

В таблице с такими же колонками и строками на место изложенных теоретических аспектов вставьте скриншоты из казахстанских СМИ, иллюстрирующие их.

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 десятков фейков.



Фейк – это ложная новостная история или визуальный материал, затрагивающий общественно важные темы, созданный для масового распространения онлайн с целью увеличения трафика или дискредитации общественного движения, публичной персоны, политической кампании и т.д.

Журналистская утка обладает всеми признаками фейка с тем лишь уточнением, что создается журналистом и изначально распространяется в СМИ, поэтому выделять ее в отдельную категорию нет необходимости.

Помимо фейка есть еще две сходные категории.



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



Пранк – намеренная шутка или розыгрыш.

Для начала отметим 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 2.3.

Параметр	Фейк	Сплетня	Пранк
Намерение	Есть	Может отсутствовать	Есть
Задача	Массовая дез-информация	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 не ограничена	Отдельный человек или группа лиц. При публикации пранка в медиа аудитория не ограничена

Таблица 2.3. Различия между фейками, сплетнями и пранками

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

Важно отметить, что авторы фейка и сплетни всегда до последнего стремятся, чтобы их информация 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.

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 2.4 представлены основные различия между фактчеком и верификацией.

Параметр	Фактчек	Верификация
Для кого польза?	Всем окружающим	Самому человеку
Предмет	Информация, массово распространенная 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

Таблица 2.4. Сравнение фактчека и верификации

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

Итоги



Узнайте у своих родных и друзей, в какие из современных мифов они верят. Выслушайте их доводы и попробуйте поменять позицию, начав разрушать мифы. Постарайтесь оппонировать в случае, если они начнут приводить аргументы в защиту своей позиции. Обсудите в классе впечатления от беседы. Если кто-то из родных и друзей твердо убежден в какой-либо лжетеории, дайте им почитать этот учебник.



Объединитесь в группы по три-четыре человека. Подберите в новостных лентах по три-четыре материала, подходящих под категории фейка, сплетни и розыгрыша. Обязательно наличие всех трех категорий. Представьте заголовки материалов вашим одноклассникам. Пусть они попробуют распознать, что именно кроется под броским заголовком: фейк, сплетня или розыгрыш.

С помощью знаний по основам права или экспертов установите уголовную или административную ответственность за распространение ложной информации.

3

ГЛАВА

ФЕЙК И ФАНТАЗИЯ

ЧЕМУ МЫ
ВЕРИМ И ПОЧЕМУ



КЛЮЧЕВЫЕ СЛОВА:

культура
искусство
персонаж
сказка
эмоция



Вы узнаете:

- чем сказки полезны для детей и взрослых,
- как можно манипулировать эмоциями при помощи музыки или ее отсутствия,
- зачем в историях встречаются хорошие и плохие персонажи.

Вы научитесь:

- замечать манипуляции в произведениях искусства,
- видеть художественные приемы в окружающей реальности,
- распознавать архетипы в медиа.

Вымысел в искусстве: кино, театр, литература

Кино, театр и книги представляют собой обширную галерею персонажей – хороших и плохих, героев и злодеев. Они созданы писателями, режиссерами, сценаристами – людьми, которые обычно остаются за кадром в то время, как зрители очаровываются вымышленными героями.

Когда мы идем на популярное театральное представление или в кино, выбираем роман или детектив, мы обычно заранее знаем, что эти истории – ненастоящие. Мы понимаем, что это плод чьей-то фантазии. Однако любопытный парадокс заключается в том, что чем более правдоподобна эта фантазия, тем больше мы отдаляемся вполне реальным эмоциям и влиянию творцов.

Посмотрев интересный фильм или прочитав роман талантливого писателя, мы непроизвольно формируем мнение о героях и антигероях. При этом достаточно лишь задать себе несколько вопросов, обратить внимание на важные детали, чтобы понять: иногда мы излишне героизируем одних, превращая других во врагов и «плохих парней». Это происходит потому, что нам страшно даже представить, что зло может победить. Вероятно, поэтому «плохие парни» в кино в конце зачастую проигрывают.



Задание 3.1

Вспомните известных киногероев, которых вы знаете, и обсудите, какие эмоции вызывают у вас эти персонажи, ответив на вопросы.

1. Почему определенный 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 так утрированно: некоторые герои злые, ревнивые, предатели, лжецы и даже физически безобразные (особенно в фантастических фильмах, таких как «Властелин колец»), в то время как другие – чувствительные, самоотверженные, спешат помочь, искренние и ангельски красивые (например, эльфы, ангелы и т. д.)?



Задание 3.2

Вы много раз в кино и в анимационных фильмах видели саков, скифов и гуннов. Опишите, как они выглядят, каковы их характеристики, во что они одеты. Как вы думаете, насколько образы в искусстве соответствуют реальности? Узнайте, как на самом деле выглядели доспехи саков, скифов или гуннов.

Чем отличаются сказки для детей и для взрослых

Давайте попытаемся разобраться в том, что именно заставляет нас верить образам в искусстве, забывая о прочих важных вещах. И начнём с прародительницы любого искусства – сказки.

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

Одним из самых известных исследователей и аналитиков сказок был психоаналитик, доктор Бруно Беттельгейм. Он написал широко известную книгу под названием «Польза от волшебства» (рисунок 3.1). В этой книге ученый анализирует сказки и механизмы их влияния на людей. Он объясняет, почему они так важны для нашей несовершенной цивилизации.

Что такое сказка в традиционном понимании? Это история с более или менее строгой моралью в конце. В ней существуют магические силы, заклинания и необыкновенные существа – феи, волшебники, великаны, драконы и единороги. На протяжении



Рисунок 3.1. Книга «Польза от волшебства»
Бруно Беттельгельма (ист. – Flip.kz)

веков сказки выполняли одну главную задачу – оказывать влияние на моральное воспитание подрастающего поколения.

Сказки для детей помогали им запомнить основные правила, принятые в определенной культуре. Они по сути представляли собой своеобразные путеводители, своды универсальных культурных правил.



Задание 3.3

В жанре социальной рекламы разработайте плакат, в котором согласно сюжета казахской народной сказки главный герой призывает детей следовать нормам морали.

Польза детских сказок

Бруно Беттельгейм считает, что родители часто совершают ошибку, защищая своих детей от суровой реальности. Ведь в действительности 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 умны, но бессердечны, а третий – глупый, но хороший. Такая поляризация и счастливый конец сказки помогают ребенку отождествиться с сочувствующим, хорошим героем.



Это интересно!

Различные испытания героев в сказках отражают обычай общества: например, такое крупное событие в мировых культурах как переход или посвящение мальчиков и девочек во взрослую жизнь. Чтобы стать мужчиной или женщиной в традиционных культурах нужно преодолеть некое препятствие – это и есть посвящение.

Однако есть и другой тип сказок, где героя – даже если он обманывает злодея или ворует что-то у злого великана – не осуждают. 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, сказки формируют интеллект, очищают эмоции, помогают понять проблемы, с которыми человек сталкивается, и показывают, как их можно решить.

Фильмы ужасов и кинофантастика

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, обычно мы имеем в виду его прекрасную сторону. Мы счастливы, когда герой, преодолев препятствия, получают награду в виде руки принцессы и половины королевства. Начинается праздник, после которого все непременно живут долго и счастливо. Но до счастливого конца еще предстоит пройти долгий путь: бороться за жизнь, обманывать демонов или гигантов и решиться на другие не менее опасные поступки. И если так рассудить, по большей части эти сказочные истории – не более чем фильм ужасов.

Режиссер Дэвид Кроненберг считает, что 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 объединяют не только схожие сюжетные линии – и те, и другие помогают зрителям всех возрастов преодолевать глубинные фобии. Фактически это одна из форм психотерапии, которая утверждает нас в мысли, что нам повезло больше, чем персонажам этих историй. Выходит, фильмы ужасов или фэнтези для взрослых – это и выход из реальности, и средство исцеления страхов.



Задание 3.4

В сказках для детей и для взрослых часто встречаются одни и те же сюжеты, которые называются архетипами. Например, «из грязи в князи», когда социальное положение главного героя резко улучшается. По такому сценарию построены, например, истории о Гадком утенке или Золушке.

Изучив соответствующие источники, определите наиболее распространенные в искусстве архетипы и приведите примеры по ним из известных книг, фильмов и сериалов (в том числе, казахстанских). Насколько эффективно их использование в манипулятивных целях?

Музыка и эмоциональные манипуляции в кино

Использование музыки в фильмах – это секретное оружие, которое продюсеры применяют, чтобы манипулировать нашими эмоциями и формировать нужную реакцию на историю. Одни и те же кадры благодаря разному музыкальному сопровождению могут показаться романтическими, грустными или даже зловещими. Музыка способна формировать и более тонкие градации эмоций.

Вы, должно быть, сами нередко замечали, как музыка в течение всего нескольких секунд может изменить то, что мы чувствуем. В реальном мире мы не окружены музыкой, при наблюдении за людьми или окружающей средой мы не испытываем столь ярких эмоций, какие нам могла бы подарить музыка. Мы можем эмоционально реагировать на окружающие звуки (например, на пение птиц), однако нужно понимать, что наши чувства при этом никак не связаны с реальным назначением этих звуков или значением для издающих звук существ. К тому же музыкальные звуки имеют гораздо более яркую структуру, чем естественные: для них характерны не только мелодия и ритм, но также качество звука (темпер), гармония и тональность (мажорная или минорная).

Несмотря на некоторые исключения, музыка в мажорной тональности и в быстром темпе, вероятнее всего, вызовет счастливые, положительные эмоции. Меланхоличные, миролюбивые или романтические пьесы, как правило, либо медленные, либо в минорных тональностях. Музыка, предназначенная для испуга, часто нерегулярна с точки зрения ритма и склонна ощутимо менять динамику.

Различные составляющие музыки обрабатываются в разных частях мозга. Там, где есть ритм, мы чувствуем желание постучать, кивнуть или даже танцевать. Однако большая загадка все еще заключается в том, как музыка влияет на ментальные и физические измерения наших эмоций. Психические реакции человека могут быть связаны с такими физическими реакциями, как увеличение частоты сердечных сокращений, изменение кровотока и ощущение покалывания на коже. Почему именно музыка столь эффективно вызывает реакцию нашего тела и психики, неизвестно: в конце концов, некоторые из ее особенностей (например, гармония) являются недавними человеческими изобретениями и не могли сыграть никакой роли в процессе эволюции нашего мозга.

Еще одной интересной особенностью фильмов, как это ни парадоксально, может стать использование тишины или окружающих звуков при сопровождении 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 полную тишину используют 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.



Задание 3.5

Объединитесь в группы по три-четыре человека и снимите видеоролик, в котором один из вас будет читать стихотворение. Наложите на ролик музыку и продемонстрируйте в классе. Обсудите разницу восприятия видео с музыкой и без нее.

Как с «Прибытия поезда» началась история кино

Короткометражный безмолвный фильм «Прибытие поезда на вокзал Ла-Сьота» длиной в 50 секунд был создан в 1896 году Огюстом и Луи Люмьерами. Они были одними из первых, кто создал движущиеся картишки. Если верить широко известной истории, когда тихое черно-белое изображение движущегося локомотива начало заполнять экран, люди в парижском кинотеатре подумали, что он собирается въехать прямо в них. Они запаниковали и бросились к выходу.

Рекомендуем вам самостоятельно оценить кинематографическое мастерство братьев Люмьер, найдя фильм на YouTube по ключевому словосочетанию «прибытие поезда».

Многие из ранних работ братьев едва ли можно было классифицировать как фильмы даже в то время. В основном речь шла о коротких фрагментах. «Прибытие поезда» выделялось на фоне остальных 1400 однominутных фильмов. Действие происходит на платформе железнодорожного вокзала. 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 поражает своей простотой и способностью привлечь зрителей к действию на экране.

Слово против технологии

Мир меняется, и детям больше не обязательно читать сказки. Они играют в игры на компьютерах, и у них, как правило, есть мобильный телефон вместо книги. Тем не менее, писатели настойчиво пишут сказки, которые в некоторых случаях пользуются большим успехом. Автор серии книг о Гарри Поттере – британская писательница Джоан Роулинг – доказала скептикам, что в наши дни слово все еще может брать верх над технологиями (рисунок 3.2).



Рисунок 3.2. Серия книг о Гарри Поттере, Дж. Роулинг
(ист. – hprosmen.ru)

Итоги



Подумайте, почему такие известные фольклорные персонажи казахских сказок как Алдар-Косе и Кожа Насыр – несмотря на множество их шалостей, за которые в современном Казахстане легко угодить под суд – все равно почитались у народа. Как это связано с манипуляцией в искусстве? Найдите примеры в материалах казахстанских СМИ, когда герои-нарушители получали в обществе положительную оценку своих действий.



Создать удачный фейк без определенного понимания принципов художественного мастерства чрезвычайно сложно. Изучите при помощи поисковика и различных источников тему взаимосвязи искусства с фальшивым контентом. Подготовьтесь к обсуждению с учителем следующих вопросов:

- 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?

4

ГЛАВА

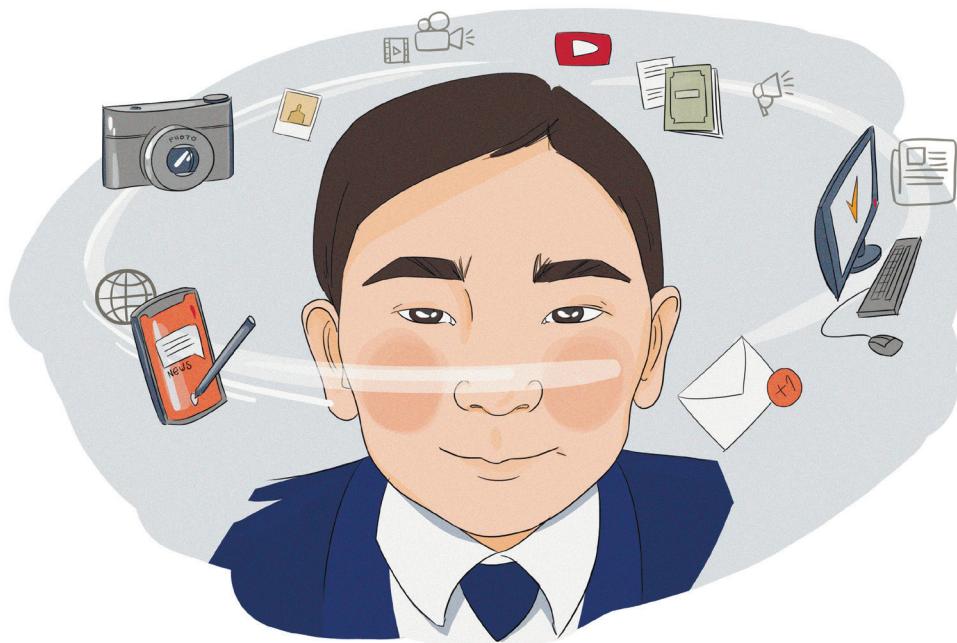
ИНФОРМАЦИЯ

ИСТОЧНИКИ ИНФОРМАЦИИ



КЛЮЧЕВЫЕ СЛОВА:

информация
источник информации
информационные угрозы
искажение информации



Вы узнаете:

- какими признаками обладает качественная информация,
- как человечество живет в условиях «информационной деревни»,
- почему достоверность информации определяется каскадами.

Вы научитесь:

- исследовать свое личное медиаполе,
- оценивать новостную подачу в разных источниках,
- замечать угрозы, которые скрывает ежедневный поток информации.

Информация и ее признаки



Слово «**информация**» мы слышим каждый день. Новости, которые мы узнаем, 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 через те или иные детали, штрихи, признаки. 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 кислое, летнего или осеннего урожая, мягкое или твердое, растет на дереве, в нем много «железа», имеет гладкую кожуру и т.д.

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

- актуальная, важная
- правдивая и неправдивая
- научная, новостная, бытовая
- быстро создается и передается
- 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. При этом признаки яблока можно объединить в своеобразные группы: по вкусу, цвету, качеству и т.д. В случае с информацией поступим так же: систематизируем и сформулируем семь главных признаков информации – **ценность, влияние, гибкость, продуктивность, логистичность, интерактивность, проверяемость**. В Таблице 4.1 подробно описан каждый признак.

Признак	Описание
Ценность	Касается непосредственно вашей жизни. То есть, данная информация имеет определенную ценность именно для вас.
Влияние	Побуждает к действиям. Может влиять как на одного человека, так и на большое количество людей.
Гибкость	Под воздействием аргументов или других обстоятельств – например, научных открытий, которые опровергают или уточняют уже имеющиеся данные – информация изменяется или «изгибаются».
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 лживы, доказана или не обоснована.

Таблица 4.1. Признаки информации

Искажение признаков информации и его последствия

Ни для кого не является секретом или открытием, что информацию сегодня очень часто используют не только для информирования, создания новых знаний, позитивных продуктов, но и в негативных целях. В настоящее время в обиход вошли такие понятия, как «информационная война», «информационная атака», «пропаганда», «манипуляция», «фейк». Эти понятия связаны с использованием информации в негативном ключе.



Задание 4.1

Вспомните и зафиксируйте примеры негативного использования информации. Не вдаваясь в детализацию, определите, что за вид злоупотребления информацией был использован в том или ином случае.

Вышеуказанные понятия – от информационной войны до фейка – несут негативный смысл. Фейк – это плохо, манипуляция – это плохо. Это искажение, искривление, игра информацией, говорим мы, обобщая отрицательные явления. Но информация становится неправильной или негативной не просто так – изменяются в соответствующую сторону ее признаки, которые как раз и ответственны за негативный окрас сообщений, новостей, публичных заявлений и пр.

Пример

У нас есть очень интересная и редкая книга. Она находится в библиотеке. Чтобы ее прочитать, люди записываются в очередь за месяцы вперед. Но однажды кто-то умудрился сделать фотокопию этой книги и выложил ее, к примеру, в группу в одной из соцсетей. К чему это приведет? В библиотеку никто не пойдет, очередь исчезнет, потому что люди будут читать книгу с экрана ноутбука в любое удобное им время.

Но через какое-то время 10 человек решили: «О, а я тоже могу написать что-то подобное – 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 интереса к жанру, кто чтобы сравнить, а кто потому что все читают и говорят об этом.

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

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

Вспомним, что одно из ключевых свойств информации – ее ЦЕННОСТЬ. Описанный пример продемонстрировал нам механизм

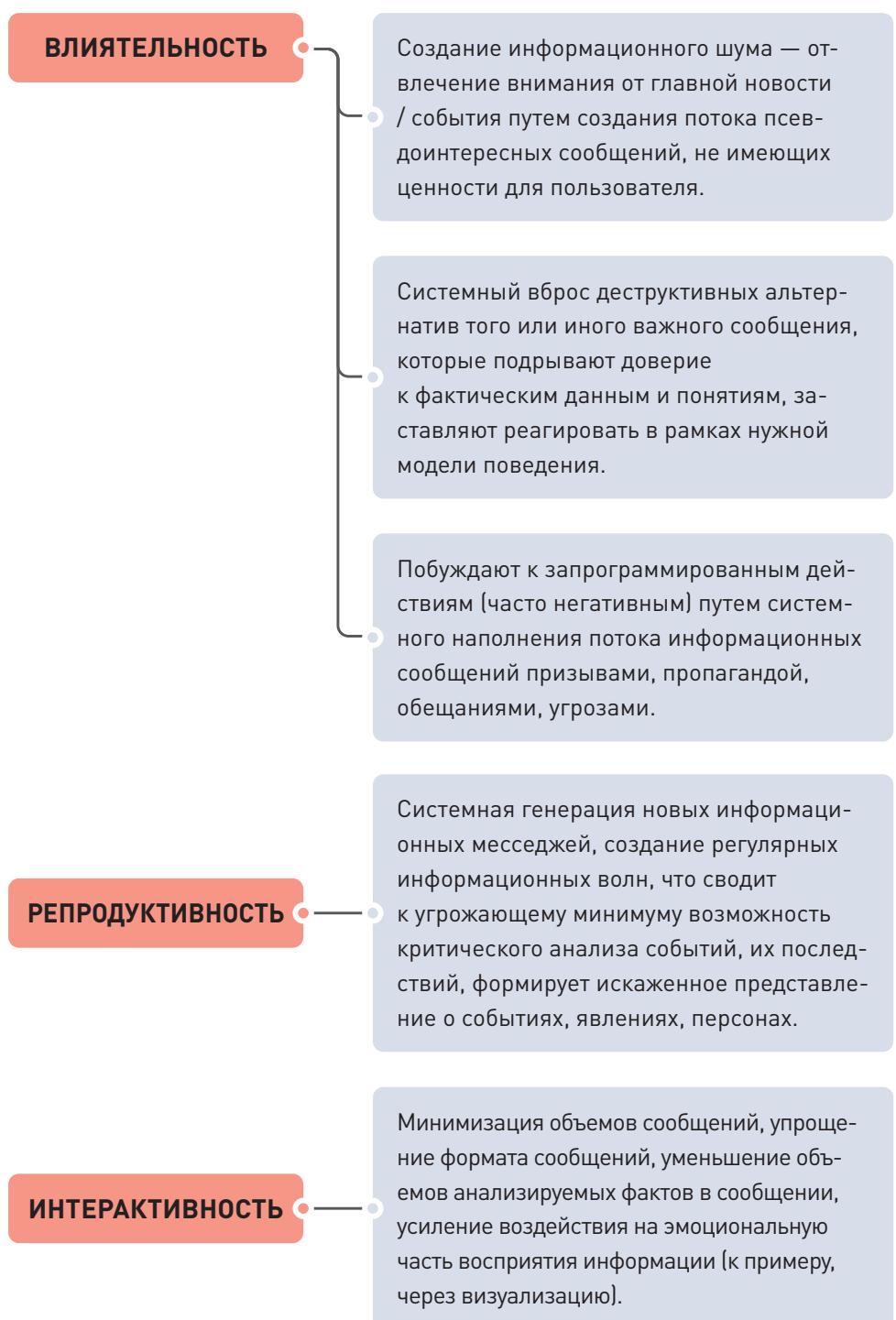
обесценивания информации. То есть, воздействуя на один из признаков информации, мы меняем смысл / значение / акценты самой информации.

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

Рисунок 4.1 демонстрирует, как различные свойства информации могут быть использованы для придания негативного смысла информации.



Рисунок 4.1. Схема использования свойств информации (продолжение)



ЛОГИЧНОСТЬ

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

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.

Рисунок 4.1. Схема использования свойств информации

**Задание 4.2**

На примере кейса об обязательной вакцинации в Казахстане проанализируйте способы, с применением которых данной позитивной информации придали резко негативный характер. Отразите эти моменты на схеме.

**Задание 4.3**

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 можете вспомнить только отрывочные факты);
- сколько новостей вы просмотрели / прочитали самостоятельно (учтываются и просмотры только по заголовкам);
- сколько новостей вы прочитали полностью.

Распределяйте новости по каналам получения:

- телевидение,
- интернет-СМИ,
- печатные медиа,
- радио,
- лента новостей в социальных сетях,
- чей-то пересказ.

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 анонсирования 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 (рисунок 4.2).

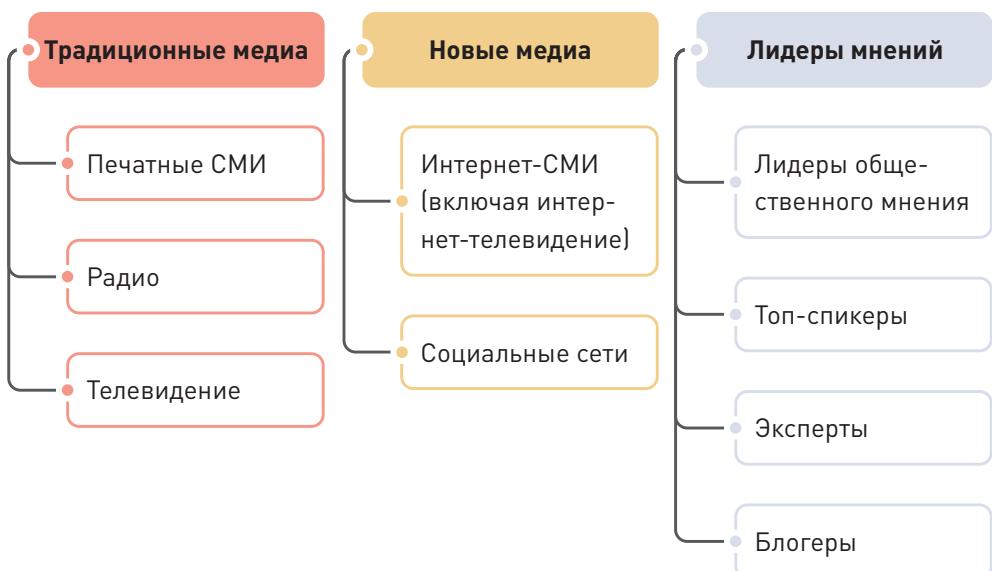


Рисунок 4.2. Классификация источников информации

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

Как видим, третья группа источников 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 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 в этом

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

Глобальное информационное пространство

Анализ современных источников информации и их признаков показал, что вместе 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, – полная практическая 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 годов их вытеснили видео-блоги. Если на заре появления Telegram это был мессенджер для коммуникаций, то сейчас в нем появился информационный функционал – Telegram-канал. Еще вчера в Instagram мы только делились фото, а теперь используем его и для переписки.

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

Почему же при этом мы подразумеваем некую скрытую угрозу, 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».



Задание 4.4

Попробуйте вспомнить и записать, какие последние новости за неделю вы можете назвать о событиях: в мире (1), в Казахстане (2), в вашем городе (3). Подумайте, почему количество новостей различается.

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 потребителя 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 рядовой обыватель 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. 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. Рисунок 4.3 красноречиво демонстрирует принцип информированности жителей «информационной деревни», которыми, по большому счету, являются мы с вами.

Обилие информации практически исключает возможность ее препроверки. Приверженность тем или иным медиа, лидерам мнений, блогерам 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.



Рисунок 4.3. «Информационная деревня»

Обилие информации практически исключает возможность ее проверки. Приверженность тем или иным медиа, лидерам мнений, блогерам 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.



Это интересно!

По данным бюро экспресс мониторинга общественного мнения DEMOSCOPE, в 2015 году основным источником информации для казахстанцев (48% опрошенных) было телевидение. Еще 40% респондентов сообщили, что в основном получают информацию из интернета. Радио выбрали лишь 7% опрошенных, печатную прессу – 4%.



Задание 4.5

Проведите мини-опрос среди своих друзей и родных, узнайте, из каких источников они преимущественно получают информацию. Определите, насколько изменилась ситуация с 2015 года. Расскажите о главном источнике информации для себя. Обсудите результаты в классе.

Механизм искажения информации (принцип каскадности информирования)

Ранее мы говорили о сложности получения достоверной информации. Этому способствуют целый 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, день, просто утром), для меня является «новым». Уже после может сработать механизм критического мышления: «А посмотрю-ка я на дату публикации новости.

Может, это поздняя перепубликация одного ресурса с другого?» Но не всегда этот механизм включается.

В то же 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 зачастую оперируем искаженной информацией и на ее основе 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, уполномоченные органы с официальным сообщением, уполномоченные лица с заявлением и ведущие, топовые СМИ (телевидение или интернет-СМИ) с новостями.

Эти сообщения достаточно оперативны (если система информирования работает в рамках цивилизованных правил), лаконичны, не содержат много деталей, но достаточно информативны, чтобы сориентировать аудиторию в том, что это за событие, каковы его последствия. Это – **«первый каскад информирования»** (рисунок 4.4).



Рисунок 4.4. Первый каскад информирования

Далее в информирование включаются те каналы и источники, которые не успели поучаствовать в «разделе пирога» в первом каскаде. Причин этому (как объективных, так и субъективных) может быть много: попросту не успели, не хватило ресурсов для оперативности, специфика работы и т.д. Рисунок 4.5 демонстрирует составляющие второго каскада информирования, рисунок 4.6 – третьего каскада информирования.



Рисунок 4.5. Второй каскад информирования

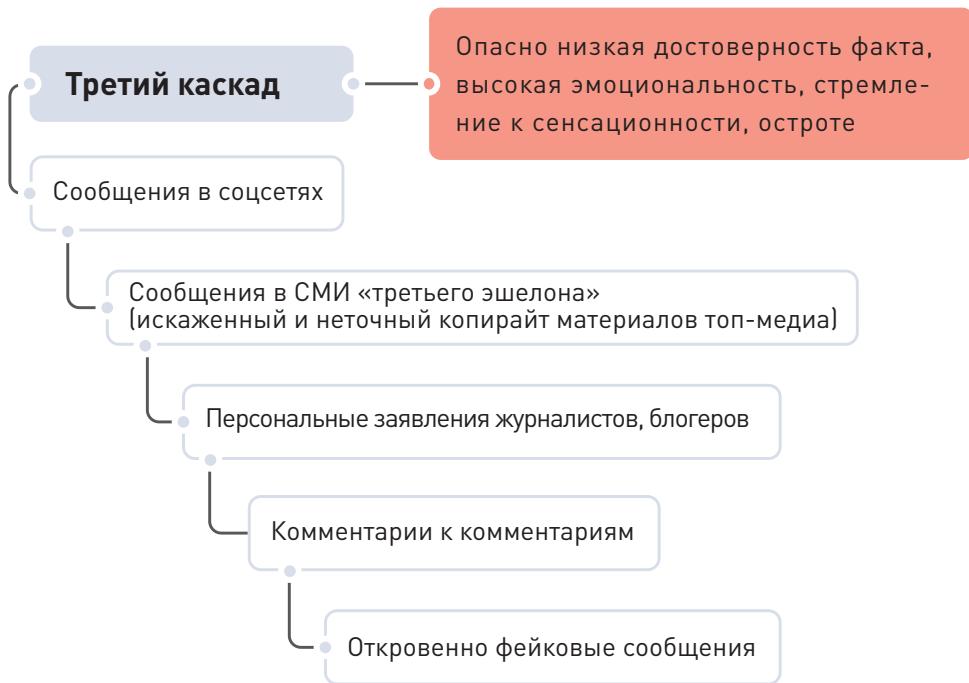


Рисунок 4.6. Третий каскад информирования

Не так сложно заметить, что от каскада к каскаду достоверность фактов о событии снижается (рисунок 4.7), так как все большую роль начинают играть не факты как таковые, а мнения, суждения, трактовки, вариации на тему, рассуждения, заявления о нем.



Рисунок 4.7. Схема искажения информации



Задание 4.6

Объединитесь в группы по три человека. 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 указано в качестве первоисточника информации;
- точность передачи информации;
- использованы ли дополнительные данные;
- искажены ли данные.

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

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

Говоря о выборе той или иной информации, мы часто сталкиваемся с ее «изобилием». Помните термин «информационная деревня»? Главная его характеристика – 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 попадаем в ситуацию, когда 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 рискуем вовсе потерять изначальный смысл реальных фактов события.

Описанная схема сегодня является объективной реальностью. Ее проявления имеют уже устоявшиеся названия: информационный шум, информационные волны (или цунами), информационный троллинг.

Информационный шум

Информация стремится к нам отовсюду, из разных источников, каждую минуту. Из-за огромного количества схожего контента мы зачастую 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 пролистывание на 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 деталях, отделить факты от мнений и рассуждений, уловить главную идею. В этом и кроется главная 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 вымысленных, фейковых. Рисунок 4.8 демонстрирует системные угрозы информационного шума для потребителей информации.

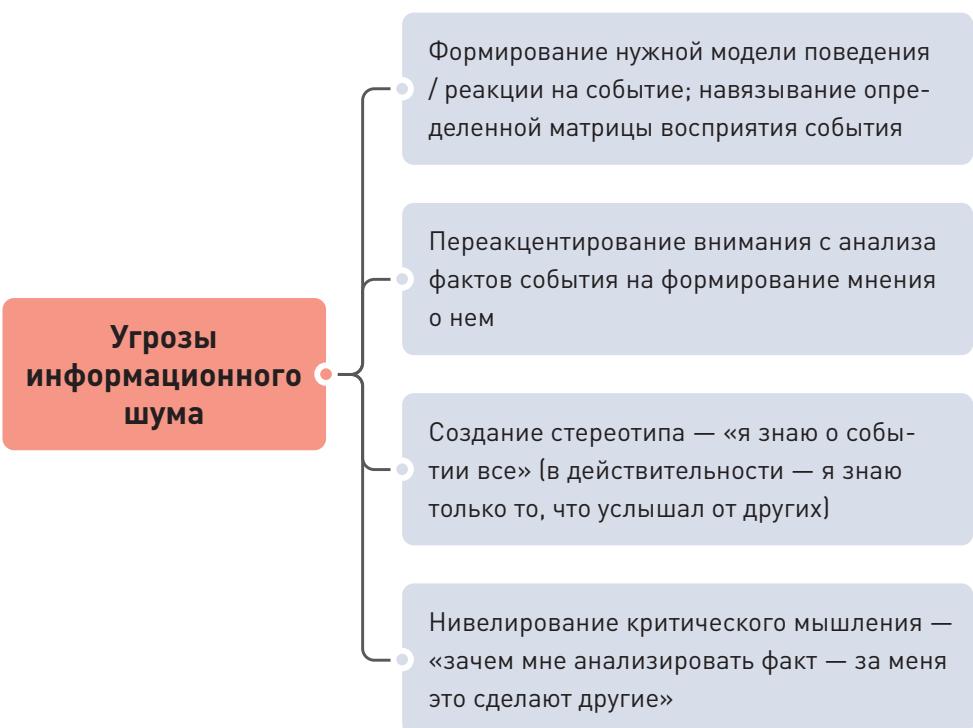


Рисунок 4.8. Угрозы информационного шума

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 течение нескольких дней, но чаще всего это искусственное явление. Как правило, информационные волны создаются группой медиа для привлечения внимания к какой-то теме или же наоборот — для отвлечения внимания 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 массивный информационный удар в виде следующей или нескольких. И так может повторяться ежедневно.

Рисунок 4.9 демонстрирует, чем грозит аудитории такая ситуация.



Рисунок 4.9. Угрозы информационных волн

Информационный троллинг

Понятие «троллинг» пришло в информационное пространство из сленга социальных сетей. В простой доступной интерпретации троллинг сводится к забалтыванию какой-то темы, словесному подшучиванию над кем-то или чем-то. В инфополе троллинг имеет немного иное определение и представляет собой системную, целенаправленную «загрузку» медиапространства громкими, но бессодержательными информационными проявлениями по теме события. Они отвлекают внимание, но базируются на речах знаковых персон, ссылаются на псевдопризнанные источники, несут больше эмоциональную нагрузку, чем фактологическую. Рисунок 4.10 показывает, какие угрозы кроются в, казалось бы, безобидном троллинге.

Теперь вы знаете, как устроено новостное поле, и что мы живем в большой «информационной деревне». В следующих главах разберемся, как не попасться на удочку манипуляторам.

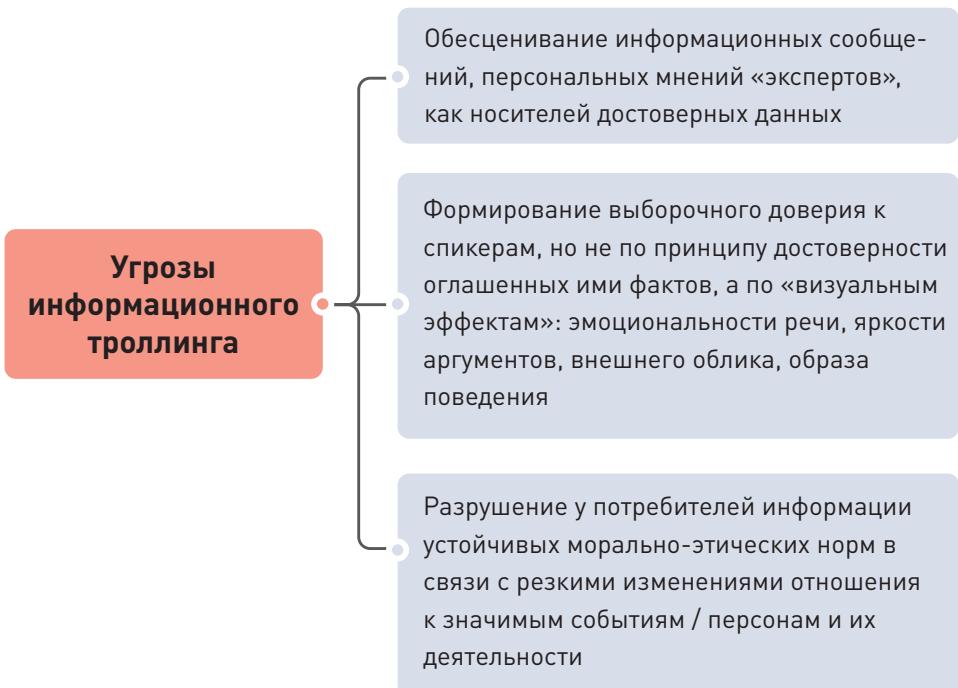


Рисунок 4.10. Угрозы информационного троллинга



Задание 4.7

Поиграйте в игру «Глухой телефон». Один ученик должен быть ведущим. Остальные учащиеся делятся на две группы: первая выходит за дверь, а вторая остается в классе и будет выполнять роль экспертов. Ведущий приглашает в класс одного из учеников первой группы и сообщает ему новость, состоящую из сотни слов, с фактами. Затем приглашается второй ученик из первой группы, и первый передает ему то, что он услышал от ведущего. Второй доносит новость до третьего и так до тех пор, пока за дверью не останется последний ученик. Эксперты при этом должны внимательно следить за тем, на каком этапе и как именно исказилась информация. В конце игры необходимо еще раз прослушать изначальное сообщение и сравнить его с изложением последнего члена первой группы. Проанализируйте, как информация может изменяться и искажаться.

Итоги



Объединитесь в группы по три-четыре человека. Выберите определенную тему и сделайте фотоколлаж. В одной его части разместите угрозы информационного шума, информационных волн и информационного троллинга, а в другой – параллельно каждой угрозе расположите скриншоты из новостных лент, открытых пабликов или газет, подтверждающих их наличие.



Объединитесь в группы по три-четыре человека. Подготовьте «правильную новость». В новости должны найти свое отражение не менее трех 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 2 тысяч знаков.



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

5

ГЛАВА

ФОРМАЛЬНАЯ ЛОГИКА

КУРС МОЛОДОГО
БОЙЦА



КЛЮЧЕВЫЕ СЛОВА:

манипуляция

логика

критическое мышление

аргумент



Вы узнаете:

- откуда произошло слово «манипуляция»,
- что изучает логика, и кто создал ее научную базу,
- как используют логические уловки в медиа.

Вы научитесь:

- отличать злонамеренные манипуляции от позитивных,
- распознавать логические ошибки и уловки,
- бороться с манипуляциями при помощи законов формальной логики.

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), очередности вступления в бой, если необходимо – отступления и т.д. Речь шла об искусстве управления людьми с какой-то целью, изначально – с военной. Нас, как эту «горсть» людей (манипулу), бросают на определенный 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: например, испытывать чувство вины, делать чужую работу, уважать кого-то «по умолчанию» и т.д.



Манипуляция – это лишь инструмент, которым при желании можно пользоваться и в благих целях. Примеры таких позитивных манипуляций мы можем наблюдать в повседневной жизни: например, во взаимодействии родителей с детьми, учителей с учениками, начальников с подчиненными. В этих случаях к манипуляциям прибегают во имя обоюдных интересов, не имея намерения навредить человеку, который подвергается этим безобидным уловкам.

Так ли это плохо?

Манипуляция – не всегда зло. Взрослые в общении с детьми, учителя в общении с учениками, генералы в общении с солдатами, правительство в общении с народом часто пытаются сделать все быстрее, донести решение или мысль, которые до этого были обдуманы целыми поколениями или специальными институтами. И либо они ленятся объяснять, либо считают, что объяснить – долго.

Как же 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 и даже собственные убеждения. Оно лежит в основе человеческого прогресса и научного мышления. Оно предписывает нам перепроверять всю информацию и свои 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 нас математики и программисты – это иначе зашифрованная речь. У речи есть формы: мы ведь строим предложения по определенным формулам. Например, если в конце предложения стоит вопросительный знак, значит, это вопрос, если точка – утверждение. Или, если мы обращаемся к конкретному человеку, мы сразу определяем его статус в речи: родственный («папа, мама, дядя» и т.д.) или социальный («господин президент», «уважаемый», «эй ты!»).

 **Логика** – это наука о законах мышления и его формах. Формы речи изучаются и определяются именно в ее рамках.

Последовательность суждений тоже имеет смысл. Чтобы сделать правильный вывод, нужно руководствоваться четырьмя законами формальной логики. Их никто намеренно не придумывал, они были сформулированы на основе человеческого опыта.

Форма – важнейшая часть мышления. Мы должны научиться формально определять, что правда, а что манипуляция, то есть ложь (даже если «во благо»). Это азы критического мышления.



Задание 5.1

Попробуйте определить, правильно ли с формальной точки зрения построены следующие утверждения:

1. Все Ладинки имеют хвосты.

Канила тоже имеет хвост.

Значит, Канила – Ладинка.

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

История манипуляций и борьбы с ними

Более 2500 лет назад в Древней Греции активно распространялись школы софистики. Там давали уроки начинающим политикам. Их учили, как при помощи ораторского искусства добиваться своих целей. От философов софисты отличались тем, что более всего чтили достижение практической цели. Тогда и родилась формула «цель оправдывает средства».

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

Три из них сформулировал Аристотель:

Закон тождества

«...иметь не одно значение – значит, не иметь ни одного значения», писал 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:

Канила – хороший и скромный человек, любит ездить на велосипеде.

Из него получится хороший аким города!

В первой части утверждения говорится о личных качествах человека, а вывод делается о его профессиональных качествах, что далеко не тождественно.

Или:

Ладинка – человек.

Ладинка в то же время робот.

Ладинка не может быть одновременно и 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:

Ладинки – неопасные существа.

Некоторые из Ладинок могут навредить

Из этого следует, что Ладинки – совсем не безопасные существа, даже если большинство из них таковыми все же является. Подобные ложные обобщения встречаются сплошь и рядом.

Закон исключенного третьего

Два противоречащих друг другу суждения не могут быть одновременно истинными или 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:

Ладинки ничего не соображают в кухне!

Ладинки, готовящие борщ, великолепны!

Либо Ладинки ничего не смыслят в кухне, либо Ладинки могут готовить вкусные блюда, но никак не одновременно и то, и другое.

Закон достаточного основания

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

Он был добавлен в формальную логику спустя 2000 лет ее существования в XVIII веке выдающимся немецким ученым Вильгельмом Лейбницием.

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

Почему в формальную логику вторгся неформальный закон? К тому времени был накоплен большой багаж знаний, на страницах книг было

высказано много мнений, и люди путались, считая книжное мнение единственным правильным. Однако в книгах было много суждений, которые читатели ошибочно воспринимали за истину в последней инстанции.

Нарушение этого логического закона мы видим ежедневно.

Например:

Доказано, что есть хлеб вредно!

Многие люди «ведутся» на подобные утверждения. При этом кем доказано, когда, почему, как, не говорится. А нам нужно получить ответы на эти вопросы, прежде чем верить источнику.



Задание 5.2

Объединитесь в группы по три-четыре человека и обсудите, каким законам формальной логики противоречат эти утверждения:

1. Я познакомился с Ладинкой. Хорошая девушка. А с другой стороны, нечестная.
2. Я всегда выступаю за законность, поэтому обругал человека, бросившего окурок мимо урны.

Классификация логических уловок (ошибок)

В целом логическая ошибка и логическая уловка – это одно и то же. Отличие лишь в том, что ошибка допускается несознательно, а уловка вводится в речь специально. Они строятся на противоречии четырем основным законам формальной логики.

Ignoratio elenchi, или «подмена тезиса»

В переводе с латыни – «невежественное опровержение». Это попытка отвлечь оппонента, представив «аргумент», не имеющий отношения к первоначальной теме обсуждения. Прием хорошо известен «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 формальной логики – закону тождества.

Уловка в том, чтобы построить свое «доказательство» на том, что оппонент сделал какое-то слабое или неверное утверждение. Благодаря этому у аудитории (а часто даже и у самого оппонента) создается ощущение, будто он действительно сделал такое утверждение. Например, часто можно встретить следующее заявление:

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

Легко увидеть, что вывод «вечно всем недовольны» строится как раз на подмене понятий, ведь оппонент был всего лишь недоволен дорогами и бордюрами. Следовательно, все дальнейшие рассуждения о пагубности пессимизма, о необходимости самому что-то изменить в жизни – это продолжение удачно использованной логической уловки. Никакого отношения к логике и реальности эти рассуждения иметь не будут.



Это интересно!

Ignoratio elenchi – это всегда манипуляция, но не обязательно негативная. «Позитивные» примеры мы каждый день встречаем 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 распространённости логическая уловка – это *petitio principii* («предвосхищение основания»). Она преследуют нас изо дня в день во всех каналах коммуникации. Эта логическая уловка строится на нарушении четвертого закона логики – достаточного основания.

Поскольку уловка не формальная (ее нельзя определить просто по неправильному построению логической цепочки), идентифицировать ее сложнее. Именно эта уловка чаще всего встречается в социальных сетях: человек для обоснования своих выводов относительного какого-то предмета, явления или другого человека использует аргумент, вызывающий сомнения и сам нуждающийся в доказательстве.

Ярким примером использования такой уловки стало название диска Элвиса Пресли, вышедшего в 1959 году: «50 миллионов фанов Элвиса не могут ошибаться». Конечно, могут! В мире живет 7,8 миллиардов человек, и мнение 50 миллионов человек – недостаточное основание для принятия их точки зрения как единственно верной.

В Казахстане эта уловка хорошо работала в условиях паники по поводу случаев заболевания менингитом и смерти нескольких заболевших весной-летом 2018 года. Рассылки в мессенджерах недвусмысленно говорили нам: «Если заболели и умерли уже несколько человек, то каждый из нас может заболеть менингитом и умереть». На самом же деле заболеть мог только тот, кто контактировал с носителем менингококковой инфекции и обладал ослабленным иммунитетом.

Разновидности petitio principii

Argumentum ad hominem – «атака на человека»

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

Это одна из самых бесхитростных уловок – переход от обсуждения предмета спора к обсуждению личности, участвующей в этом споре. И хотя ее очень легко разоблачить, она используется регулярно и с большим успехом. Главное правило для нас: важно не КТО говорит, а ЧТО он говорит.

Пример:

Ладинка сказала, что Канила украл деньги из бюджета страны.

Но Ладинка сама осуждена за коррупционные преступления.

Следовательно, верить Ладинке нельзя.

В действительности мы можем верить ей, а можем и не верить. Важно понимать, что личность Ладинки значения не имеет, имеют значение лишь факты, приведенные ею.

Наблюдать, как эта уловка работает в реальности, можно было на всем протяжении противостояния между «защитниками Кок-Жайляу» и властями, предпринимателями, желающими построить в этом алматинском урочище курорт. Когда в ответ на критику, что строительство может погубить природу, угрожать городу оползнями и т.д., «защитников Кок-Жайляу» стали называть «экологическим Талибаном», мы опять столкнулись с элементарной заменой атаки на аргумент атакой на личности.

Даже если предположить, что «защитники» превратились в какую-то секту, возводящую в абсолют свои экологические идеи, это ровным счетом никак не опровергает их аргументов. Аргументы могут быть опровергнуты только другими аргументами.

Argumentum ad verecundiam – «апелляция к авторитету»

Другая версия «предвосхищения основания» – уловка *argumentum ad verecundiam*, что в переводе с латыни – «аргумент к скромности», но означает, наоборот, «апелляцию к авторитету».

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

Этот прием любят использовать в рекламе, когда различные знаменитости «продают» еду, напитки, технику и т.д. Часто производители рекламы идут на прямой подлог, ссылаясь на мнимых авторитетов. Многочисленные «ассоциации стоматологов», «сообщества терапевтов», «союзы финансистов» и т.д. на самом деле созданы исключительно для рекламы конкретного товара.

Но главная ошибка кроется не просто в ссылке на мнение авторитета, а в вере, что его мнение безошибочно. И тут важно вовремя заметить, что футболист не является специалистом по чипсам, а боксер – специалистом по банкам, что самые лучшие экономисты многократно ошибались, а фальшивые стоматологи стремятся лишь к тому, чтобы подороже продать вам самую обычную зубную пасту в новой упаковке.

Argumentum ad antiquitatem – «апелляция к традиции»

Примеры манипуляций: «Так считается издавна», «Так делали на протяжении веков» и пр. При этом за века изменились условия существования человека, наука шагнула вперед, трансформировались нравственные устои общества. 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 подается 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 у интер-

нет-пользователей, оставляющих комментарии к спорным постам в социальных сетях.

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, введенную оппонентом в заблуждение.

Argumentum ad baculum – «палочный аргумент»

Это даже сложно назвать аргументом в привычном смысле слова. Оппонента попросту заставляют согласиться с чужим мнением: «Если вы не согласитесь, произойдет что-то плохое». Мы можем столкнуться с этим в банке, например, когда начинаем спорить по поводу трактовки того или иного пункта договора, а нам говорят: «Или вы соглашаетесь с нами, или мы не дадим 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 времен нам знакомо идеологическое клише – «Кто не с нами, тот против нас!». Это изначально ложное суждение вытекает из нарушения четвертого закона логики – достаточного основания. Для утверждения «он против нас» требуется гораздо больше доказательств помимо 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. В данном случае 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». Несмотря на то, что никакой связи между джазом и предательством, конечно, нет, эта конструкция в разных вариациях с успехом используется манипуляторами 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 ученому соседу»).

В современных реалиях этим в основном грешат чиновники, затрудняясь 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.

Fallacia fictae universalitatis – «ложное обобщение»

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

Эта ошибка лежит в основе любой ненависти: от национальной («все представители этого народа 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 эта уловка тоже распространена и приводит к возникновению устойчивых стереотипов о мужчинах, женщинах, представителях различных профессий. Еще один пример ложного обобщения – *post hoc, ergo propter hoc* («после этого, значит, по причине этого»).

Это попытки констатировать причинно-следственные связи там, где на самом деле их нет, а есть простая последовательность не связанных между собой событий.

Например древние суеверия, когда пролет кометы или солнечное затмение ассоциировались со стихийными бедствиями, или любые бытовые приметы: от чёрной кошки, перебегающей дорогу, до встретившейся женщины с пустым ведром. Вероятно, когда-то эти события действительно совпадали с какими-то несчастиями, и, не имея возможности объяснить причину несчастий, люди связали их с предыдущими событиями – кометой или кошкой.

Часто мы сталкиваемся с этой ошибкой и в других обстоятельствах, довольно серьезно влияющих на нашу жизнь. Иногда мы поступаем, как дикие племена, создающие «карго-культы» (к примеру, они возводят мо-

дели самолетов и поклоняются им, помня о том, что когда-то с них скидывали бесплатную еду).

Думая о вершинах, которые когда-то покорила компания под руководством иностранца, на работу в качестве руководителя стремятся принять любого иностранца – без оглядки на уровень его профессиональных компетенций. В других случаях, бизнесмены могут копировать некие внешние условия работы успешных компаний (кофе-машину и удобные пуфики) и ошибочно ожидать таких же результатов, не заботясь о профессиональном росте сотрудников и создании условий для эффективного труда.

Логика не стоит на месте, и сейчас появилось множество научно-популярных статей, чьи авторы указывают и на другие варианты логических уловок. Если вас заинтересовала тема, вы легко можете найти их в сети. Все они в той или иной степени являются вариациями рассмотренных в этой главе классических ошибок и строятся на нарушении хотя бы одного из законов логики.

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

Итоги:



К какой логической уловке относятся эти утверждения?

1. Канила не дает нам денег.

Мы страдаем.

Канила плохой.

2. Ладинка из Ладинии.

Ладинка постоянно выбрасывает мусор у подъезда.

Все из Ладинии – такие же неряшливые, как Ладинка.

3. Вы пишете это потому, что просто не знаете, кто правит миром.



Разделитесь на две команды и выполните задание в два этапа. На первом этапе каждая из команд по выбранной теме (одна команда – одна тема) готовит текст с применением всех уловок:

→ Подмена тезиса

- Предвосхищение основания
- Аргумент к человеку
- Аргумент к скромности
- Апелляция к традиции
- Апелляция к незнанию
- Аргумент к тошноте
- Апелляция к милосердию
- Палочный аргумент
- «не следует»
- «То же посредством того же» / «порочный круг»
- Ложное обобщение

На втором этапе каждая из команд готовит опровержение тексту другой с соблюдением законов логики.



По одной из актуальных тем (например, «Трансплантация органов», «Пандемия», «Похудение» и т.п.) найдите в материалах СМИ примеры манипулирования с намеренным нарушением:

- закона тождества;
- закона противоречия;
- закона исключения третьего;
- закона достаточного основания.

Обсудите эти утверждения в группе и предложите свои контраргументы в соответствии с законами логики.

6

ГЛАВА

МЕДИА И РЕКЛАМА



КЛЮЧЕВЫЕ СЛОВА:

реклама
пропаганда
PR-кампания



Вы узнаете:

- на какие сферы жизнедеятельности реклама оказывает влияние,
- какие функции выполняет реклама,
- какие стереотипы используют рекламодатели.

Вы научитесь:

- различать виды наглядных материалов,
- распознавать манипуляцию в рекламе,
- создавать собственные рекламные образцы.

Реклама и медиа

Слово «реклама» произошло от латинского *reclamere*, что в переводе означает «утверждать, выкрикивать». По другой теории, у «рекламы» французское происхождение – *reclame*, что переводится как «привлекать к себе внимание». От источника к источнику разнятся и определения этого термина. У каждого из нас есть собственное представление о рекламе и опыт, как она влияла на нас.

Толковый словарь русского языка С. И. Ожегова предлагает следующее определение:

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

В рамках нашего предмета 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.

История рекламы

Человечество торгует тысячи лет – примерно столько же существует реклама. 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. В местах продажи слышались громкие и повторяющиеся крики продавцов. Самый старый рекламный текст был найден в Древнем Египте, в городе Мемфис: «Я Рино с Крита, по повелению богов толкую сны».

Современная реклама в том виде, в котором мы ее знаем, берет начало от изобретения первого печатного станка Иоанном Гуттенбергом в 1450 году. Это открытие ознаменовало качественно иной этап развития маркетинговых технологий.

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

Первыми примерами социальной рекламы (рисунок 6.1) считаются работы Джеймса Флегга 1917 года «Ты нужен Американской армии!». Следом подобные плакаты появились и в Советском Союзе: «Ты записался добровольцем?».

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



Рисунок 6.1. Реклама армейской службы

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

→ **Социальную** (достижение общественно полезных целей, информирование общества о различных инновационных достижениях, анализ и сравнение различных изделий, формирование эстетических представлений). К социальной рекламе относятся, например, плакаты о необходимости соблюдения чистоты в общественных местах, охране лесов от пожаров, баннеры с разъяснением услуг электронного правительства.

→ **Нравственно-правовую** (продвижение этических и правовых норм). Сюда можно отнести рекламные ролики, направленные на соблюдение правил дорожного движения, охрану общественного порядка, своевременную уплату налогов, защиту прав детей, запрет использования детского труда.

→ **Духовную** (формирование патриотизма или манипуляция общественным сознанием). В качестве примера можно привести рекламу, призывающую любить свою Родину, страну, родной город или аул. Кроме того, это может быть манипуляционный призыв к общественным работам в духе «прояви себя патриотом».

→ **Политическую** (агитационные материалы, формирование имиджа политика или политической партии). Здесь следует иметь в виду все политические кампании, то есть рекламу во время выборов.

→ **Идеологическую** (фактор, влияющий на становление и формирование мировоззрения человека). Такая реклама призывает, к примеру, заботиться о детях, постоянцах домов престарелых, воспитанниках детских домов, сопротивляться жестокому обращению, противостоять педофилии и любым формам насилия.

→ **Психологическую** (воздействует на желания и мечты покупателя, не взывая к его разуму). Здесь имеется в виду реклама, начинающаяся с таких вопросов, как «желаешь быть красивой?», «мечтаешь посмотреть мир?», «хочешь стать студентом лучшего университета?» и т.д.

→ **Коммуникативную** (функция коммуникации между рекламодателем и рекламополучателем, поскольку перед рекламой поставленна задача донести необходимое сообщение до потребителей товаров и услуг). Сюда можно отнести рекламу конкретных видов деятельности или товаров.

→ **Образовательную** (в процессе просмотра рекламы, а также внедрения новых технологий товаров и услуг, человек может почерпнуть для себя информацию абсолютно из всех сфер жизни). Из такой рекламы зритель узнает и причины появления налета на плитке в ванной комнате, и оценит последние инновационные разработки в компьютерной технике.

→ **Экономическую** (стимулирование потребителей к приобретению товаров и обеспечение экономической целесообразности производственно-сбытовой деятельности предприятий). Упомянутую функцию выполняет любая реклама, которая нацелена на реализацию товара и получение большей прибыли.

→ **Эстетическую** (культурную). Во многих рекламных роликах очень качественно подобраны цвета и звуки, которые могут повлиять на человека, вызвав в нем 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 свои особенности в разработке и подаче рекламы, она остается универсальным инструментом передачи информации. Она понятна людям разных национальностей и вероисповеданий.

Виды визуальных материалов

Реклама многогранна: она может предстать перед нами как в виде кандидата на пост президента страны, так и в виде сюрприза в шоколадной конфете. Но все же ее можно классифицировать, разделить по видам, каждому из которых присуща своя специфика. Разновидности рекламы выделяют в зависимости от ее назначения.

С различными видами визуальных материалов мы ежедневно сталкиваемся на улице, просматривая сайты и ленты социальных сетей, телевизионные каналы и газеты. Рекламные постеры есть даже у нас дома. Каждый из этих рекламных образцов имеет конкретную цель. С помощью одних компаний хотят продать нам товар, с помощью других призывают к социальной ответственности. В то время как одна рекламная брошюра пропагандирует участие в выборах, другая агитирует за конкретного кандидата. В таблице 6.2 собраны основные рекламные разновидности.

<p>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.</p>	
	<p>Социальная реклама – это когда посредством рекламы обществу хотят объяснить какие-то проблемные моменты общественного устройства. Например, вред ранних браков для здоровья подростков, необходимость обеспечения равных возможностей для детей с особенностями (например больных аутизмом) или для лиц с инвалидностью, чтобы они имели возможность выходить на улицу, посещать развлекательные центры, кинотеатры.</p>

Агитация – это 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.



НАША ПАРТИЯ – САМАЯ ЛУЧШАЯ!
ГОЛОСУЙТЕ ЗА НАШУ ПАРТИЮ!

Политическая агитация – это тоже вид рекламы. Ее мы видим во время выборных 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, призванной навязать 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. Информация сообщается исключительно для того, чтобы тот, кто ее прочитал, просто был осведомлен о мероприятии или событии.

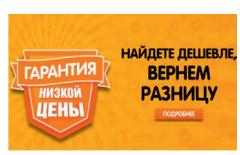
<p>PR-кампания – ряд мероприятий, проводимых для организации коммерческой, политической или социальной кампании (например, розыгрыш лотереи среди покупателей определенного магазина).</p>	
---	--

Таблица 6.2. Виды рекламных материалов



Задание 6.1

Разделитесь на три группы. Каждая группа получает набор карточек (рисунок 6.3). Обсудите внутри группы и подпишите, к какому виду сообщения относится каждый постер.

 JASYL JOL		
		
		

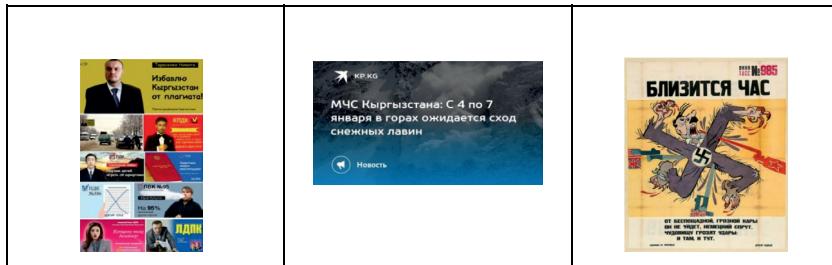


Рисунок 6.3. Рекламные постеры



Задание 6.2

Первая группа придумывает социальную рекламу, вторая группа – коммерческую рекламу, третья группа – рекламу-информирование. Можно нарисовать постер, подготовить сценку, снять ролик на телефон или сделать что-то другое. Допустим любой сюжет, который вы посчитаете нужным. Предмет (товар или услугу) рекламы можете выбрать самостоятельно. Презентуйте рекламу в классе.



Задание 6.3

Найдите и прочитайте закон Республики Казахстан о рекламе. Отметьте, какие требования предъявляются к рекламе в Казахстане, что можно, а что нельзя рекламировать. Обсудите в классе.



Это интересно!

Американские историки проекта Random History подсчитали, что в мире на рекламу ежегодно тратится более 500 миллиардов долларов США. В среднем по телевизору дети видят 40 000 рекламных роликов в год. Американская ассоциация психологов утверждает, что дети до восьми лет еще не умеют мыслить критически, поэтому безоговорочно верят всему, о чем говорят в рекламе.

Функции рекламы

Согласно исследователю Уильяму Уэллсу, реклама выполняет семь основных функций. Они базируются на том, что может получить рекламодатель от своей рекламы, или почему решает ее использовать:

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

Реклама, как и любое другое медийное явление, подразумевает создание послания и отправку его группе людей в расчете на то, что они отреагируют на него определенным образом. Мы каждый день встречаем огромное количество рекламных обращений – по телевизору и по радио, в газетах и журналах, в интернете и на билбордах. Реклама, хотим мы этого или нет, влияет на человека, его поступки, выбор, стиль жизни. Можно сказать, реклама манипулирует человеком. Она влияет на общество, а общество, в свою очередь, влияет на развитие рекламы.

Мы уже изучили основные виды манипуляций, работая с Главой 5. 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, когда часть информации опускают или искажают, обобщают до неузнаваемости, выдумывают ложную информацию, задают вопрос и не дают возможность ответить, ссылаются на авторитеты. Метафоры, юмор, шутки также могут использоваться как средство манипулирования.

Ученый в области психологии С. Л. Братченко выделяет пять видов манипулирования:

- манипулирование потребностями (использование желаний, влечений, интересов);
- «духовное» манипулирование (формирование у человека определенных идеалов и ценностей);

- интеллектуальное манипулирование (навязывание человеку мнений, точек зрения);
- манипулирование чувствами (использование эмоций);
- символическое манипулирование (формирование устойчивой реакции человека на определенные символы).



Задание 6.4

Рассмотрите рисунок 6.4. Ответьте на вопрос, сколько зубной пасты вы выдавливаете на зубную щетку, и выберите соответствующий вариант – А, Б или В.



Задание 6.5

Разделитесь на три группы в соответствии с выбранным ответом в задании 6.4. Обсудите, почему вы используете именно столько зубной пасты. Подумайте, сколько пасты рекомендуют стоматологи использовать для чистки зубов. Приведите из жизни другие примеры влияния рекламы на человека.



Рисунок 6.4. Манипуляция в рекламе

Приемы 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** – дает информацию о товаре или об услуге, разъясняет, для чего они предназначены. 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 апеллируют к любви, семье, друзьям, хорошим временам и чувствам, которые с ними связаны. Реклама говорит: купите этот 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 попадаются в рекламе 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 долго жить, 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 рассмотрим психологические установки в рекламе. Следующие стереотипы широко используются авторами рекламных материалов:

→ *Дефицит – всегда хорош и ценен.* Прекрасного не может быть много. Лучше, когда товар существует в строго ограниченном количестве.

→ *Дорогой товар – значит, хороший товар.*

→ *Традиционное добротно и достойно покупки.* 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 – «швейцарские», а лучший костюм – Hugo Boss.

→ *Раз все так делают – значит, это правильно.*

Какие еще манипуляционные инструменты используют 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, чтобы прочитать его, читатель должен пролистать весь журнал – в том числе, и рекламные вкладки.

Другой метод манипулирования используется 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.

Итоги:



Найдите информацию о том, по каким правилам составляются рекламные тексты. Напишите рекламный текст, применяя следующую форму построения:

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

ГЛАВА

7

КИБЕР- БЕЗОПАСНОСТЬ



КЛЮЧЕВЫЕ СЛОВА:

пароль
персональные данные
безопасность



Вы узнаете:

- что входит в понятие кибербезопасности,
- как защитить личные аккаунты в социальных сетях от кибератак,
- в чем риск использования чужого устройства для входа в свои аккаунты.

Вы научитесь:

- составлять надежные пароли,
- настраивать двухфакторную аутентификацию,
- разбираться в настройках безопасности социальных сетей, мессенджеров и почтовых сервисов.

Безопасность в социальных сетях

Угрозы интернета и социальных сетей

Всеобщая цифровизация несет не только огромное количество благ и удобств, но и множество дополнительных угроз, число которых постоянно увеличивается. Пожалуй, среди вас почти нет людей, кто не имеет аккаунта в социальных сетях и мессенджерах. Социальные сети позволяют нам многое: читать новости, общаться с друзьями, делиться событиями из своей жизни, находить сообщества по интересам или создавать их самостоятельно. Мы чаще всего не задумываемся о безопасности, пока что-то не случится с нами или нашими друзьями. Давайте представим возможные проблемы заранее, чтобы избежать их в будущем.



Задание 7.1

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.

Возможен другой вариант развития событий. 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: якобы через неделю вернете всю сумму. Кто отправил эти сообщения? Вы это были или не вы? Что случилось? Ответ тот же: вас взломали.

Вы можете возразить, сказав: «Да кому нужно меня взламывать? Я не известный человек, да и денег у меня нет». Но у злоумышленников могут быть другие мотивы. Например, вы – администратор сообщества в социальной сети, и буквально за пару минут после взлома вашего аккаунта вы можете лишиться возможности управлять своей группой. 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. В следующий раз вы можете получить сообщение со ссылкой на видео с вашим участием или предложение стать участником какого-нибудь проекта. Помните, что вариантов заманить беспечного пользователя соцсетей очень много. Результат один: вас обманывают, получая от вас деньги или информацию. Вы и не заметите, как продиктуете мошеннику номер вашей банковской карты или щелкните по ссылке, через которую в ваш компьютер проникнет вирус-тロян.



Это интересно!

По прогнозам Cybercrime Magazine, в 2021 году компании по всему миру продолжат укреплять свою кибербезопасность. В 2022 году бюджеты на защиту данных достигнут 170 миллиардов долларов США. В 2021 году в сфере кибербезопасности будет работать 3,5 миллиона человек, а количество хакеров в 2022 году достигнет 6 миллионов человек. В 2030 году 90% населения мира будут пользоваться интернетом.

Кража личной информации

«Я никому не нужен», или «мне нечего скрывать» – это слабая и пассивная позиция. Чаще всего за ней прячутся интернет-пользователи, которые не могут или не хотят разбираться в вопросах безопасности. Чем плоха такая позиция?

У каждого человека есть информация, которая не предназначена для публичного пользования: переписка, фотографии, видео, личные записи. Беспечные же пользователи соцсетей хранят в своих фотоальбомах сканы личных документов (на всякий случай), записывают в заметки пароли к своим аккаунтам, отсылают друзьям фотографии, которые не стали бы выкладывать в социальные сети. Представьте, что кто-то получил доступ ко всему этому. Публикация фотографий и переписки может обернуться для вас репутационными потерями. Вы можете стать жертвой шантажа или вымогательства. Ваши средства с банковской карты могут исчезнуть, а удостоверение личности «всплынет» 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, переходя на личности (пишет о ваших особенностях, фигуре, имени, увлечениях). Он язвит вам 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, когда шутки переходят в травлю и преследование (буллинг), речь уже идет о преступлении против личности.

В тяжелых случаях в буллинге могут участвовать несколько человек. В этом случае жертве сложнее «спрятаться», она постоянно под ударом. В конечном счете, ей приходится удалять аккаунт или менять имя в социальной сети. Далее мы подробнее поговорим об угрозах в интернете и рассмотрим варианты их предотвращения и нейтрализации.



Задание 7.2

Обсудите, какие виды кибербуллинга вы наблюдаете в социальных сетях. Подумайте, как будете действовать в случае, если ваши друзья или вы сами подвергнетесь онлайн-травле, к кому обратитесь за помощью. Поделитесь своими идеями с учителем.

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. В любой стране такие действия вне закона, однако сама возможность регулярно привлекает злоумышленников и скучающих 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, ежесекундно отправляя множество вариантов. Один из них с большой вероятностью довольно быстро подойдет, если пользователь не озабочился созданием надежной комбинации символов.

Каждый год Британский Национальный центр кибербезопасности публикует списки самых популярных (а потому и совершенно бесполезных) паролей, известных взломщикам по всему миру. Так, в 2019 году лидерами рейтинга стали пароли «123456», «123456789» и «qwerty». Даже не думайте их использовать! Любой даже самый начинающий хакер взломает ваш аккаунт за секунды.

Топ-10 самых популярных паролей в 2019 году:

123456
123456789
qwerty
password
111111
12345678
abc123
1234567
password1
12345

Как создать пароль, устойчивый ко взлому

«Стойкость» паролей можно проверить при помощи нескольких онлайн-сервисов. Первый из таких – «How Secure Is My Password?». Однако будьте осторожны: мы не рекомендуем проверять в этом сервисе свой реальный пароль или использовать пароль, введенный в него ранее. Используйте пароли, похожие на те, которые вы ввели в поле на сайте сервиса.

Еще один вариант для проверки паролей – Strength Test (в поисковике можно найти по запросу «strength test rumkin»). Этот сервис подсчитывает степень энтропии, то есть предсказуемости появления какого-либо символа. Пароли с энтропией более 36 бит считаются достаточно защи-

щенными.

Вы также можете попробовать сервис для проверки паролей Password Check от Kaspersky.

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 (например !@#-\$%&). В некоторых сервисах в пароле можно использовать пробел – это еще более усложнит жизнь взломщикам.

Вы можете придумать пароль самостоятельно. В качестве основы используйте слово, которое вы запомните – допустим, dolphin (дельфин). В таком виде пароль будет мгновенно взломан. В нем всего семь символов, так что можно добавить к нему местоимение «ты»: my dolphin (мой дельфин). На взлом этого пароля уйдет неделя.

Теперь заменим некоторые буквы на цифры и спецсимволы (8yd#lph1n), добавим прописную букву (8yD#lph1n) и еще спецсимволы (8y!_D#lph1n). На взлом этого пароля уйдет 400 лет. Это хороший результат.

Пароль можно записать в блокнот и хранить дома в надежном месте. Советуем набрать его на клавиатуре несколько раз, чтобы запомнить. Разумеется, запомнить разные пароли к нескольким сервисам сложно, и ниже мы расскажем, как можно себе помочь.

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

Создание пароля с помощью списка слов

Метод Diceware предполагает создание пароля из нескольких случайно подобранных слов. Это исключает возможность угадывания продолжения пароля, если первое слово все же стало известно.

Представьте, что ваш пароль начинается на «Я помню чудное...». Что дальше? Мгновение? Это цитата из стихотворения Пушкина. А что последует после «Как приручить...»? Дракона, правда ведь? Люди 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, коду 11111 соответствует слово «абажур». Вам нужно бросить кубик пять раз, записать цифровые результаты бросков, а потом найти слово, соответствующее получившемуся коду. Например, за пять бросков кубика выпало 16231. Это слово «вече».

Для хорошего пароля рекомендуется пять слов, поэтому в общей сложности кубик необходимо бросить 25 раз. Запишите все коды и найдите слова. Представим, получились следующие слова: «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. К тому же он довольно длинный. Для его расшифровки потребуется 84 квинтиллиона (18 нулей после значения) лет! Из-за своей непредсказуемости он подойдет даже для защиты финансовой информации.

Запомнить такой пароль будет немного легче, чем пароль из классического варианта. Для этого слова «вече», «хлам», «озноб», «борщ», «железо» нужно связать в любую фразу. Скажем, «собрались на *вече*, убрали *хлам*, почувствовали *озноб*, съели *борщ* и пошли поднимать *железо*». Можно создавать и смешные варианты – главное, чтобы как минимум один хорошо запомнился.

Метод парольной фразы

Этот вариант удобен тем, что созданный пароль поддается запоминанию без особых усилий. Правда, есть риск сделать его предсказуемым, как описывалось выше, но попытаться стоит. Итак, выбираем короткую фразу, которую легко запомнить. Это может быть цитата из 3-4 слов – любимая фраза вашей бабушки или строка из учебника. Выбирайте тщательно, ведь эта фраза останется с вами надолго.

Например, берем фразу «Что наша жизнь? Игра!» из оперы «Пиковая дама». Набираем ее на латинице без пробелов: *Xnpyif;bryum&Buhf!*. Знак вопроса благодаря английской раскладке превратился в знак «&», а восклицательный знак остался. Надежность пароля – высокая, но он длинноват для дальнейшего использования. Поэтому

перефразируем: «Наша жизнь – игра!». Получилось Yfif;врут-buhf! Для расшифровки этого пароля потребуется 82 миллиарда лет. Хороший пароль, который легко запоминается.

Метод парольной фразы хорош еще и тем, что основной пароль (сложный, придуманный на основе фразы) можно использовать для всех сервисов, добавляя к нему те или иные символы. Например, мы набираем в английской раскладке «Наша жизнь – игра!» и добавляем в начале или в конце фразы символы, связанные с конкретным сервисом: DR – это «ВК» в английской раскладке, vskj – «мыло» для пароля от электронной почты, ajnrb – «фотки» для пароля от аккаунта в Инстаграм. Надежность каждого из паролей при этом очень высока.

Советы по использованию паролей

- Не используйте пароли на основе последовательностей на клавиатуре (например, QWERTYUIOP или 1QAZ2WSX). Они небезопасны.
- Не используйте дату вашего рождения, кличку домашнего животного, свои увлечения, имена родных или друзей при составлении паролей. Хакеры часто пользуются «социальной инженерией»: узнают все о человеке, которого пытаются взломать, а затем все собранные данные служат основой для подбора пароля.
- Не используйте имена популярных артистов и спортсменов, названия брендов и фильмов.
- Не храните 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 же можете получить код для подтверждения входа разными способами: посредством SMS на ваш номер телефона, с помощью специ-

ального приложения, воспользоваться списком резервных кодов и др.

На момент написания этого учебника двухфакторную аутентификацию поддерживали социальные сети «ВКонтакте», Instagram, Facebook, «Одноклассники», мессенджеры Telegram и WhatsApp (6-значный pin-код при входе со смартфона), почтовые сервисы Gmail, Mail.ru и Yandex. Вы можете проверить, поддерживает ли сервис дополнительный уровень безопасности, поискав ответ в справке сервиса или воспользовавшись поисковиком.

Самый простой способ защититься – включить подтверждение входа с помощью кода из SMS-сообщения. Как правило, эту опцию можно включить в настройках безопасности сервиса.

Например, если зайти во «ВКонтакте» и в правом верхнем углу экрана кликнуть на собственное фото, у вас появится возможность зайти в настройки. Далее выбираем из меню справа раздел «Безопасность». Самый первый пункт – «Подтверждение входа» (рисунок 7.1). Если уже здесь вы всего лишь укажите свой номер телефона, вы защитите свой аккаунт почти на 100%.

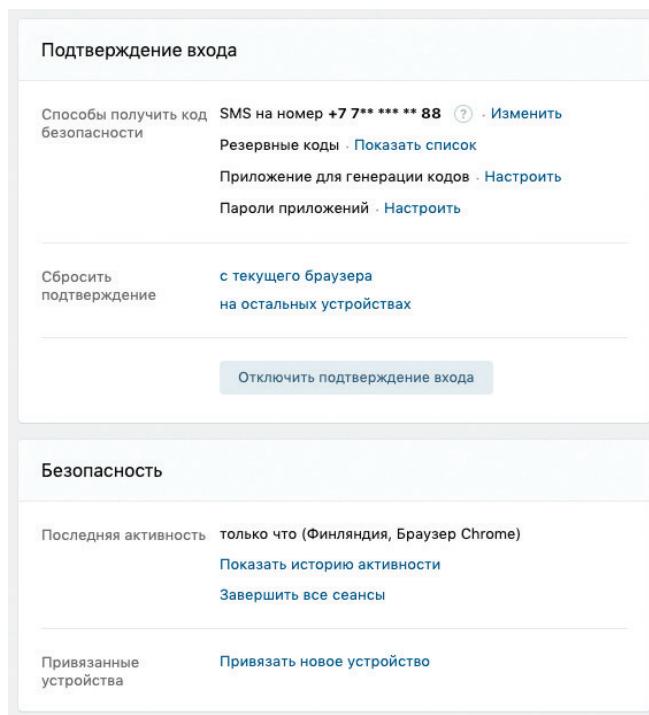


Рисунок 7.1. Настройки безопасности «ВКонтакте»

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.

Приложения для генерации кодов позволяют получать коды даже без подключения к сети и сотовой связи. Одним из таких приложений, например, является Google Authenticator (рисунок 7.2). Он работает и в рамках iOS, и для Android. Для работы с приложением нажмите «Настроить» рядом с нужной опцией в меню социальной сети.

Подтверждение входа на сегодняшний день является самым доступным и надежным способом защиты аккаунта. Взломы аккаунтов стали бы крайне редким явлением, если бы интернет-пользователи включали 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?». При этом пользователи представляют себе этот трудоемкий процесс: ввод пароля, потом ожидание кода по SMS...

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 – код для подтверждения понадобится вам только в самый первый раз.



Рисунок 7.2. Скриншот приложения Google Authenticator

Потом вы на какое-то время вообще забудете о кодах и паролях (надеемся, не навсегда). Ваш аккаунт будет надежно защищен, и если какой-нибудь взломщик подберет пароль к вашему аккаунту (а такого не должно произойти, если следовать описанным выше правилам создания надежных паролей), он столкнется с проблемой: ему потребуется код, единственным обладателем которого будете вы. Попытка взлома будет тщетной, а вы – спокойны.

Опасности входа в аккаунт на чужом компьютере

Завершим разговор о безопасности личных аккаунтов важным дополнением. Иногда нам приходится открывать свой профиль или электронную почту на компьютере в библиотеке или интернет-кафе. Школьники и учителя регулярно делают это в школе – в компьютерном классе например. Давайте рассмотрим эту ситуацию с точки зрения безопасности.

Что плохого может произойти? Вы вошли в соцсеть или почту, сделали все запланированное, закрыли вкладку/браузер и, возможно, даже выключили компьютер. При этом ваше имя и пароль для входа с большой долей вероятности сохранились в браузере, и следующий пользователь этого компьютера сможет без всяких усилий открыть ваш аккаунт, заглянуть в переписку, изучить всю доступную личную информацию. Хотели бы вы этого? Наверняка, нет. Давайте разберемся, как защититься.

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

Сохранение паролей в современных браузерах настроено автоматически для удобства пользователей. Правда, для компьютера в общественном месте эта функция едва ли является удобством, ее стоит отключать. Но что делать, если она включена? Быть внимательным. При вводе пароля браузер вас спросит, сохранить ли его для дальнейшего использования. Твердо жмите «Нет». Это и есть способ нейтрализации первой угрозы.

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 нашего последнего 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 «Выход». Но даже в этом

случае ваш аккаунт появится на странице входа в сервис, ожидая ввода пароля. Такие вот они прилипчивые – эти cookie.

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

Стараться не входить в свои аккаунты на чужих компьютерах. Вы можете переслать сообщение, сохранить файл в облачном сервисе, создать совместный документ, то есть использовать любой из многочисленных способов сделать информацию доступной всем, не открывая свой аккаунт.

Но если вам все-таки нужно открыть свой аккаунт на чужом компьютере, следуйте этой инструкции:

1. Переведите браузер в приватный режим (Firefox, Opera) или режим инкогнито (Chrome). В этом режиме не сохраняются 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 «Выход».
4. Закройте браузер.

Для надежности можно сразу после работы на чужом компьютере сменить пароль. В данном случае советуем оценить все риски (насколько вы доверяете тому месту, где пользовались компьютером?) и учесть собственный уровень тревожности.

Если все вышеперечисленное кажется вам 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 тоже сделает ваш вход в свой аккаунт на чужом компьютере безопаснее.

Итоги:

Воспользуйтесь способами, изложенными в этой главе, и создайте различные пароли. Проверьте надежность паролей при помощи онлайн-сервисов «How Secure Is My Password?», Strength Test и Password Check. Обсудите, как сервисы оценили ваши пароли.



* Объединитесь в группы по три-четыре человека. Каждая из групп должна выбрать себе одну из социальных сетей / один из мессенджеров / один из почтовых сервисов. Согласуйте свой выбор с другими командами во избежание повторов.

Примерив на себя роль блогера, в формате видеоролика подготовьте по выбранной соцсети / мессенджеру / почтовому сервису обучающий материал для лиц, не обладающих специальными знаниями и навыками по обеспечению своей безопасности на этих популярных в Казахстане платформах.

Обсудите критерии ролика заранее (объем, продолжительность, ясность, понятность и др.) и представьте свой проект.

8

ГЛАВА

КОНФИДЕНЦИАЛЬНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ



КЛЮЧЕВЫЕ СЛОВА:

спам
мошенничество
компьютерный вирус
кибербуллинг



Вы узнаете:

- к каким негативным последствиям могут привести ваши рутинные действия в интернете,
- какую личную информацию необходимо защищать от злоумышленников,
- как распознать сетевые риски и угрозы.

Вы научитесь:

- ограничивать рекламный спам,
- защищать свои персональные данные и гаджеты,
- противостоять онлайн-травле.

Источники проблем

Никому из нас не хотелось бы рассказывать публично о своих секретах. Каждый гражданин имеет право на тайну переписки. Любой человек будет против использования своих фотографий и текстов без разрешения. Эти постулаты давно перекочевали в цифровой мир, однако там – в Сети – за нами все равно постоянно следят: как легально, так и нелегально.

Мы ежедневно тратим несколько часов на интернет и социальные сети. Мы оставляем там свой «цифровой след»: открываем сайты и заходим в приложения, листаем фотографии, смотрим видео, ставим лайки, пишем комментарии, публикуем тексты и фотографии. Все это говорит 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.

В таблице 8.1 рассмотрим подробнее, кто способен доставить нам проблемы в интернете.

Источник проблем	Цель	Способы достижения цели
Рекламодатели	Деньги	Рекламные сообщения, предложения товаров и услуг, акции
Цифровые преступники		
Мошенничество	Деньги, материальные ценности, аккаунты	Рекламные сообщения, предложения товаров и услуг, акции, выгодные предложения
Компьютерные вирусы	ПК, смартфон, аккаунты	Отправка вредоносных файлов, ссылок на сайты
Вовлечение в противоправную деятельность	Личность, психика	Сообщения, чаты, закрытые сообщества
Кибербуллинг	Личность, психика	Сообщения, чаты, комментарии в аккаунте жертвы, закрытые сообщества
Грабеж	Деньги, материальные ценности	Мониторинг публикаций в аккаунтах (ценности в доме, отъезд), геометки

Таблица 8.1. Основные риски для интернет-пользователей

Чтобы уберечь граждан, правоохранительные органы – в зависимости от законодательства страны – проводят мониторинг социальных сетей для предотвращения распространения экстремистских и противозаконных материалов. Помните, что любая положительная реакция на подобные материалы (комментарий, лайк, репост и т.п.) может повлечь ответственность того, кто ее проявил, даже если и не знал, что это противозаконно.

Рекламодатели

Мы видим рекламу повсюду – во всех каналах коммуникации. Ее цель – продать аудитории товар или услугу. Реклама нацелена на деньги пользователей. Она 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 этой логике, можно понять, почему так много рекламы на сайтах с бесплатным доступом и ощутить разницу при внесении 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 нас «иммунитет» против рекламы. Современный человек развил в себе так называемую «баннерную слепоту» – способность не замечать рекламу на сайтах.

При этом постепенно реклама становится все 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. Разумеется, если его получится найти.

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

1. Ограничьте возможность незнакомых людей отправлять вам сообщения в социальных сетях и мессенджерах (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). Как правило, достаточно оставить лишь право комментировать.
3. Удаляйте сообщения рекламного характера, на которые вы не давали согласия. Помечайте их как спам, жалуйтесь на них в службу поддержки, блокируйте отправителей.
4. Страйтесь 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 найдите в письме ссылку «Отписаться от рассылки» и отпишитесь.
7. Смело отмечайте как спам сообщения в почте, социальных сетях и мессенджерах. Современные сервисы используют машинное обучение и мощные фильтры спама, так что этим вы поможете не только себе, но и другим.

Мы рассмотрели самые простые рекомендации, однако современные рекламодатели идут дальше и анализируют огромные объемы информации о нас – рядовых пользователях интернета.

Нужно 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. Что они еще могут знать? Вашу историю просмотра сайтов, количество открытых страниц, время на сайте и глубину просмотра каждой страницы. Это неполный перечень возможностей современных систем интернет-аналитики. На основе анализа сервис аналитики определяет ваш возраст и пол, может найти ваши аккаунты в социальных сетях, а затем – электронную почту и телефон, если вы их опубликовали.

Понимание того, что в интернете фиксируются все наши шаги, должно сделать вас осторожнее и внимательнее. В таблице 8.2 описано, к чему приводят самые обычные, на первый взгляд, действия.

Действие	Результат	Способ защиты
Запрос в поисковой системе (Яндекс, Google)	Появление баннерной и контекстной рекламы на тему запроса	Используйте поисковую систему, которая не отслеживает запросы пользователей (DuckDuckGo)
Открытие рекламного сайта	Появление баннерной рекламы на тему сайта, рекламных постов в соцсетях и даже личных сообщений	Используйте в браузерах приватный режим (Firefox, Opera) или режим инкогнито (Chrome). Установите специальное расширение для браузера (AdBlock, uBlock, Privacy Badger или любое другое)
Предоставление адреса электронной почты или (что хуже) номера телефона (для регистрации на сайте, получения бесплатного контента)	Получение спама по электронной почте, в личных сообщениях, рекламных SMS и звонков	Нигде не указывайте основной адрес электронной почты и номер телефона

Таблица 8.2. Поведение интернет-пользователей и обусловленные им риски

Как обезопасить себя от цифровых преступников

Давайте подробнее рассмотрим основные группы цифровых преступников. Одним из них нужны наши деньги, другие стремятся задеть нас эмоционально. Все они опасны, и стоит научиться противостоять им.

Мошенничество

«Вы получили перевод», «Вы выиграли в лотерею», «Мой дядя оставил вам завещание», «Последний день распродажи со скидкой 99%» – эти и многие другие похожие сообщения интернет-пользователи получают ежедневно. Почта, социальные сети, сайты, SMS – мошенники могут использовать любые доступные им каналы коммуникаций, чтобы заманить в свои сети наивных пользователей.

Что характерно для мошеннических схем?

- Обещание быстрой и легкой выгоды (получения товара, денег, услуги).
- Ограничение во времени (нужно действовать как можно скорее, чтобы у потенциальной жертвы не было возможности обдумать все «за» и «против»).

- Ограничение предложения («остался последний товар, последний день»).

Сообщения мошенников похожи на агрессивную рекламу. Они могут быть яркими, «кричащими», вызывающими эмоции и побуждающими к действию. При этом, как правило, все заканчивается 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. Все сделано красиво и «по-настоящему», чтобы покупатели поверили.

В Казахстане к такой тактике во время пандемии COVID-19 и объявленного карантина не раз прибегали мошенники, пытаясь продать гражданам сомнительные лекарственные препараты. На соответствующем сайте после долгого описания чудесного средства интернет-пользователям предлагали ввести личные данные для якобы бесплатного (!) получения препарата. Впоследствии оказывалось, что акция по безвозмездной раздаче закончилась, и гражданину все же придется заплатить.

Будьте осторожны! Не следует переводить деньги до получения товара или услуги, всегда интересуйтесь возможностью сделать оплату после получения. Вносить предоплату советуем исключительно на проверенных сайтах и приложениях. Некоторые сайты (Aliexpress, Ebay) практикуют так называемую «защиту покупателя»: если вы не получили товар или у вас есть претензии к нему, вы имеете право вернуть свои деньги.

Некоторые мошенники специализируются на махинациях с банковскими картами или переводами. Например, если у вас уже есть банковская карта, вы можете получить ложное SMS-сообщение о переводе или зачислении средств на нее. После этого мошенник свяжется с вами и предложит решить «проблему». Он попросит у вас сообщить номер карты и CVV-код, который находится на ее обороте рядом с подписью (рисунок 8.1). После предоставления необходимых данных вы лишитесь всех денег. В таких случаях стоит помнить о том, что никто – даже работники банка – не могут спрашивать ваш CVV-код, а проблемы с ошибочными переводами можно решить в отделении банка, но никак не с вашим участием.

Отдельно стоит выделить мошенников, отправляющих ложные письма от различных сервисов или банков (фишинг). Эти письма вызывают доверие: в них есть логотип компании, фирменные цвета, обращение к вам по имени. Поверив содержанию письма, вы можете ввести на открывшемся сайте логин и пароль, навсегда потеряв доступ к аккаунту. А если мошенник создаст убедительную копию сайта вашего банка? Вы рискуете навсегда лишиться и всех своих денег, поверив ему.



Рисунок 8.1. CVV-код (ист. — helcim.com)

Как защититься от мошенников?

1. Ограничивайте поток рекламы в свой адрес, так как мошенники используют те же уловки. Удаляйте сообщения мошенников, помечайте их как спам, жалуйтесь на них в службу поддержки, блокируйте отправителей.
2. Критически относитесь ко всем неожиданным и выгодным предложениям. Не действуйте сгоряча, подумайте о последствиях, спросите совета у близких, поищите информацию о продавце/сайте/сервисе в интернете.
3. При получении письма обращайте внимание на отправителя. Реальные компании указывают полное имя, а адрес электронной почты содержит название предприятия. Едва ли уважаемый банк или известный магазин будет делать рассылку с cimba.pimba@yahoo.com.
4. Не указывайте нигде в интернете и не пересылайте никому по почте и в SMS номер карты, имя владельца, дату окончания действия и CVV-код. Это относится и к вам, и к банковским картам ваших родителей. Помните, что платить онлайн следует только со старшими!
5. Для платежей через интернет откройте виртуальную карту (такую возможность сегодня предлагают многие банки). Перечисляйте на нее средства только перед переводом.
6. Не покупайте ничего в интернете со 100%-й предоплатой. Ищите варианты с оплатой при получении. Если вы все-таки платите заранее, убедитесь в надежности сайта.

7. Не верьте объявлениям в социальных сетях. Настаивайте на личной встрече, ничего не высыпайте и не переводите первым. Лучше потерять время или переплатить в обычном магазине, чем потерять все.

Компьютерные вирусы

Целью злоумышленников, распространяющих компьютерные вирусы, как правило, являются личные данные пользователей (файлы компьютера; информация, отправленная в интернет: например, пароли и данные карт), получение доступа к аккаунтам в социальных сетях и на сайтах, вымогательство денег после блокировки компьютера,ключение компьютера в сеть для атак на сайты (ботнет) и др. Иногда вирусы распространяют и ради развлечения.

Как защититься от вирусов?

1. Установите на компьютер антивирус. Множество достаточно качественных вариантов доступны бесплатно (например Avast).
2. Настройте «Зашитник Windows», если вы пользуетесь этой операционной системой. Отметим, что операционные системы Macintosh и Linux менее подвержены воздействию вирусов.
3. Не открывайте ссылки в письмах, сообщениях и SMS без проверки – не важно, получили вы их от незнакомых людей или друзей. Сообщения при этом могут быть очень привлекательные, обещать что-то интересное или важное. Однако кликкая по ненадежной ссылке, вы рискуете попасть на сайт с вредоносным кодом, который «заразит» ваш компьютер или смартфон. Другой вариант: вы получаете ссылку и сообщение от друга: «Привет! Смотри, какое о тебе сняли видео!». Как только вы перейдете по ссылке, вирус поразит ваш компьютер или аккаунт (от вас сотнями будут уходить вирусные сообщения). Ссылки на наличие вируса можно проверить в разных сервисах: например в бесплатном онлайн-сканере Dr.Web.
4. По той же причине не скачивайте и не открывайте файлы из писем и сообщений (особенно от незнакомых отправителей). Открыв фотографию, документ в формате Word или видео изложения, вы можете активировать вирус.

Вовлечение в противоправную деятельность

Не всех злоумышленников интересуют деньги и материальные ценности. Некоторые нацелены на вашу личность, желают управлять вами. Спустя время жертвы жалеют о том, что отправились на встречу с вербовщиками, занялись экстремистской деятельностью. Иногда, к сожалению, главной целью преступников может быть и доведение до самоубийства. Как избежать печальных последствий?

1. Максимально защитите себя от внимания незнакомых людей. В социальных сетях не добавляйте в друзья тех, кого вы плохо знаете. Если вы получили запрос от человека старше вас, прежде чем его принять лучше спросить совета у взрослых. Составьте обобщенный портрет тех, кого будете добавлять в список друзей. Например, это могут быть люди, которых вы знаете лично, либо те, чьи публикации вам интересно и полезно читать, известные люди или те, кто разделяет ваши взгляды и интересы. Добавляйте в друзья только таких людей.
2. Проверяйте аккаунты людей, которые написали вам сообщение, остались комментарий, поставили лайк или пытаются попасть в число друзей. Это могут быть фейковые аккаунты. Как определить подлинность?
 - Проверьте фото на аватаре. Подозрительным будет отсутствие на нем портрета человека или чужое изображение.
 - Если возможно, посмотрите список друзей. Если у вас есть общие друзья, вы можете спросить у них об этом человеке.
 - Посмотрите, о чем и как часто пишет человек. Отсутствие постов или большое количество репостов дают основания для подозрений.
 - Обратите внимание на активность друзей пользователя на его странице. Если активности нет или она очень слабая – это тоже плохой знак. Однако имейте в виду, что фейк может «дружить» с другими фейками, поэтому друзей фейка тоже стоит проверить.
 - Проверьте раздел «Личная информация» на наличие данных. Их отсутствие должно насторожить.
 - Один из способов разоблачения – прямые вопросы. Но стоит понимать, что общение со злоумышленником, который наверняка обладает навыками убеждения, может закончиться не в вашу

пользу. Мы не рекомендуем общаться с незнакомцами в интернете даже для того, чтобы «вывести их на чистую воду».

- Не добавляйте в друзья людей с закрытыми аккаунтами в социальных сетях.

Тематические сообщества в социальных сетях и чаты в мессенджерах тоже могут представлять опасность. Современный интернет дал нам возможность находить единомышленников. Чем бы мы не интересовались, мы всегда найдем в сети тех, кто поддержит наш интерес, с кем можно обсудить самые разные темы. В этом случае от общения в интернете мы получаем пользу и удовольствие. Однако нужно проявить особую бдительность, если разговор в сообществе или в чате вдруг начнет уходить 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 на отвлеченные темы. Следует помнить, что любые беседы о вашей личной жизни, семье, ваших ценностях и мотивах могут быть неспроста. Часто преступники мастерски владеют навыками, позволяющими разговорить и расположить к себе любого человека.

Всякий раз, общаясь с кем-то в интернете, вы должны себя спрашивать: а тот ли это человек, за которого себя выдает? Вы думаете, что это девушка или юноша, ваш сверстник, а на самом деле вашим собеседником может оказаться взрослый мужчина, который умело маскируется. Иногда – при появлении таких подозрений – возникает идея проверить человека, назначив ему встречу в реальности, но делать этого ни в коем случае нельзя. Это тоже может быть ловушка.

Что же делать? И верить нельзя, и встречаться ради проверки тоже нельзя? Да, из соображений безопасности. Как показывает опыт, и онлайн-общение «по душам» с незнакомцами, и встречи «чтобы проверить» могут привести к плохим последствиям. Главная защита – максимальное ограничение общения с незнакомыми людьми в интернете, особенно на интимные темы.

Тролли (кибербуллинг)

 **Буллинг** (от английского *bullying* – «запугивание», «издевательство», «травля») – это агрессивное преследование одного из членов коллектива (школьников или студентов) со стороны другого члена коллектива. Буллинг не всегда выражается в физической агрессии. Чаще речь идет о психологическом насилии в форме словесной травли (оскорблений, злые и непристойные шутки, насмешки), распространения слухов и сплетен, бойкота.

Важно сразу отметить, что травля во многих странах считается правонарушением. Таким образом, жертва буллинга может рассчитывать на помощь от родителей, учителей, полиции. Главное – не молчать о проблеме.

Травлю человека в интернете называют «кибербуллингом». Таблица 8.3 объясняет, благодаря каким возможностям онлайн-травля может быть даже более опасной, чем нападки на человека в реальности.

Угроза	Как защититься
Круглосуточное вмешательство в личную жизнь. Агрессор может писать вам днем и ночью в социальных сетях или по SMS.	Заблокировать агрессора, помечать его комментарии и публикации как спам.
Неограниченность аудитории, быстрая распространение информации. Сообщения могут быстро распространяться в сети, их может увидеть большая аудитория.	Блокировать сообщения агрессора в сообществах, жаловаться на его сообщения в службу поддержки (пункт «Пожаловаться» у публикаций есть во всех социальных сетях). Публично признать факт травли в интернете. Написать о происходящем в своем аккаунте, чтобы получить поддержку от друзей.
Анонимность преследователя. Агрессор может действовать анонимно, создав фейковый аккаунт.	Заблокировать агрессора. Публично признать факт травли. Лишить агрессора анонимности (может помочь, но не так сильно, как кажется).
Возможность использования личной информации. У каждого пользователя социальных сетей в аккаунте содержится много личных данных, фотографий, видео и публикаций, которые могут стать объектами насмешек.	Заблокировать агрессора. Ограничить доступ к фотографиям, видео и стене для тех, кто не является вашим другом. Пожаловаться на агрессора, если оскорбляющие вас публикации появляются в его аккаунте. Сообщить администрацию или в службу поддержки, если травля происходит в сообществе.

Таблица 8.3. Характерные черты кибербуллинга и способы борьбы с ним

Грабители

Эта группа злоумышленников хоть и малозаметна, но тоже черпает информацию о потенциальных жертвах, 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 из жизни. Неудивительно, что человек, задумавший кражу, довольно быстро решится на нее, глядя на публикации в открытом доступе.

Особенно удобно будет организовать кражу после того, как вы публично сообщите о семейном отпуске. И пока вы будете радоваться новым впечатлениям, злоумышленник будет подбирать ключ к вашему замку. До этого он уже прочитал все ваши посты об украшениях и бытовой технике и теперь только и ждет момента, чтобы завладеть ими. Как только вы напишите, что поехали на курорт и будете отсутствовать неделю, домашний отправится к вам.

Конечно, вы можете делиться радостью от поездки с друзьями, но публикаций об этом в социальных сетях стоит делать исключительно «для друзей». При этом нужно быть уверенным, что в списке друзей нет посторонних или случайных людей.

Не следует хвастаться в социальных сетях и мессенджерах дорогими приобретениями, украшениями и прочими предметами, способными привлечь внимание грабителей. Не стоит также публично сообщать о времени вашего отсутствия – особенно если ваш дом будет пустовать.

Что знают правоохранительные органы

Правоохранительные органы в каждой стране занимаются мониторингом социальных сетей и мессенджеров для предотвращения распространения экстремистских и противозаконных материалов. Такой контент может пропагандировать насилие и нетерпимость (в том числе по нациальному, религиозному признаку), призывать к насилию или свержению власти, пропагандировать наркотики или алкоголь.

Кажется, что любой воспитанный и законопослушный гражданин и так не будет публиковать ничего подобного. Так в чем здесь угроза?

Дело в том, что интернет-пользователи зачастую недостаточно осведомлены о том, какие материалы являются противозаконными, или не понимают, какие действия могут быть опасными для них с точки зрения закона. В действительности список является довольно внушительным.

Нельзя публиковать и репостить любые материалы, которые...

- призывают к осуществлению экстремистской деятельности,
- оправдывают необходимость экстремистской деятельности,
- обосновывают или оправдывают национальное и (или) расовое превосходство,
- оправдывают практику совершения военных или иных преступлений,
- призывают к насилию по отношению к этнической, социальной, расовой, национальной или религиозной группы,
- пропагандируют наркотические и психотропные вещества,
- пропагандируют суицид и провоцируют его совершение,
- содержат признаки порнографического характера,
- содержат нецензурные слова и выражения,
- содержат любую информацию противоправного характера.

И это далеко не исчерпывающий перечень. Не забываем, что все наши действия в интернете фиксируются. Это не анонимная среда. В онлайн-пространстве не получится избежать следования законам.

Обратите внимание, что с точки зрения действующего законодательства публикация и репост – одинаковые по значимости действия. Да, может быть, изначально не вы явились автором поста, но вы его распространяете, а значит, в той же степени виновны.

**Это интересно!**

Не всегда суды и полиция учитывают, с каким комментарием вы сделали репост той или иной публикации. Иногда к ответственности привлекают и тех, кто выступает против незаконной деятельности. Представим, вы хотели осудить насилие или распространителей наркотиков и поэтому сделали репост чьей-то записи. Ваш праведный гнев понятен, но вы фактически распространили противозаконные идеи. Вопреки вашему замыслу кто-то, напротив, может воспринять их.

Будьте осторожны, не делайте репостов! Не помогайте злу распространяться. Можно написать о возмутительном явлении собственный пост, упомянув о том, что вы прочли ранее.

Не стоит комментировать публикации с противозаконным содержанием и уж тем более ставить им «лайк». Это может быть расценено как поддержка описанных идей. Кроме этого, комментарии и «лайки» повышают рейтинг поста. Это, в свою очередь, приведет к тому, что пост с незаконным содержанием увидит еще больше людей.

Не вступайте в сообщества и чаты, где делают противозаконные или сомнительные с точки зрения закона публикации. Обращайте внимание на название сообщества, его «шапку», описание, просмотрите посты за последние две недели. Иногда безобидное, на первый взгляд, сообщество раз в неделю выкладывает публикации экстремистского содержания. Выходите и отписывайтесь от таких групп сразу же, как увидели подобный пост. Можно также отправить жалобу в службу поддержки.

Отписывайтесь от друзей в социальных сетях, которые публикуют противозаконный контент. Если ваш друг внезапно начал это делать, постарайтесь выяснить причину. Возможно, его аккаунт взломан, или он связался с плохой компанией.

Как сохранить личное пространство в соцсетях

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

Теперь пришло время вам проанализировать собственные аккаунты на наличие слабых мест. Проведем эксперимент на примере социальной сети «ВКонтакте» (или любой другой), которой пользуются большинство ваших одноклассников. Посмотрим на ваши аккаунты с трех перспектив: глазами вашего друга в соцсетях, незнакомого вам пользователя соцсети и совсем постороннего.



Задание 8.1

Для первой части эксперимента вам потребуется смартфон вашего друга, который подписан на вас в соцсети. Попросите друга открыть ваш аккаунт на своем телефоне и вместе проанализируйте увиденное по списку ниже. Отметьте то, что сможете увидеть. Ставьте по одному баллу за каждый пункт.

1. Фотографии профиля.
2. Телефон, электронная 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, 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» доверить информацию из списка выше?



Задание 8.2

Для второй части эксперимента найдите человека, которого вы не добавляли в друзья в социальной сети. Попросите его открыть ваш аккаунт на своем телефоне и вновь вместе проанализируйте увиденное по списку из задания 8.1. Отметьте то, что сможете увидеть. Ставьте по одному баллу за каждый пункт.

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

К особенно чувствительной информации относятся контакты (телефон, электронная почта), отметки на карте и фотографии, на которых вы отмечены. Эти данные не должны быть доступны тем, кто не является вашим другом в соцсети. Почему? Ваши открытые контакты могут внести в базу для спам-рассылки, рекламных звонков или SMS. Отметки на карте – это подробный рассказ о вашей жизни, работе, отдыхе. Зачем делиться этим с незнакомцами? Фотографии, на которых вы отмечены, часто не подконтрольны вам. Вы можете следить за своими фотоальбомами, но ваши друзья могут опубликовать фото с вечеринки, которые

вы не хотели бы показывать незнакомым людям. Представьте, что ваш аккаунт просматривает ваш будущий работодатель (такая практика уже существует). Это тот самый «взгляд пользователя соцсети». Что вы хотели бы, чтобы он увидел?

В настройках «ВКонтакте» предусмотрена возможность увидеть свой аккаунт таким, каким его видят другие пользователи сети. Откройте раздел «Приватность» в настройках и найдите ссылку в нижней части страницы. Есть и другой способ посмотреть на свой аккаунт глазами незнакомого вам пользователя: откройте свой профиль и допишите в адресной строке в конце адреса «?as=-1» (должно получиться вот так: https://vk.com/id***?as=-1).



Задание 8.3

Для третьей части эксперимента вам нужно временно выйти из своего аккаунта и открыть его в отдельной вкладке, не вводя имя и пароль. Таким образом вы сможете оценить свой аккаунт по списку из задания 8.1 с точки зрения тех, кто не зарегистрирован в социальной сети. Отметьте то, что сможете увидеть. Ставьте по одному баллу за каждый пункт.

В третьей части эксперимента («взгляд со стороны») лучшим результатом следует считать 0–3 балла. Всем, кто не зарегистрирован в соцсети, должны – максимум – быть доступны только ваше имя и фотография профиля.

Сегодня во многих соцсетях есть возможность закрывать профиль от всех, кроме друзей. На наш взгляд, с точки зрения безопасности такой вариант является наиболее приемлемым для пользователей до 18 лет. Если же вы оставляете профиль открытым, внимательно проверьте настройки доступа к информации в вашем профиле. Эти настройки доступны в каждой социальной сети.



Итоги:

В таблице 8.4 собрана информация о настройках приватности в четырех популярных социальных сетях. Внимательно рассмотрите возможности каждой сети. Определите, насколько защищены ваши профили в указанных соцсетях. Включите настройки приватности в своих аккаунтах.

	Instagram	VK	OK	Facebook
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 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	-	+	-	+

Таблица 8.4. Настройки приватности социальных сетей*

*Данные приводятся на август 2020 года. Версии настроек могут отличаться в зависимости от времени и региона. Социальная сеть может изменить настройки, убрать или добавить новые.

**Платная возможность

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



Используя знания и навыки, полученные при изучении Главы 6 («Медиа и реклама»), подготовьте в любой форме – коммерческая / социальная реклама, агитация, политическая агитация, пропаганда, информирование, PR-кампания – обращение к жителям Казахстана, которое нацелено на информирование общества об одном из источников цифровых угроз (рекламодатели, мошенники, компьютерные вирусы, вовлечение в противоправную деятельность, кибербуллинг, грабители). Представьте работу в классе.

9

ГЛАВА

ПРОВЕРКА НА ДОСТОВЕРНОСТЬ ФОТО И ВИДЕО



КЛЮЧЕВЫЕ СЛОВА:

фотофейк
видеофейк
поиск
алгоритм



Вы узнаете:

- при помощи каких алгоритмов можно разоблачить фото- и видеофейки,
- кто производит фото- и видеофейки,
- почему дипфейки являются более серьезной угрозой в перспективе.

Вы научитесь:

- проверять подлинность фото- и видеоматериалов за считанные минуты,
- определять врезки на фото;
- работать с видеоинструкциями по использованию тех или иных сервисов.

Инструменты проверки фото

С ростом количества дезинформации и фейков, которые попадают в наше инфополе, к счастью, растет и число технических решений, которые помогают бороться с фейками. 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 обнаружить манипуляцию.



Задание 9.1

Рассмотрите фото ниже (рисунок 9.1). 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 его описания? Аргументируйте свою точку зрения:

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



Рисунок 9.1. Скриншот
(ист. – Facebook)

Кто производит фейки

Из-за обилия фото- и видеофейков может показаться, что они массово производятся с какой-то определенной целью группами людей или отдельными злоумышленниками. В действительности это не так, и большая их часть создается «на коленке» случайными пользователями, которые делают их от скуки или не предполагая широкого охвата. Скучающие где-нибудь в Алматы или под Карагандой Василий, Серик или Акбота видят фотографию, придумывают к ней забавную (по их мнению) подпись и выкладывают в своих аккаунтах в социальных сетях. Моментальная скорость распространения информации и невысокий уровень критического мышления в обществе способствуют тому, что

фейки легко расходятся в социальных сетях и даже попадают в новостные ленты. 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 внимание 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? Кроме этого, есть ряд инструментов, которые помогут вам проверить, где впервые появилось фото, и действительно ли на нем было изображено то, о чем сказано в описании.

Если вы пользуетесь браузером Google Chrome (а мы очень рекомендуем пользоваться именно им) или Firefox, то установите расширение RevEye (рисунок 9.2).

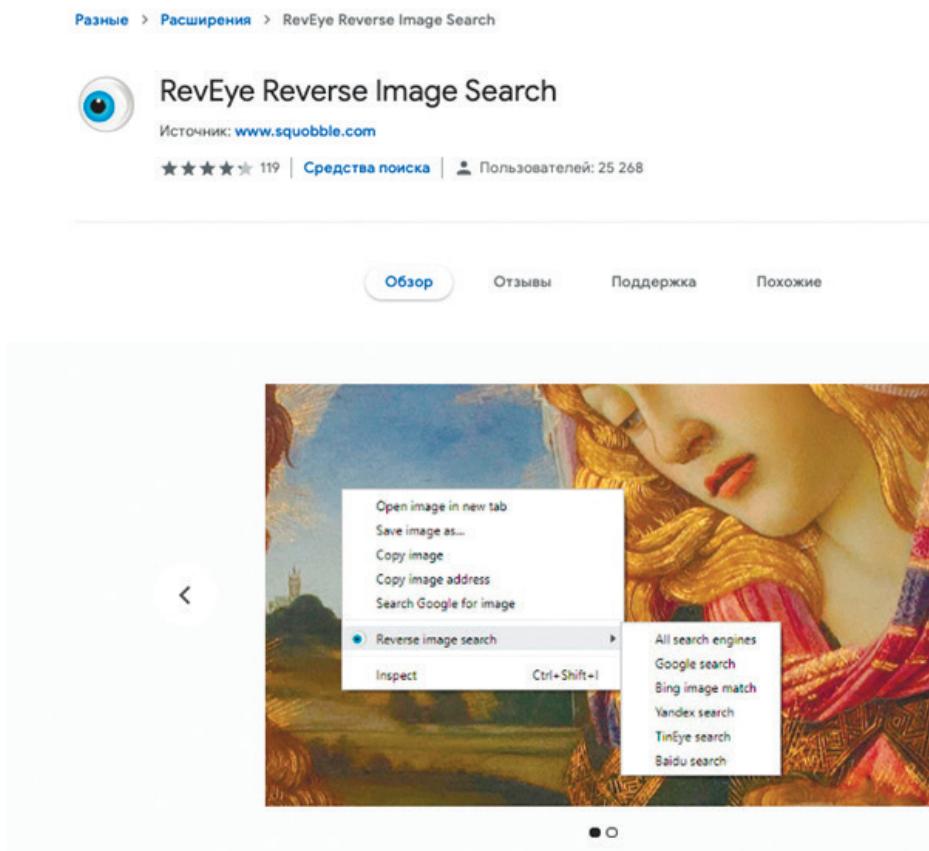


Рисунок 9.2. Скриншот (ист. — интернет-магазин Chrome)

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 перечисленные технологии поиска основаны на разработках Google. Самый простой способ проверить фото с вашего смартфона – сохранить картинку, а затем загрузить ее в Google Images. В этом специальном сервисе вы можете самостоятельно задать параметры поиска: искать ли самое большое точно совпадающее изображение или опубликованное в определенный период времени.

Возможности Яндекс.Картинки

Поиск Яндекса по картинкам (который, на первый взгляд, устроен совершенно аналогично сервису Google) может дать вам гораздо более точные результаты – особенно если вы ищете фото, на котором четко видны лица людей. Алгоритмы искусственного интеллекта поисковой системы Яндекс позволяют найти аккаунт незнакомого вам человека в соцсетях, даже если он случайно попал на фото (и беспечно относится к конфиденциальности своего аккаунта). Поэтому если поиск в одном поисковике не дал результатов, попробуйте другой. Иногда даже весьма непопулярный в Казахстане Bing может принести точные результаты.

- Перед тем как проверять изображение с помощью технических средств, внимательно его рассмотрите. Фейки чаще всего очень грубо смонтированы, и следы монтажа видны невооруженным глазом – могут отсутствовать тени, наклон деревьев может не соответствовать направлению ветра, части фотографии могут неестественным образом перекрывать друг друга, люди на фото могут быть одеты не по погоде и т.д. 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 все-таки начали поиск, помните: 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 и вы попробуйте отзеркалить его в графическом редакторе, а затем снова провести поиск.

- Для анализа фото на предмет использования Photoshop и монтажа можно использовать онлайн-сервис Forensically. Он покажет вам, как определить врезки на фото.

Как на жаре плавились автомобили

Летом 2019 года ряд интернет-ресурсов – в том числе казахстанских – сообщил, что «8 июня в Кувейте жара достигла +63 градусов по Цельсию, от чего начали плавиться машины». В качестве доказательств медиа сопровождали тексты соответствующими фотографиями (рисунок 9.3).

63 градуса по Цельсию! В Кувейте автомобили плавятся от аномальной жары

20 июня, 2019 Мир

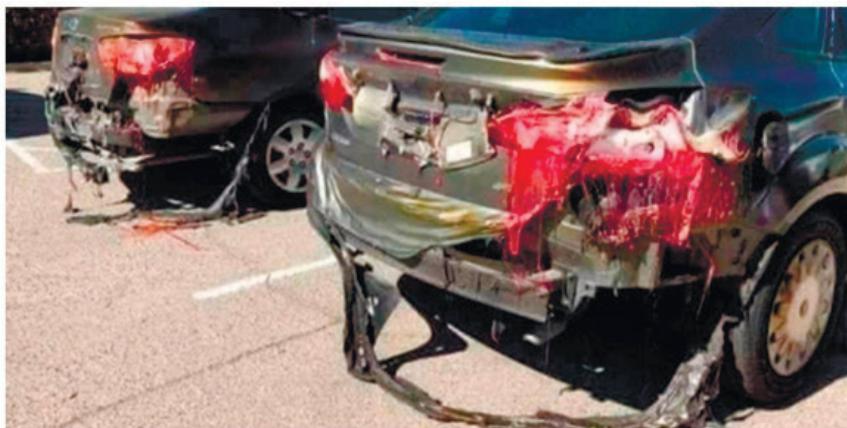


Foto: Culturacollectiva.com

Рисунок 9.3. Скриншот (ист. — Neonomad.kz)

Во-первых, внимательно рассмотрим изображенные автомобили. На картинке видно, что расплавились только задние фары и бамперы. Весьма сомнительно, что прочный пластик и стекло расплавились из-за температуры воздуха ниже, чем в бане или сауне.

Во-вторых, проверяем фото через Google Image Search (рисунок 9.4) и выясняем, что оно к жаре в Кувейте никакого отношения не имеет. Да, действительно, задняя фара машины расплавилась, но не от солнечного тепла, а от пожара, произошедшего вблизи автомобиля.

Google Image Search results for 'машины расплавились от жары' (cars melted from heat). The search bar shows 'ZhARA-750x375.png' and 'машины расплавились от жары'. Below the search bar are filters: 'Все' (All), 'Картинки' (Images), 'Карты' (Maps), and 'Ещё' (More). To the right are 'Настройки' (Settings) and 'Инструменты' (Tools). The results section shows two items:

- mysea — история — LiveJournal**
mysea.livejournal.com › category › история ▾
mysea — история — LiveJournal
1080 × 558 - ... ли в Кувейте 63 градуса (вроде в прошлом году был там рекорд +54), но фото сделано в Аризоне. И расплавились машины от пожара неподалеку.
A photo thumbnail shows melted car parts.
- joyreactor.cc › post ▾**
лето в Аризоне выдалось жарким / потекла :: автомобили ...
joyreactor.cc › post ▾
150 × 113 - 25 июн. 2018 г. - Крышка багажника ближней машины металлическая, но цвет покрытия изменился. Такой жары не может быть даже в Аризоне.
A photo thumbnail shows melted car parts.

Рисунок 9.4. Скриншот результатов обратного поиска фото (ист. — Google)

Событие на фото произошло 19 июня 2018 года в городе Тусон, США. По данным местных СМИ, из-за пожара в строящемся общежитии The Mark при Университете Аризоны некоторые детали машин, находившихся на стоянке, расплавились.



Задание 9.2

Найдите на платформе YouTube и посмотрите обучающие ролики по работе с Google Image Search, RevEye и Forensically. Обсудите инструменты с учителем.



Задание 9.3

Проанализируйте фотомонтаж Джими Хендрикса с аккордеоном (рисунок 9.5), сравните изображение с оригиналом (рисунок 9.6). Найдите признаки, указывающие на то, что фото с аккордеоном – фейковое. Проверьте его с помощью инструмента RevEye. Определите, из каких фотографий смонтирован этот фейк.



Рисунок 9.5. Фейковое фото известного гитариста Джими Хендрикса с аккордеоном (ист. — 1000.com)



Рисунок 9.6. Оригинальное фото гитариста Джими Хендрикса (ист. — 20minutos.es)

Проверка видео

Итак, вам прислали ссылку на видео, или вы увидели его в соцсетях. 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 ваших действий мы уже описали выше. Как и в случае с фото, вам нужно проверить, соответствует ли то, что происходит на видео, описанию к нему. Не пытаются ли с помощью подписи манипулировать вами (смотрите раздел «Логические уловки» в Главе 5)? Уже на этом этапе довольно часто можно с большой вероятностью определить, фейк перед вами или нет.

Проверка оригинальности

Подобное видео могли выложить в интернете ранее – возможно, в ином контексте или с другой 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 своих базах схожие изображения.

Но есть и более технологичный способ проверки – организация Amnesty International разработала инструмент под названием Youtube Data Viewer. Вам нужно вставить в него ссылку на ролик, он сгенерирует из него отдельные кадры (которые посчитает ключевыми) и найдет 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.

Если вам недостаточно поиска, завязанного на поисковик Google, или вам кажется долгим путь поиска, попробуйте протестировать другой инструмент под названием InVid. 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, получить из него ключевые кадры, по которым можно произвести детальный поиск.

Казахстанский кейс от Factcheck.kz

В разгар пандемии COVID-19 в Казахстане пользователи социальных сетей и мессенджеров распространяли конспирологическую теорию о том, что лучшим способом уничтожения казахстанцев является распы-

ление коронавируса с самолетов. В качестве подтверждения граждане пересыпали друг другу видео, на котором самолет сбрасывает на землю «неизвестное красное вещество» (рисунок 9.7). Авторы рассылки предполагали, что распыление происходит над Мангыштаяу.

Для проверки видео копируем ссылку на него и вставляем ее на странице сервиса Youtube Data Viewer, который генерирует нам несколько ключевых кадров из видео со ссылками на Google Image Search (рисунок 9.8).



Рисунок 9.7. Скриншот из вирусного видео (ист. — Instagram)

Youtube DataViewer

<https://www.youtube.com/watch?v=LIODfxl5ot0>

Самолёт распыляет неизвестную жидкость красного цвета, 2020

Video ID: LIODfxl5ot0
Upload Date (YYYY/MM/DD): 2020-07-10
Upload Time (UTC): 11:52:35 (convert to local time)

Thumbnails:



Рисунок 9.8. Скриншот результатов поиска (ист. — Youtube Data Viewer)

Переходим по ссылкам и среди похожих изображений находим многие другие, на которых запечатлены самолеты, распыляющие нечто красное (рисунок 9.9).

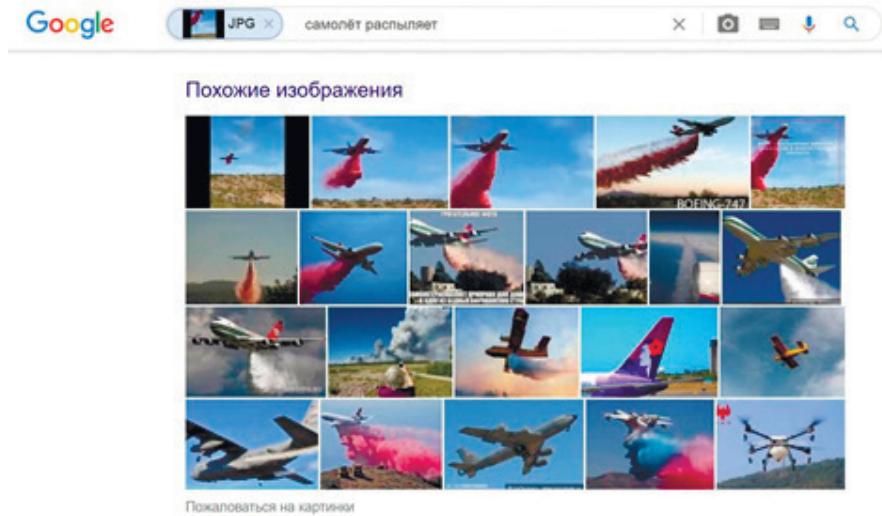


Рисунок 9.9. Скриншот результатов поиска (ист. — Google Images)

Кликая по фото, довольно быстро находим, например, ссылку на статью National Geographic Россия, посвященную тушению пожаров в Калифорнии в 2019 году. Проверяем, писали ли о стихии другие издания.

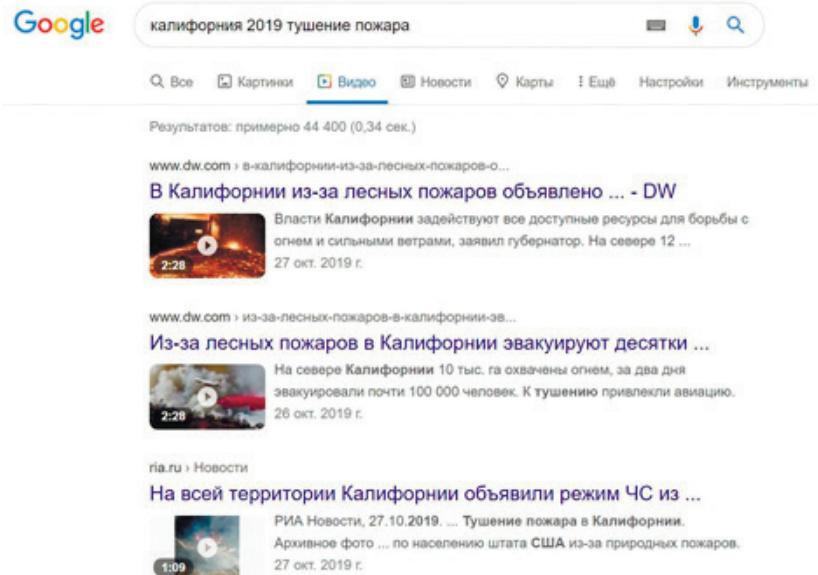


Рисунок 9.10. Скриншот результатов поиска (ист. — Google)

Поиск подтверждает, что в октябре 2019 года на всей территории американского штата Калифорния из-за сильных лесных пожаров было объявлено чрезвычайное положение (рисунок 9.10). По информации СМИ, власти США задействовали все доступные ресурсы для борьбы с огнем и беспрецедентными сильными ветрами – в том числе, воздушные танкеры DC-10, которые используются для тушения пожаров в США с 2006 года. У них характерная окраска, а в Казахстане таких танкеров попросту нет. Красный цвет связан с входящим в состав смеси для борьбы с огнем оксида железа – он помогает увидеть, какие участки уже были обработаны.

Если видео или фото – фейковое, вы с большой вероятностью найдете его оригинал 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.

Информационное оружие будущего

Фото- и видеофейки уже не кажутся специалистам главной проблемой XXI века – им на смену приходят так называемые дипфейки. Это видеоролики, созданные искусственным интеллектом на основе огромного количества изображений. Дипфейки искусно имитируют речь и движения человека, его мимику и эмоции. Распознать такое фальшивое видео без компьютерных алгоритмов чрезвычайно сложно.



Это интересно!

Экспертам удалось обнаружить у дипфейков ряд недостатков, заметных невооруженным глазом: люди на таких видео моргают либо крайне редко, либо неестественно (и двигают глаза в разные стороны), либо совсем не моргают. Помимо этого можно обнаружить подозрительную подвижность головы, необычный оттенок глаз или неестественные физиологические знаки.

Вполне вероятно, что уже совсем скоро нейросети, которыми пользуются создатели дипфейков, «научатся» заставлять людей на видео моргать естественнее, и тогда «разоблачителям» придется совсем нелегко.

Надо отметить, что противодействием дипфейкам озабочились уже практически все крупные технологические платформы: к примеру, Facebook проводит открытые конкурсы среди разработчиков, в поддержку им Google публикует базу данных с тысячами дипфейков. С другой стороны, ученые стремятся к созданию такой защиты для фото- и видеоматериалов, чтобы они не могли быть изменены с помощью дипфейк-технологий.

Правоохранительные органы тоже пристально следят за новой технологией, которая даже в самом безобидном виде может стать реальным поводом для уголовного преследования. Дипфейк-технология позволяет злоумышленникам «вставлять» изображение лица человека на фото или видео, которые порочат его честь и достоинство. Кроме этого, такими поддельными изображениями пользуются и мошенники – например, накладывают на видео лица и голоса известных людей, которые обещают пользователям призы за переход по ненадежной ссылке.

С другой стороны, следует отметить, что дипфейки несмотря на их плохую репутацию могут использоваться и во благо. Одна из крупнейших рекламных компаний в мире, например, применяет эту технологию в качестве инструмента для корпоративного обучения. В результате десятки тысяч сотрудников холдинга по всему миру получают персонализированные обучающие видеоролики, в которых к ним обращаются по имени и на родном языке. Другой пример: стриминговый сервис Hulu снял рекламный ролик с дублерами, а затем использовал дипфейк-технологии, чтобы наложить лица звезд в клип.

К слову, пандемия COVID-19 значительно подстегнула интерес рекламного бизнеса к использованию дипфейков для решения тех или иных задач. Спрос на услуги стартапа Synthesia, работающего с видео при помощи технологий искусственного интеллекта и обещающего клиентам возможность создавать ролики без актеров и съемочных групп, за неполный 2020 год вырос в 10 раз.



Это интересно!

Аудиоредактор Descript, применяющий технологии искусственного интеллекта для обработки записей, предлагает своим пользователям за отдельную плату синтезировать своего звукового двойника, чтобы при необходимости исправить в записанном подкасте оговорку или вставить пару слов. Технология по сути представляет собой звуковой дипфейк: вы подделываете собственный голос.

Итоги:

Объединитесь в группы по три-четыре человека. Найдите в сети и изучите инструкцию по использованию сервиса *YouTube Data Viewer*. С помощью этого инструмента найдите оригинал видеоролика, достоверно известного как фейк. Обсудите, насколько этичны действия создателей ролика.

С помощью любой компьютерной программы, позволяющей записывать видео с монитора, на примере выбранного видеоролика покажите неопытным пользователям алгоритм работы по определению оригинальности подобных материалов. Заранее согласуйте критерии видео.

ГЛАВА 10

«ТЕМНЫЕ» СОЦИАЛЬНЫЕ МЕДИА



КЛЮЧЕВЫЕ СЛОВА:

«темные медиа»
мессенджер
рассылка



Вы узнаете:

- что такое «темные» социальные сети,
- какое место занимают «темные медиа» в структуре современного интернет-трафика,
- как фактчекеры и компании борются с распространением фейков в мессенджерах.

Вы научитесь:

- проверять на достоверность видео-, аудио- и текстовые сообщения из мессенджеров,
- критически воспринимать получаемые в мессенджерах сообщения,
- анализировать свою активность в мессенджерах.

Что такое Dark Social

Понятие «темных» социальных медиа – сравнительно новое. Оно пришло в русский язык калькой с английского dark social, хотя первым таким каналом является переписка посредством обычной электронной почты.

Все, что мы делаем на своих страницах в соцсетях – публично или доступно более-менее ограниченному кругу лиц. Переписка же – дело частное, конфиденциальное. Получить к ней доступ могут только хакеры (как от них защититься, мы говорили во время изучения Главы 7) или правоохранительные органы по решению суда.



Сегодня под «темными медиа» мы, в первую очередь, подразумеваем именно переписку в мессенджерах. «Темными» каналами их называют из-за непрозрачности. Для удобства будем называть такие медиа «дарксошиал».

Почему Dark Social так важны

В последние три года дарксошиал обеспечивает от 60 до 90% интернет-трафика в мире. На Рисунке 10.1 представлены данные за 2016 год, свидетельствующие о том, что в 84% случаев люди предпочитают делиться ссылками, пересылая их друг другу в рамках мессенджеров.

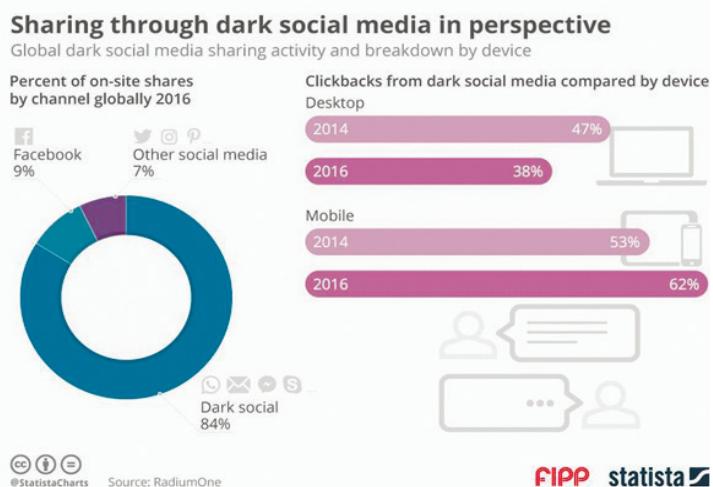


Рисунок 10.1. «Темные медиа» в глобальном интернет-трафике

И именно через мессенджеры распространяется огромное количество фейков, дезинформации и опасных манипуляций. Известны случаи жестокого самосуда в Индии и Мексике, произошедшие из-за массовых фейковых рассылок о похищении детей. Например, на одном из видео к группе детей, играющих на улице, подъехал скутер. Водитель забрал одного из детей. По данным правоохранительных органов, из ролика была вырезана концовка, где мотоциклист вернул ребенка обратно и поднял плакат с надписью «Нужно мгновение, чтобы похитить ребенка». В действительности это был пример социальной рекламы.

В Казахстане во время пандемии COVID-19 через мессенджер WhatsApp распространялось аудиосообщение от некой «женщины из Сарыагаша». Она, ссылаясь на «надежный» источник информации, рассказывала, что несколько дней назад в воздух был распылен вирус, отправляющий пожилых людей, а теперь распространяют вирус, отправляющий детей. Голос из аудиосообщения призывал немедленно «закрывать двери и окна, не отпускать детей на улицу».

Спустя некоторое время в сети появилось видеоизвинение, на котором подозреваемая женщина – жительница Отырарского района – признала, что сама получила аудиосообщение из какого-то чата и лишь перенаправила его в чаты коллектива и одноклассников. Обвиняемая утверждала, что не знала, что информация является ложной, и пообещала впредь не распространять такие данные.

Следует иметь в виду, что незнание закона не освобождает от ответственности. Так, распространители заведомо ложной информации привлекаются к ответственности по ст. 274 Уголовного Кодекса Республики Казахстан.

Дарксошиал – самый сложный материал для фактчекинга, ведь в данный момент легальных способов проверки источника распространения информации в мессенджерах не существует. Большинство создателей мессенджеров стоят перед дилеммой: «анонимность или прозрачность» – предоставлять ли ваши персональные данные третьей стороне (например спецслужбам) или максимально защитить их. Этой неопределенностью пользуются как журналисты-расследователи, так и злоумышленники.



Задание 10.1

Посчитайте, сколько сообщений вы получаете в WhatsApp в день/неделю. Подумайте, какое внимание вы уделяете каждому из них.

Определите, какие сообщения вы просто читаете, а какие – отправляете другим. Объясните, почему вы решаете переслать то или иное сообщение.



Это интересно!

Во время Единого национального тестирования в 2020 году среди пользователей мессенджеров распространялось видео, на котором ко лбам школьников якобы прикрепляют некие проверочные устройства. «Наших детей чипируют», – комментировали видео взволнованные казахстанцы. В действительности ролик не имел никакого отношения ни к ЕНТ-2020, ни к чипированию. Видео было снято в 2019 году, и на нем тестируют устройство, изобретенное профессором Назарбаев Университета. О том, что действие происходит не в 2020 году, говорит тот факт, что школьники спокойно сидят за партами по двое, а их лица не защищены масками.

Как проверять рассылки в мессенджерах

Тексты

Здесь вам в первую очередь пригодятся знания о формальной логике, почерпнутые из Главы 5. Рассылки в мессенджерах довольно часто используют манипуляции, описанные в упомянутой главе. Всякий раз, когда рассылка вызывает у вас гнев или другие яркие эмоции, задумайтесь: возможно, вас попросту хотят использовать для дальнейшего распространения недостоверной информации.

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

На что стоит обратить внимание в рассылке (алгоритм проверки)

- Оцените, насколько грамотно написано сообщение. Часто фейки пишутся «на коленке» со множеством ошибок и не перепроверяются после.
- Во многих мессенджерах сообщение, пересланное вам от третьего лица, помечается особым образом. Если вам пришло сомнительное сообщение от близкого человека, проверьте, он ли на самом деле его написал.
- Никогда не открывайте ссылки на незнакомые ресурсы. Для проверки вбейте название ресурса (не саму ссылку!) в Google и посмотрите, что про него знает поисковик.
- Если стиль письма странный или неестественный, значит, рассылка с большой вероятностью была переведена на русский с другого языка, а потом запущена в мессенджеры. Существуют рассылки, которые появляются ежегодно на протяжении уже 20 лет. Самое поразительное, что люди до сих пор им верят и распространяют!

Аудио

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

Видео

Чтобы проверить видео, придется приложить больше усилий. Вам помогут инструменты, описанные в Главе 9. Напомним, что у вас фактически есть два основных варианта действий:

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

Также можно пойти по олдскульному пути, самостоятельно сделав скриншот ключевого кадра и проверив его через сервисы поиска картинок. Выберите наиболее удобный для себя способ проверки.



Задание 10.2

Проверьте 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 из мессенджеров, не представляют особой сложности. Главное, всякий раз получая сомнительную рассылку, задумываться и приучить себя критически подходить к любому сообщению из непроверенного источника.

Как пролить свет на Dark Social

В 2020 году на фоне инфодемии сеть международных фактчекинговых организаций (IFCN) запустила специальный чат-бот в WhatsApp по теме коронавируса. Пользователям мессенджера он открыл доступ к тысячам материалов из более чем 70 стран мира. Чат-бот также фактически предложил желающим каталог глобальных организаций по проверке фактов. Основой для работы чат-бота стала база данных CoronaVirusFacts, которая представляет собой результат работы фактчекеров по всему миру. База обновлялась ежедневно, чтобы пользователи через свои смартфоны могли отслеживать самую актуальную информацию об инфекции.

В том же году IFCN совместно с Africa Check и Volume запустила фактчекинговый подкаст «What's Crap on WhatsApp». В пятиминутных эпизодах пользователям WhatsApp рассказывают о фейках, распространяемых в мессенджере, и опровергают их.

Сам мессенджер WhatsApp, которым в мире пользуются более 2 млрд человек, также вводит определенные ограничения с целью минимизации распространения ложной информации. В 2018 году WhatsApp, например, лишил своих пользователей возможности пересыпалть одно сообщение более чем пяти другим людям. Эта мера, как утверждается, уменьшила объем вирусных сообщений во всем мире на 25%.

В 2020 году компания внедрила еще одно нововведение, ограничив возможность пользователей пересыпать в несколько чатов за раз так называемые «часто пересылаемые сообщения» (помечаются символом в виде двойной стрелки). Следом WhatsApp начал тестирование простого способа проверки таких сообщений – нажатие на символ увеличительного стекла загрузит сообщение при помощи браузера в Google, и пользователь сможет увидеть источник информации или ее опровержение.

Редакция казахстанского фактчекингового ресурса Factcheck.kz практически ежедневно проверяет распространяемые через мессенджеры сообщения и определяет степень их достоверности. Примеры таких рассылок приведены в таблице 10.1.

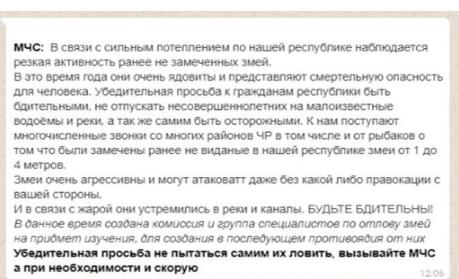
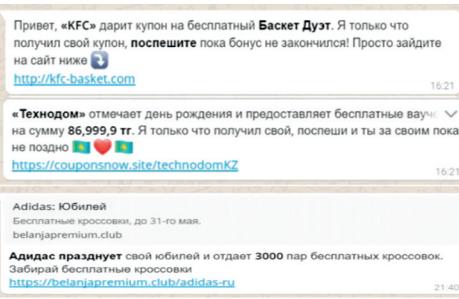
 <p>MЧС: В связи с сильным потеплением по нашей республике наблюдается резкая активность ранее не замеченных змей. В это время года они очень ядовиты и представляют смертельную опасность для человека. Убедительная просьба к гражданам республики быть бдительными, не отпускать несовершеннолетних на малоизвестные водоемы и реки, а так же самим быть осторожными. К нам поступают многочисленные звонки со многих районов ЧР в том числе и от рабаков о том что были замечены ранее не виданные в нашей республике змеи от 1 до 4 метров. Змеи очень агрессивны и могут атаковать даже без какой либоprovокации с вашей стороны. И в связи с жарой они устремились в реки и каналы. БУДЬТЕ БДИТЕЛЬНЫ! В данное время создана комиссия и группа специалистов по отлову змей при приеме изучения, для создания в последующем противоядия от них Убедительная просьба не пытаться самим их ловить, вызывайте МЧС а при необходимости и скорую</p> <p style="text-align: right;">12.06</p>	<p>Фейковая рассылка распространялась в соцсетях, мессенджерах и некоторых СМИ России, Казахстана, Киргизстана. Официальный представитель комитета по чрезвычайным ситуациям Министерства внутренних дел Республики Казахстан заявил, что информация в сообщении не соответствует действительности.</p>
 <p>Привет, «KFC» дарит купон на бесплатный Баскет Дзэт. Я только что получил свой купон, поспешите пока бонус не закончился! Просто зайдите на сайт ниже http://kfc-basket.com</p> <p>16:21</p> <p>«Технодом» отмечает день рождения и предоставляет бесплатные ваучер на сумму 86,999,9 тг. Я только что получил свой, поспеши и ты за своим пока не поздно    https://couponsnow.site/technodomKZ</p> <p>16:21</p> <p>Adidas: Юбилей Бесплатные кроссовки, до 31-го мая. belanjarremium.club</p> <p>Адидас празднует свой юбилей и отдает 3000 пар бесплатных кроссовок. Забирай бесплатные кроссовки https://belanjarremium.club/adidas.ru</p> <p>21:40</p>	<p>Все три рассылки являются фейковыми. В ходе проверки указанных в сообщениях ссылок через сервис проверки доменных имен выяснилось, что они не ведут на официальные сайты упомянутых компаний.</p>
 <p>Сейчас у нас в городе появился новый вид мошенничества. Приходят молодые люди в белых рубашках с пистолетами и угрожают гражданам и сообщают о похищении с заложниками. Ведут переговоры с населением и собирают информацию ФИО, МЕСТО РАБОТЫ, ДАТЫ РОЖДЕНИЯ, О КОЛИЧЕСТВЕ ДЕТЕЙ И ТД. По прошествии нескольких дней происходит воровство в этих домах. Когда у этих людей требуешь удостоверение, они показывают, но в руки не дают, и фотографировать не разрешают. А когда говоришь им, что сейчас позвонишь в акимат или участковому, то они очень быстро уходят. Пожалуйста разрешите знакомым эту информацию. Будьте бдительны!</p> <p style="text-align: center;">ВНИМАНИЕ! Воры квартириван!</p> 	<p>Распространенное сообщение о людях, которые, выдавая себя за сотрудников акимата, грабят дома, является фейковым. Проверка показала, что на представленных фото изображены люди, находящиеся в розыске в связи с совершением различных преступлений. Среди них двоим судом уже вынесен приговор.</p>

Таблица 10.1. Примеры фейковых рассылок с пояснением



Задание 10.3

В классе разделитесь на три группы. Задача каждой группы – вспомнить и составить список подозрительных сообщений, которые в последние несколько месяцев приходили ее членам в WhatsApp. После того, как зафиксируете, озвучьте перечень в классе. Определите в формате дискуссии, какие сообщения встречались во всех группах, только в двух группах, только в одной группе.

Теперь вы готовы к проверке практически любой информации, однако не забывайте: ваше главное оружие – внимательность и критическое мышление. Никакие цифровые решения не смогут их заменить. Они способны лишь помочь, облегчив поиск первоисточника информации.



Итоги:

Посчитайте, сколько разных программ для обмена сообщениями установлено на ваших мобильных устройствах и компьютерах (считайте также чаты внутри браузерных версий социальных сетей). Определите, как часто вы пользуетесь теми или иными мессенджерами, переписываетесь ли вы с одними и теми же людьми в разных мессенджерах.

Если у вас три и более мессенджеров, проанализируйте, какую именно информацию (достоверную, новостную, проверенную, непроверенную, слухи, розыгрыши) и от кого (семья, друзья, одноклассники, незнакомые люди) вы получаете через них.

Обсудите, сколько программ для передачи сообщений действительно необходимо для того, чтобы оставаться на связи с близкими и получать достоверную информацию. Может быть, достаточно простого кнопочного телефона? А, может, для каждого круга общения необходим отдельный мессенджер?

Глоссарий

А

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

Алгоритм – ряд математических инструкций или правил, с помощью которых можно решить задачу (*определение из Кембриджского словаря*).

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 рядовые пользователи.

Б

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. Другие боты рассылают вирусы, спам или оставляют комментарии на сайтах (*определение из Technopedia*).

В

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

Видеофейк – умышленно искаженное видео.

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 (преимущественно за счет социальных сетей) и резко набирающий популярность.

Вычислительная журналистика (англ. computational journalism) – применение в журналистике вычислительных методов для сбора, организации и распространения новостной информации. Использует приемы искусственного интеллекта, анализа данных, визуализации, персонализации и рекомендательных систем.

Г

Газетная утка – то же, что и фейк. Точное происхождение фразы не установлено, однако бытует мнение, что некий брюссельский журналист Роберт Корнелиссен, живший во времена Наполеона, написал статью о небывалой прожорливости уток, которые поедали своих сородичей. Другая история относит нас к немецким редакторам, которые помечали непроверенную информацию аббревиатурой NT. При беглом прочтении буквосочетание читалось так же, как и «утка» на немецком – «Ente».

Геолокация – определение месторасположения пользователя с помощью интернета или мобильного телефона (*определение из Кембриджского словаря*).

Гиперпартизанский сайт – сайт, чей контент категорично отражает взгляды членов и сторонников лишь одной политической партии.

Гражданская журналистика – вид журналистики, при котором в создании, анализе и распространении информации активное участие принимают рядовые граждане, профессионально не занятые в медиасфере.

Групповое подкрепление (англ. communal reinforcement) – ситуация, при которой высказывание становится убеждением вне зависимости от того, является оно реальным фактом или нет. Имеет место внутри социальной группы, члены которой многократно воспроизводят то или иное убеждение (*определение из The Skeptic's Dictionary*).

Д

Дата-журналистика – направление в журналистике, в основе которого лежит обработка данных и их использование для создания журналистского материала. При этом данные могут служить как источником для истории, так и инструментом для более подробного раскрытия темы.

Дебанкинг (англ. debunking) – развенчание, разоблачение слуха, неправды, мифа.

Дезинформация (англ. disinformation) – намеренно распространяемая ложная информация.

Дипфейк (англ. deepfake) – видеоролики, созданные искусственным интеллектом на основе огромного количества изображений, искусно имитирующие речь и движения человека, его мимику и эмоции.

Ж

«Желтая» журналистика – журналистика низшего сорта, отдающая предпочтение громким и сенсационным новостям без какой-либо проверки фактов. Термин появился в разгар противостояния между двумя американскими медиамагнатами Джозефом Пулитцером и Уильямом Рэндольфом Херстом в конце XX века. Газета The New York World, принадлежащая Пулитцеру, в то время выпускала комикс под названием «The Yellow Kid».

З

Зомби-фейк – фейковая новость, которая время от времени вновь начинает распространяться в интернете и других медиа несмотря на опубликованное ранее разоблачение.

И

Индекс свободы прессы – ежегодный рейтинг международной неправительственной организации «Репортеры без границ». Оценивает такие параметры в СМИ как плюрализм мнений, самоцензура, независимость, законодательство и др.

Интернет-тролль – интернет-пользователь, цель которого разжечь спор и вовлечь в него как можно большее количество людей (*определение из The Guardian*).

Инфлюенсер / лидер мнений – человек, который влияет на мнения и поведение людей с помощью социальных сетей (*определение из Кембриджского словаря*).

Информационная война – противостояние с применением информационных технологий для сбора данных о противнике, а также кибератак, манипуляции, пропаганды и других коммуникационных средств для создания негативного образа соперника.

Информационное загрязнение – загрязнение информационного поля неполной, противоречивой, малоценней или не относящейся к делу информацией.

Информационная перегрузка – ситуация, при которой человек получает настолько много информации, что не может рационально ее воспринимать (*определение из Кембриджского словаря*).

Информационный пузырь (англ. filter bubble) – термин, применяемый преимущественно к социальным сетям и описывающий ситуацию, при которой человек не имеет доступа к информации, противоречащей его взглядам и вкусым, получая таким образом ограниченную перспективу. 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 информации, вследствие которой человек теряет способность адекватно воспринимать информацию.

Искусственный интеллект – способность компьютера или робота, управляемого через компьютер, выполнять задания, которые обычно 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.

К

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

Критическое мышление — рациональный, объективный анализ фактов.

Кодекс фактчекеров — свод принципов, разработанный Международной фактчекинговой сетью (IFCN) и включающий 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.

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 кэш сайта доступен при нажатии на стрелку возле ссылки на страницу сайта в поисковой выдаче.

M

Македония – страна, известная 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 AdSense 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 (*определение O'Reilly*).

Медиаграмотность – умение анализировать и оценивать различные виды и жанры медиа на предмет наличия 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 (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 основанное на фактах. Не путать с фактом.

0

Открытые данные (англ. open data) – данные, к которым каждый может получить доступ, воспользоваться и поделиться ими. Примерами открытых данных могут считаться сайты комитета статистики, мажилиса, сената или Открытого Правительства.

П

Первоисточник – самый первый, то есть оригинальный источник, где появилась новость, факт, мнение. Из-за структуры социальных сетей, сайтов и плагиата найти первоисточник зачастую сложно, но возможно, прибегнув к возможностям поисковиков.

Популизм – политика, апеллирующая к широким массам и обещающая им скорое и легкое решение острых социальных проблем (*определение из словаря Ожегова-Шведовой*).

Постправда – слово 2016 года по версии Оксфордского словаря, означающее явление, при котором общественное мнение формируется, главным образом, личными убеждениями людей и их эмоциями, а не объективными фактами.

Правдомер – измерительная шкала фактчекинговых вердиктов, обычно включающая 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» (рисунок 11.1); 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 то, что проверяют фактчекеры: утверждения политиков, чиновников или других публичных лиц, содержащие факты, данные и цифры.

Пропаганда – информация, идеи, мнения или изображения, часто дающие только часть аргументации или исказжающие ее; транслируются, публикуются или иным образом распространяются с намерением повлиять на мнение людей (*определение из Оксфордского и Кембриджского словарей*).

Псевдонаука – убеждения или методики, которые ошибочно принимают как основанные на научных методах (*определение из Оксфордского словаря*). Примеры: астрология, феномен «плоской» Земли, фен-шуй, гомеопатия, акупунктура, нейролингвистическое программирование, уфология.



Рисунок 11.1. Изображение правдомера (ист. – Politifact.com)

P

Расследовательская журналистика – вид журналистики, цель которой состоит в обнародовании информации, представляющей большой интерес для публики, которую, тем не менее, от нее скрывают (*определение из Оксфордского словаря*). Часть инструментов, использующихся в фактчекинге, применяют и в расследовательской журналистике – открытые источники, инструменты для анализа и верификации.

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

C

Слух, сплетня – сообщение о чьей-либо личной жизни, которое может быть неверным (*определение из Кембриджского словаря*).

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

Ф

Факт – реальное событие, явление, существование которого можно проверить с помощью открытых источников. В фейковых новостях факт нередко путают 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 обнародуется как достоверное (*определение из пособия «Фактчекинг как тренд журналистских расследований: возможности и перспективы»*).

Фактчекинг (англ. fact-check) – 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 (англ. fake news) – слово 2017 года по версии словаря Коллинза, означающее ложную информацию, зачастую сенсационную, распространяемую под видом новостной журналистики. Широкая дискуссия о фейковых новостях и их последствиях развернулась во время президентских выборов в США в 2016 году.

Фотофейк – умышленно искаженное изображение.

Э

Эхо-камера (англ. echo chamber) – ситуация, при которой повторяются или распространяются одни и те же мнения так, что люди не сталкиваются с противоположными им взглядами (*определение из Dictionary.com*).

Для заметок:

Учебное пособие

**Банников Павел Владимирович
Гороховський Олександр
Соколова Таша
Печищев Иван Михайлович
Радзявиčус Дайнюс
Усупбаева Айчурек
Шишкін Дмитрий Павлович**

**МЕДИА И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ
Учебное пособие для 9 – 11(12) классов**

Менеджер проекта: Кошкина А.О.
Координатор проекта: Цой С.Е.
Редактор: Бочарова М.В.
Методист: Карагабанов Р.А.
Ассистент методиста: Бурбаева Б.С.
Корректор: Жаксыбаева А.К.
Дизайнер: Артюхова А.В.
Иллюстратор: Хван И.С.

Подписано в печать _____. Формат 70x100 1/16.
Бумага офсетная. Гарнитура Tinos, DIN Pro, Oswald. Печать цифровая.
Усл.печ.л. 13 Тираж ____ экз. Заказ № 817.11.2020

