



МЕДИАГРАМОТНОСТЬ - кратко в терминах

Панова М.И., методист МАОУ ДО г. Иркутска «Дворец творчества»

Информационный_пузырь

Персональные_данные

Инфодемия

Троллинг

Медиа

Цифровой_этикет

Кибербуллинг

Родительский_контроль

Информационная_гигиена

Цифровой_след

Критическое_мышление

Цифровая_безопасность

Медиаграмотность

фильтр

Верификация

Моббинг

Фактчекинг

Медиапотребление

Медиаобразование

Фейк

Контент

Фишинг

Медиамейкинг

Постправда

Цифровые_изображения

Медиаэкология



МИГ – это медийно-информационная грамотность. Термин обозначает основные характеристики (знания, навыки и отношения), позволяющие гражданам эффективно взаимодействовать с медиа и другими поставщиками информации и развивать критическое мышление и навыки обучения на протяжении всей жизни для социализации и превращения в активных граждан.

КРИТЕРИИ МЕДИАГРАМОТНОСТИ

Приказ Министерства связи и массовых коммуникаций РФ от 28 июля 2014 г. № 226 "О Критериях медиаграмотности и методике оценки уровня медиаграмотности населения"

- а) умение пользоваться поисковыми системами и находить необходимую информацию;**
- б) способность обращать внимание на источники информации, верифицировать информацию и **КРИТИЧЕСКИ** ее оценивать;**
- в) умение защитить свои персональные данные в сети Интернет и способность не допускать утечки информации, касающейся личной жизни, которая может представлять интерес для злоумышленников;**
- г) знание о системах «родительского контроля», умение пользоваться ими, а также способность провести для детей курс личной безопасности по их действиям в социальных сетях и сети Интернет;**
- д) способность сопоставлять информацию из различных источников, стремиться проверять любую полученную информацию**

Компетенции, определяющие функциональную грамотность: система 4К (базовые навыки и умения)

1. Коммуникативность:
навыки общения, умение
выражать и отстаивать свою точку
зрения

2. Креативность:
способность к творчеству,
нестандартно, неформально
мыслить и действовать,
любопытство, инновации,
самовыражение

Компетенции XXI века

3. КРИТИЧЕСКОЕ МЫШЛЕНИЕ:
решение проблем, рассуждение,
анализ, интерпретация,
обобщение информации

4. Координация (кооперация):
лидерство, работа в команде,
сотрудничество

ТЕМАТИЧЕСКИЕ ПОЛЯ МЕДИАГРАМОТНОСТИ



Фактчекинг и
верификация
информации

Как устроены
медиа

Этика

Медиамейкинг

Цифровая
безопасность

ТЕМАТИЧЕСКИЕ ПОЛЯ МЕДИАГРАМОТНОСТИ

Фейк Постправда
Фактчекинг
Верификация
Инфодемия

Фактчекинг и
верификация
информации

Как устроены
медиа

Медиапотребление
Медиаэкология

Этика

Медиамейкинг

Медиаобразование
Цифровые_изображения

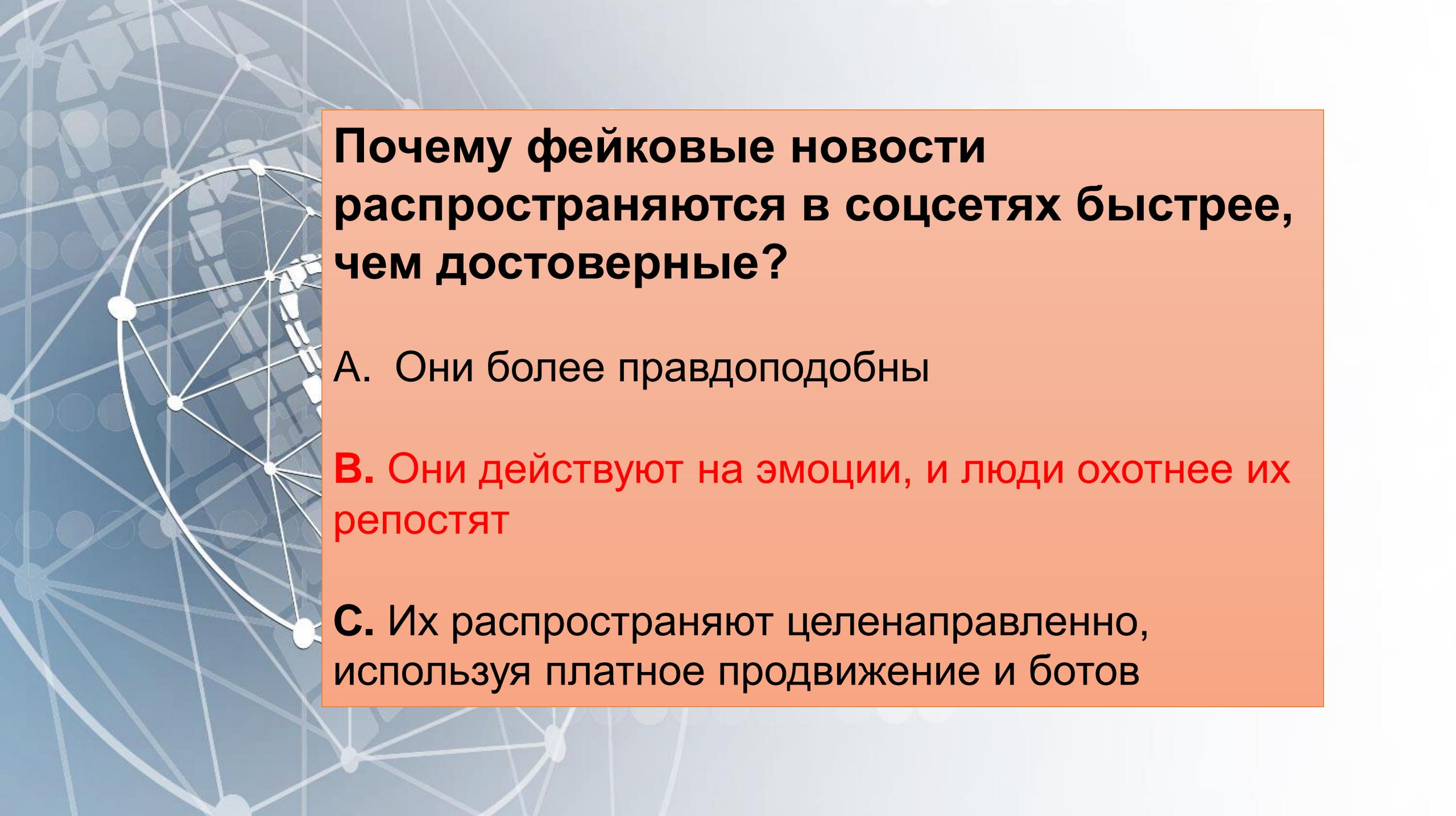
Медиамейкинг

Троллинг
Моббинг

Цифровой_этикет
Цифровой_след
Кибербуллинг

Цифровая
безопасность

Информационный_пузырь
Персональные_данные
Информационная_гигиена
Контент_фильтр
Родительский_контроль
Фишинг

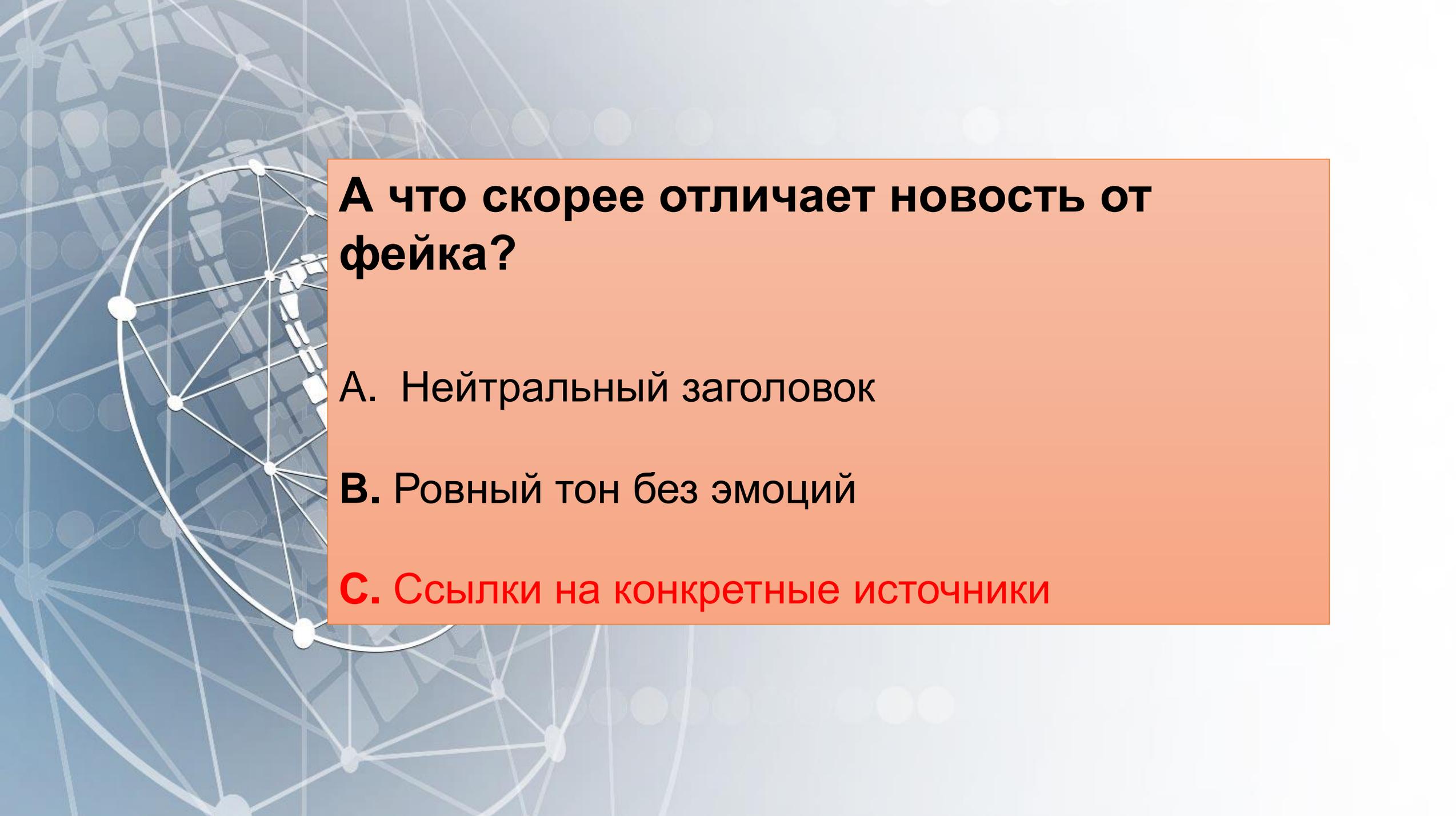
A background graphic of a network diagram with nodes and connecting lines, overlaid on a faint globe. The nodes are represented by small circles, and the lines represent connections between them. The overall color scheme is light blue and white.

Почему фейковые новости распространяются в соцсетях быстрее, чем достоверные?

А. Они более правдоподобны

В. Они действуют на эмоции, и люди охотнее их репостят

С. Их распространяют целенаправленно, используя платное продвижение и ботов

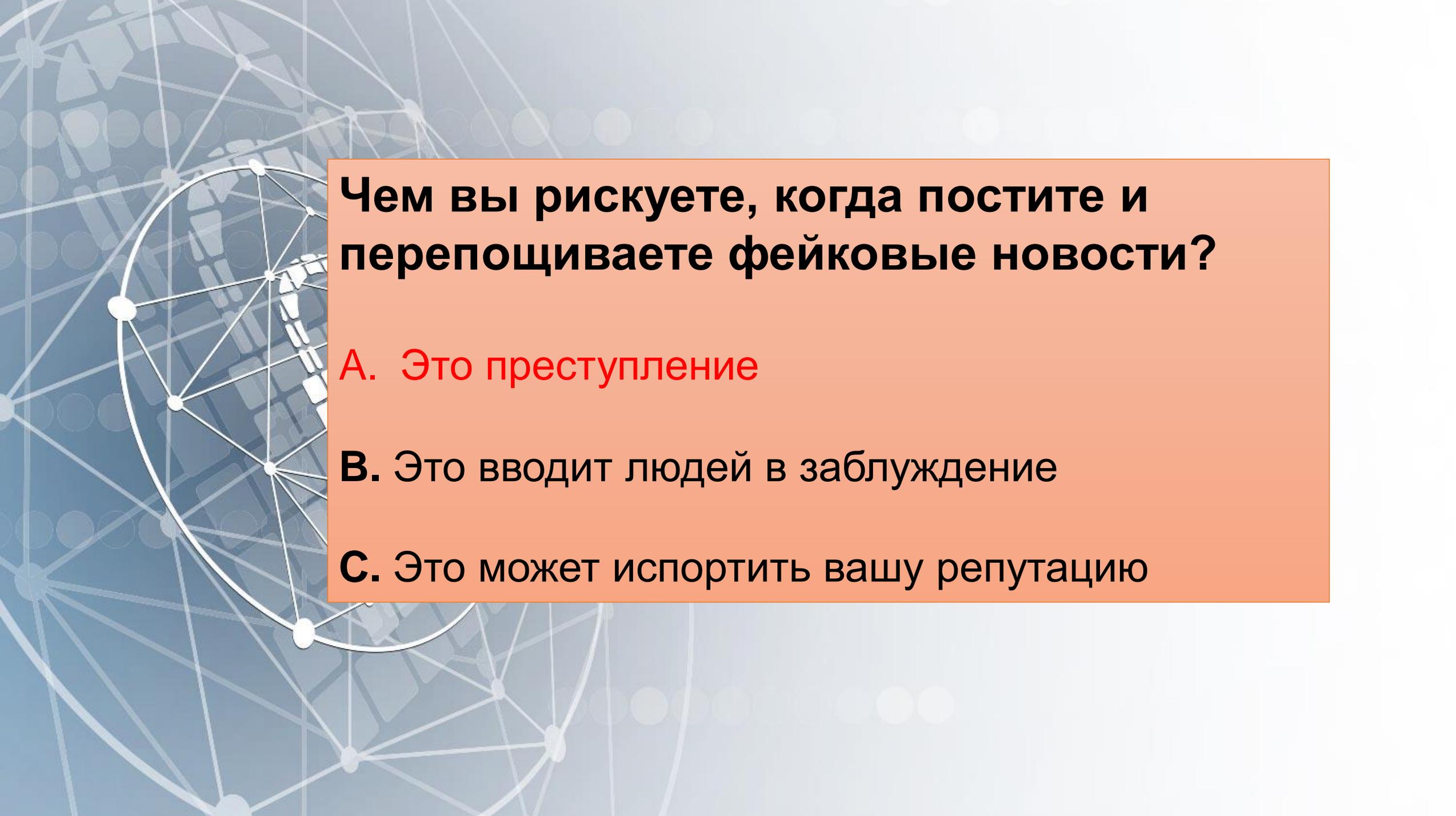
The background features a stylized globe with a network of white lines and dots overlaid on it, set against a light blue gradient. The globe is positioned on the left side of the frame.

**А что скорее отличает новость от
фейка?**

А. Нейтральный заголовок

В. Ровный тон без эмоций

С. Ссылки на конкретные источники

The background features a stylized globe with a network of white lines and dots overlaid on it, set against a light blue gradient. The globe is positioned on the left side of the frame.

Чем вы рискуете, когда постите и перепощиваете фейковые новости?

А. Это преступление

В. Это вводит людей в заблуждение

С. Это может испортить вашу репутацию

Фейк Постправда
Фактчекинг
Верификация
Инфодемия

ФАКТЧЕКИНГ И ВЕРИФИКАЦИЯ ИНФОРМАЦИИ

ФЕЙК

недостоверная, ложная, искаженная
или неполная информация,
распространяемая в медиа, а также
небрежность, опечатки и
технические ошибки, которые, уходя
в массовое сознание, создают
ложную реальность

ОБЪЯСНЯЕМ.РФ



Фейк Постправда
Фактчекинг
Верификация
Инфодемия

ФАКТЧЕКИНГ И ВЕРИФИКАЦИЯ ИНФОРМАЦИИ

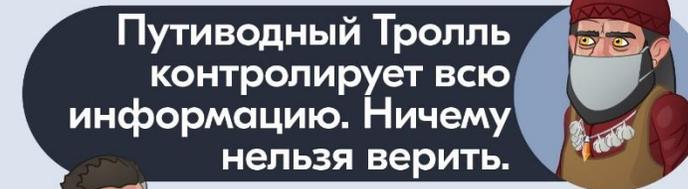
ИНФОДЕМИЯ

Заражение информационного пространства вредоносными материалами: теории заговоров, слухи, сплетни, откровенно панические и пессимистические публикации, отрицание, диссидентство и т.д.

Негативное и необъективное отражение процесса в СМИ, социальных сетях и мессенджерах



Нельзя доверять любым источникам информации. Особенно когда это касается здоровья. Доверяйте только экспертам.



Путеводный Троль контролирует всю информацию. Ничему нельзя верить.



Даже если это так, это не значит, что знакомый из чата, который видел врачей раз в жизни, и то по телеку, пишет верную информацию.

И, конечно, сами не распространяйте **непроверенную информацию**, даже если она кажется правдивой или очень смешной и увлекательной.

Фейк Постправда
Фактчекинг
Верификация
Инфодемия

ФАКТЧЕКИНГ И ВЕРИФИКАЦИЯ ИНФОРМАЦИИ

ФАКТЧЕКИНГ

Проверка точности и достоверности информации, которую медиа обрабатывают и передают своей аудитории, — залог соблюдения главных этических принципов журналистики.

Технологии проверки информации может использовать каждый.

Анализируя информацию о каком-либо событии, прежде всего нужно установить, из чего оно состоит — это могут быть факты, фактоиды или эмпирические обобщения

Факт — это
«подкрепленное
надежными
свидетельствами событие»

Фактоид — это сообщение,
в котором нет одной или
нескольких границ факта

Эмпирическое обобщение
— это описание события
«на глаз»

Фейк Постправда
Фактчекинг
Верификация
Инфодемия

ФАКТЧЕКИНГ И ВЕРИФИКАЦИЯ ИНФОРМАЦИИ

ПРИНЦИПЫ ВЕРИФИКАЦИИ ИНФОРМАЦИИ

КРИТИЧЕСКОЕ МЫШЛЕНИЕ И ЗДРАВЫЙ СМЫСЛ

Знакомый сайт, у заметки
есть автор, известно кто
финансирует сайт

Заметка имеет два или три
независимых друг от друга
источника или дает ссылку
на оригинал

Комментаторы
представляли различные
стороны конфликта
Автор компетентен

Объем вложенного труда — лучший индикатор
нефейка. Чем больше в заметке фактов, хороших
источников и комментаторов, иллюстраций,
диаграмм, скриншотов и видео, тем лучше

Прочитав первые строки и поняв
расстановку сил, ищите контекст,
полезную дополнительную
информацию и факты, которые
противоречат вашей картине мира

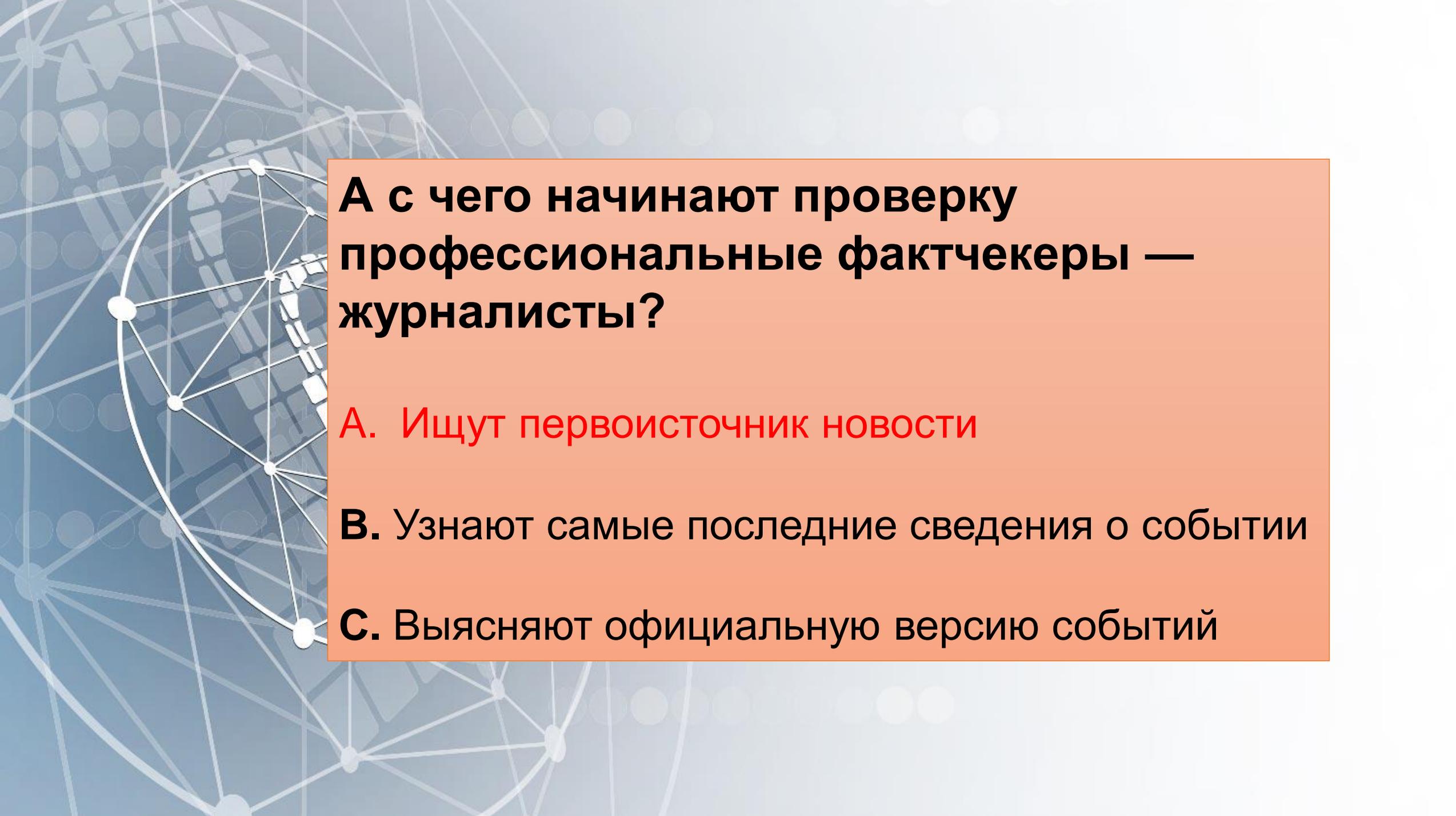
Фейк Постправда
Фактчекинг
Верификация
Инфодемия

ФАКТЧЕКИНГ И ВЕРИФИКАЦИЯ ИНФОРМАЦИИ

ПОСТПРАВДА

Тонкость границы между миром объективным, который в идеале должен быть одинаковым для восприятия всеми, и миром субъективным, миром убеждений и предпочтений, который у разных групп населения, наций, социальных групп и индивидуумов может значительно отличаться

**ПОСТПРАВДА –
ЭТО ПОБЕДА ЭМОЦИЙ
НАД ФАКТАМИ**

The background features a stylized globe with a network of white lines and dots overlaid on it, set against a light blue gradient. The globe is positioned on the left side of the frame.

А с чего начинают проверку профессиональные фактчекеры — журналисты?

А. Ищут первоисточник новости

В. Узнают самые последние сведения о событии

С. Выясняют официальную версию событий

Троллинг
Моббинг
Цифровой_этикет
Цифровой_след
Кибербуллинг

ЭТИКА

Цифровой этикет

В первую очередь это этические дилеммы, связанные с необходимостью осмыслить феномен цифрового присутствия человека и особенности его взаимодействия с другими в новой среде, осмысление новых норм морали, рождающихся в этом процессе

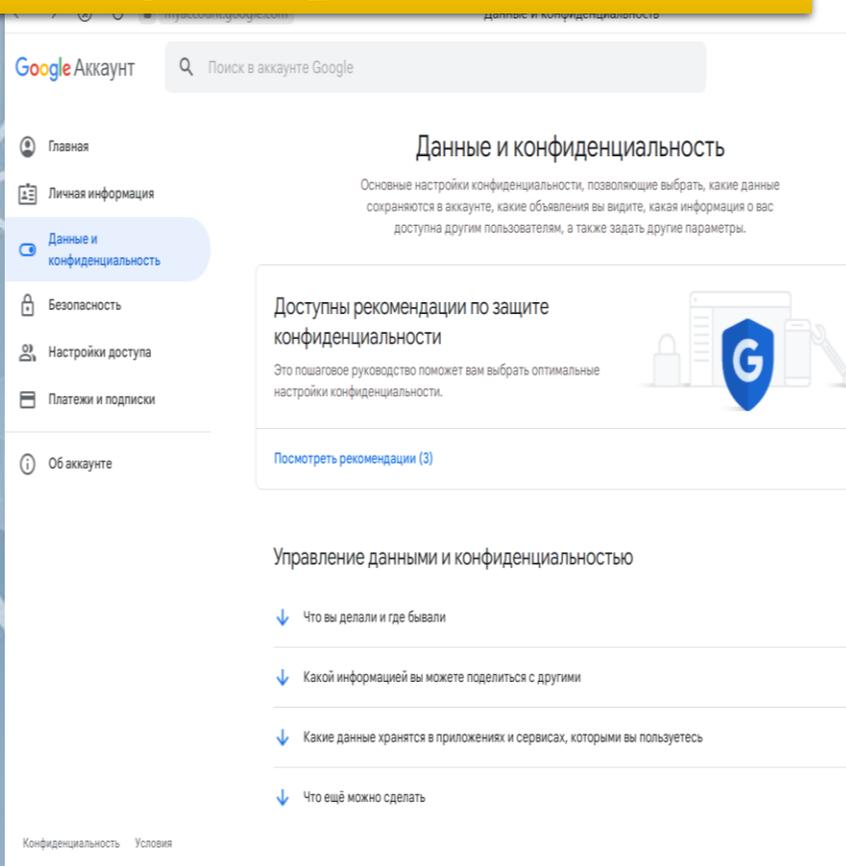
Главная цель цифрового этикета - сделать **общение** с собеседниками максимально **комфортным** для всех сторон.

Основное правило: заботьтесь о том, чтобы **удобно** в первую очередь было не вам, а вашему **собеседнику**.



Троллинг
Моббинг
Цифровой_этикет
Цифровой_след
Кибербуллинг

Google сервис «О себе»



ЭТИКА

Цифровой след

След действий, которые мы совершаем в цифровом пространстве. Принято говорить о пассивном и активном цифровом следе. Пассивный — это данные, которые собирают независимо от пользователя поисковые системы и онлайн-платформы. Активный цифровой след формируем мы сами, оставляя в интернете персональную информацию. Цифровой след называют еще слепком или тенью, по сути это электронный цифровой портрет пользователя – его репутация

Троллинг
Моббинг
Цифровой_этикет
Цифровой_след
Кибербуллинг

КоАП РФ Статья 5.61.

Оскорбление

"Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 27.01.2023)

ЭТИКА

Кибербуллинг Моббинг Диссинг
Киберсталкинг Секстинг Фрейпинг
Аутинг Кэтфишинг Газлайтинг
Викимблейминг

Травля, насмешки, оскорбления, угрозы, преследования и др. в условиях цифровой среды, то есть намеренная систематическая агрессия, направленная против жертвы с использованием электронных технологий. С этими явлениями можно столкнуться на всех медиаплатформах

Троллинг
Моббинг
Цифровой_этикет
Цифровой_след
Кибербуллинг

ЭТИКА

**Статья 282 УК -
возбуждение
ненависти
либо вражды,
а равно
унижение
человеческого
достоинства**

Действия, направленные на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично, в том числе с использованием средств массовой информации либо информационно-телекоммуникационных сетей, включая сеть «Интернет» лицом после его привлечения к административной ответственности за аналогичное деяние в течение одного года,

наказываются штрафом в размере от трехсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет, либо принудительными работами на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо лишением свободы на срок от двух до пяти лет.

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

Родительский_контроль

Фишинг

Ссылку, ведущую на ресурс, представляющий угрозу для вашего устройства, можно получить и по электронной почте, и в мессенджере социальной сети

Информационная гигиена

- для совершения важных операций использовать компьютер, в защищенности которого вы уверены,
- пользоваться только лицензионным оборудованием, постоянно обновлять софт,
- не подключать к компьютеру неизвестные флешки и другие usb-носители,
 - отключать автозапуск для внешних устройств,
 - не заряжать телефоны от чужих гаджетов,
- при работе в общественном месте не вводить важные пароли на экране ноутбука,
 - использовать мощный антивирус
- не разрешать малознакомым людям пользоваться на вашем компьютере почтовыми и социальными сервисами.

Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

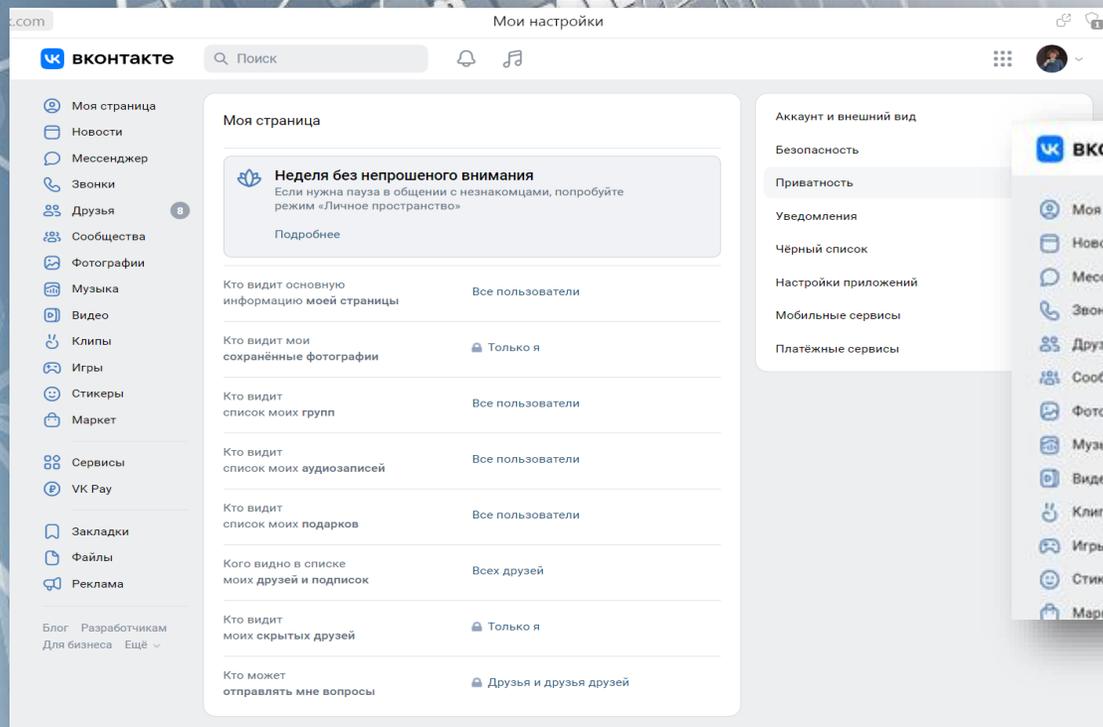
Родительский_контроль

Фишинг

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Персональные данные

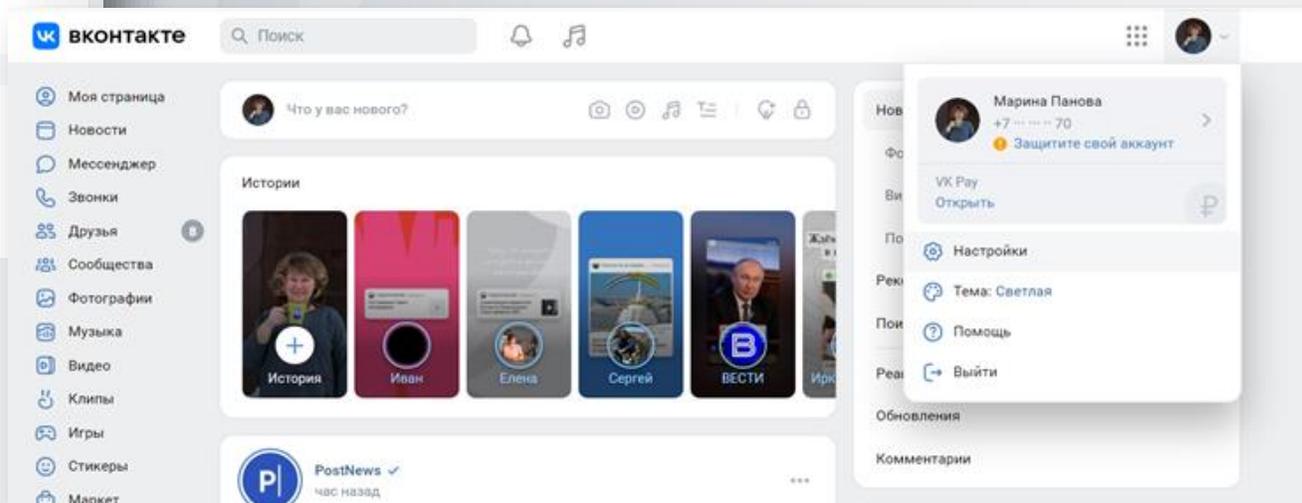
В социальных сетях можно настроить конфиденциальность вашего профиля «ВКонтакте», «Одноклассников» и любой другой соцсети



Скриншот страницы «Мои настройки» в социальной сети ВКонтакте. В центре экрана отображены настройки приватности для «Моя страница». Вверху страницы видны меню «Моя страница», «Новости», «Мессенджер», «Звонки», «Друзья», «Сообщества», «Фотографии», «Музыка», «Видео», «Клипы», «Игры», «Стикеры», «Маркет», «Сервисы», «VK Pay», «Закладки», «Файлы», «Реклама» и «Блог». В центре экрана — таблица настроек приватности:

Настройка	Текущее значение
Кто видит основную информацию моей страницы	Все пользователи
Кто видит мои сохранённые фотографии	Только я
Кто видит список моих групп	Все пользователи
Кто видит список моих аудиозаписей	Все пользователи
Кто видит список моих подарков	Все пользователи
Кого видно в списке моих друзей и подписок	Всех друзей
Кто видит моих скрытых друзей	Только я
Кто может отправлять мне вопросы	Друзья и друзья друзей

В правой части экрана видны дополнительные настройки: «Аккаунт и внешний вид», «Безопасность», «Приватность», «Уведомления», «Чёрный список», «Настройки приложений», «Мобильные сервисы» и «Платёжные сервисы».



Скриншот главной ленты ВКонтакте. В центре экрана — лента новостей с постами от «История», «Иван», «Елена», «Сергей» и «ВЕСТИ». В правой части экрана открыто меню настроек профиля, включающее: «VK Pay Открыть», «Настройки», «Тема: Светлая», «Помощь» и «Выйти».

Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

Родительский_контроль

Фишинг

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Признаки надёжного пароля

- Надёжный пароль содержит 12 символов, включает буквы в разном регистре, цифры и специальные символы (~!@#\$%^&*+-.\/\{\}[]();:|?<>=)
- Для надёжного пароля применяйте случайную комбинацию букв, цифр и других символов
- Не используйте для паролей личные данные, например, фамилию, дату рождения или кличку питомца. Такую информацию легко узнать, просмотрев ваши социальные сети
- Выбирайте за основу не слова, а фразы — они длиннее, их сложнее угадать или перебрать. Используйте для пароля смешное событие, забавную привычку, тайную мечту — такой пароль легко запомнить и трудно подобрать: «ГотовлюБорЩ_на5+баллов!@», «РекордПрохождения\$Цивилизации\$-32часа», «_Поеду1_вРио-де-Жанейро-вБелыхШт@н@х»
 - Придумайте пароль для каждого критичного аккаунта — интернет-банка, соцсетей и Госуслуг.
- Для аккаунтов, в которых не хранятся важные данные и не совершаются покупки, можно придумать простой и даже повторяющийся пароль
 - Используйте двухфакторную аутентификацию (2FA)
- 2FA — дополнительный уровень безопасности, так вы усложните путь хакерам. Плюс 2FA помогает предотвратить взлом. Если вы получили смс с кодом, который не запрашивали, значит, аккаунт пытаются взломать, нужно срочно сменить пароль

Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

Родительский_контроль

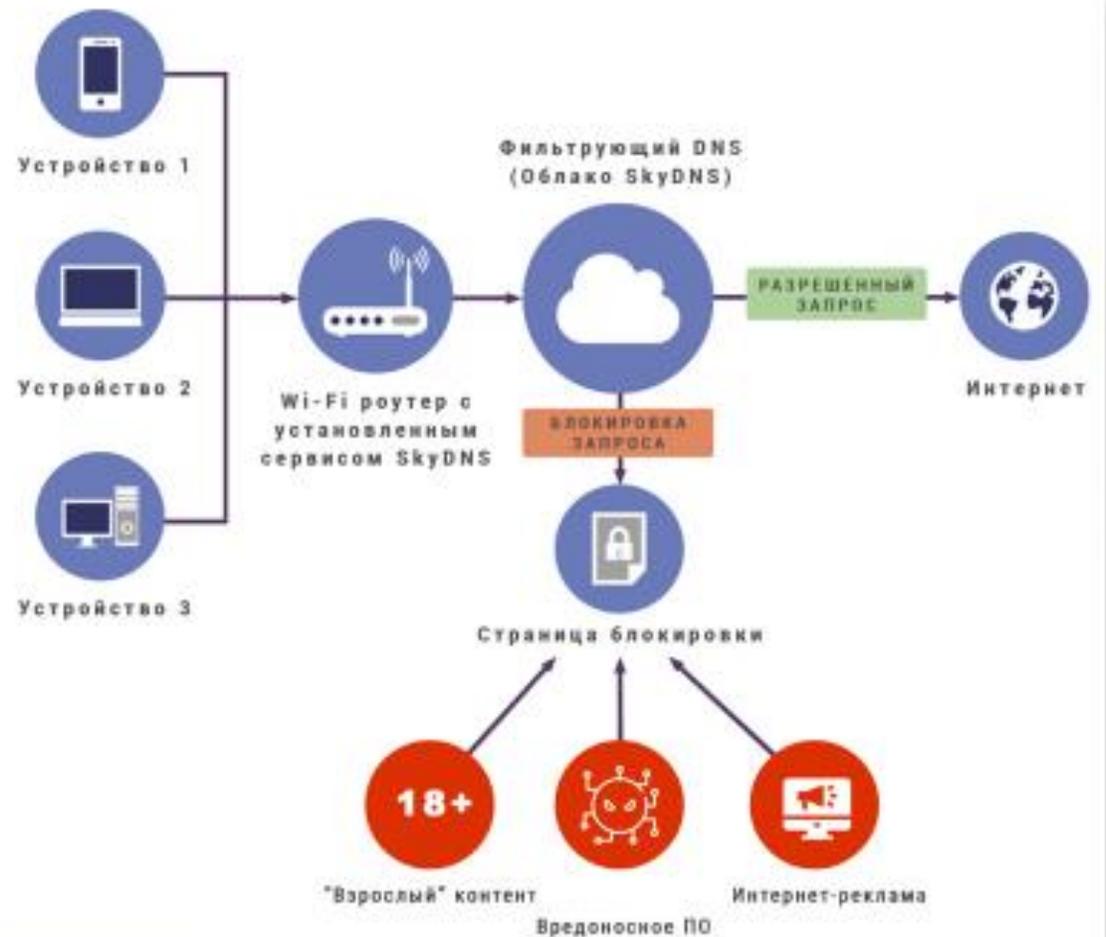
Фишинг

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Контент-фильтр

Шаг 1.
Контент-фильтр
от провайдера

Шаг 2.
Контент-фильтр
устанавливается на
технические средства
в учреждении:
на сервер или
отдельные
компьютеры и
ноутбуки



Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

Родительский

Фишинг

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Контент-фильтр

Яндекс DNS
Безопасный доменный интернет

Технические подробности

Яндекс DNS — это бесплатный рекурсивный DNS-сервис. Серверы Яндекс DNS находятся в России, странах СНГ и Западной Европе. Запросы пользователей обрабатывает ближайший дата-центр, что обеспечивает высокую скорость соединений.

	Базовый	Безопасный	Семейный
IPv4 Preferred DNS	77.88.8.8	77.88.8.88	77.88.8.7
Alternate DNS	77.88.8.1	77.88.8.2	77.88.8.3
IPv6 Preferred DNS	2a02:6b0:feed:0f::	2a02:6b0:feed:bad::	2a02:6b0:feed:a11::
Alternate DNS	2a02:6b0:0:1::feed:0f	2a02:6b0:0:1::feed:bad	2a02:6b0:0:1::feed:a11

Скорость работы Яндекс DNS во всех трех режимах одинакова. В «Базовом» режиме не предусмотрено никакого фильтрации трафика. В «Безопасном» режиме обеспечивается защита от зараженных и мошеннических сайтов. «Семейный» режим включает защиту от опасных сайтов и блокировку сайтов для взрослых.

	Базовый	Безопасный	Семейный
Быстрый и надежный DNS	✓	✓	✓
Защита от зараженных сайтов		✓	✓
Защита от мошеннических сайтов		✓	✓
Защита от ботов		✓	✓
Блокировка сайтов для взрослых			✓
Блокировка рекламы для взрослых			✓
Семейный поиск Яндекса			✓

Защита от зараженных сайтов

Яндекс ежедневно проверяет тысячи миллионов страниц на наличие вредоносного кода, выявляет тысячи зараженных сайтов. Для этого применяются сигнатурная технология Borbot и собственный антивирус Яндекса, построенный на анализе поведения исследуемых сайтов. При обнаружении подозрительной активности страница отмечается как опасная, а вредоносный код добавляется в базу вирусных сигнатур. Данные о зараженных сайтах обновляются несколько раз в сутки.

Защита от мошеннических сайтов

Яндекс также выявляет сайты, обладающие признаками мошенничества. К ним относятся, например, страницы, созданные с целью замануть номер телефона пользователя или выведующие его отправить сообщение на короткий номер, потеря данных. В «Безопасном» и «Семейном» режимах Яндекс DNS блокирует такие сайты — при попытке зайти на них, пользователь увидит предупреждение.

Защита от ботнетов

Получив в ботнет зараженный компьютер обычно управляется централизованно, через специальный C&C-сервер (от англ. command-and-control — командование и контроль). Адрес управляющего

Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

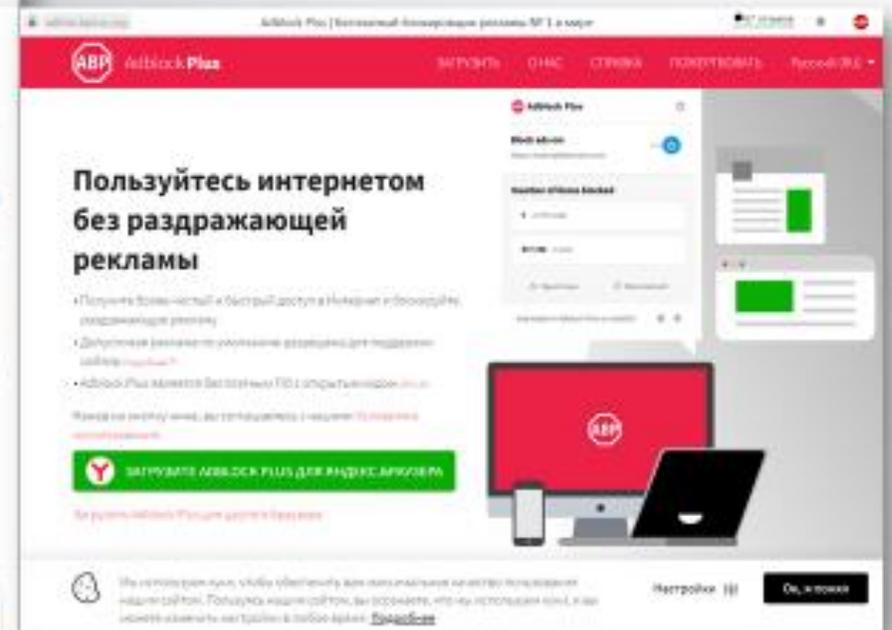
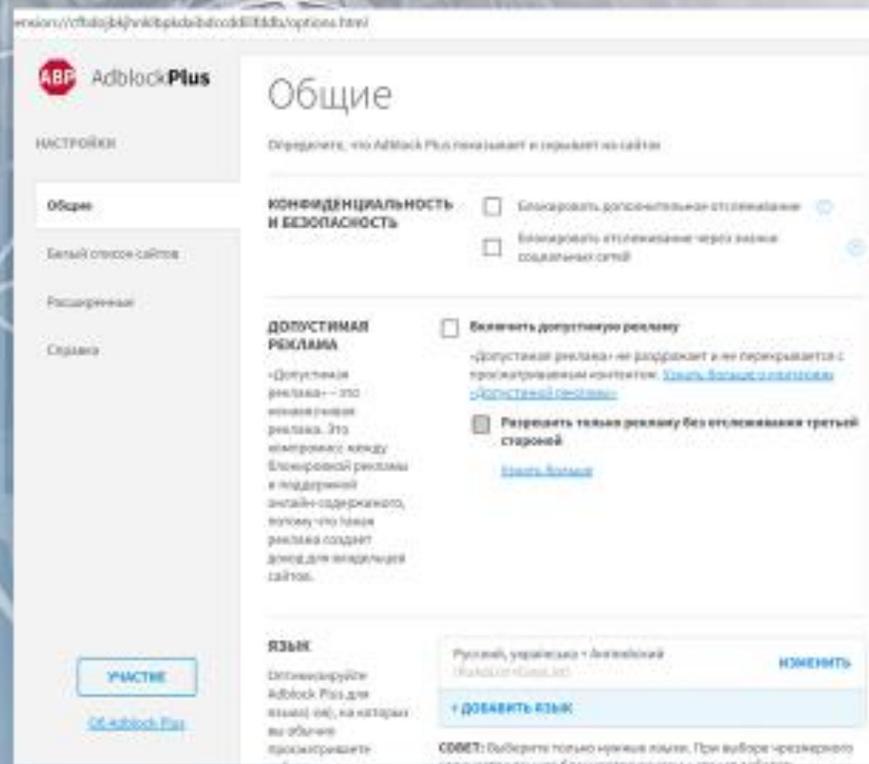
Родительский_контроль

Фишинг

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Контент-фильтр

Шаг 3. Дополнительный контент-фильтр, устанавливается по желанию персональными пользователями



Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

Родительский_контроль

Фишинг

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Родительский контроль

это программное обеспечение и инструменты, которые позволяют родителям контролировать использование интернета своими детьми

The image shows two side-by-side screenshots of a web browser. The left screenshot displays the search settings for Yandex, with a red arrow pointing to the 'Фильтрация страниц' (Page filtering) dropdown menu, which is set to 'семейный поиск' (Family search). The right screenshot shows the YouTube parental control settings page, with a red arrow pointing to the 'Безопасный режим: выкл.' (Safe mode: off) dropdown menu, which is set to 'вкл.' (on).

club.dns-shop.ru Как настроить родительский контроль на компьютере, планшете или смартфоне | Интернет | Блог | Клуб DNS

DNS КЛУБ Введите запрос Клубоины Эфир Создать Войти

Новости Обзоры Блоги Поток Коммуникатор Кьюнити Закладки DNS

Google

Настройки поиска

Результаты поиска Безопасный поиск

Языки Функция "Безопасный поиск" позволяет скрывать из результатов ссылки на контент сексуального характера, например порнографию. Настройки функции могут быть заданы администратором устройства или сети. Если вы не можете ее отключить, обратитесь к администратору.

Справка Включить Безопасный поиск Подробнее...

Яндекс Настройка

Настройка результатов поиска

Найденный документ

Область поиска

Язык найденных документов

Фильтрация страниц

семейный поиск умеренный фильтр Без ограни

Исправление запроса

Развлекательные платформы

У YouTube и Spotify доступны настройки родительского контроля. Например, можно создавать индивидуальные профили с разными уровнями управления, чтобы каждый член семьи видел только тот контент, который ему подходит.

включаем Родительский контроль на YouTube

YouTube

Безопасный режим

В безопасном режиме будут скрыты все видео с возрастными ограничениями и ролики, отмеченные пользователями как неподходящие.

Безопасный режим будет включен только в этом браузере.

Вкл. Откл.

Сохранить

О сервисе Прессе Правообладателям Авторам Рекламодателям Разработчикам +YouTube

Условия использования Конфиденциальность Правила и безопасность Отправить отзыв Новые функции © 2017 YouTube, LLC

В Spotify можно ограничить композиции для взрослых двумя путями. Первый — это отключить я

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

Родительский_контроль

Фишинг

Информационный пузырь

это совокупность средств персонализации контента в интернете.

Google или Yandex выдают в поиске не совсем то, что вы ищете. Вы получите скорее то, что они считают наиболее подходящим для вас – в соответствии с вашей ранней поисковой историей.

«ВКонтакте» сейчас не показывает ленту в хронологическом порядке. Они сортируют публикации в зависимости от ваших предпочтений. По тому же принципу они показывают рекомендуемый контент.

Все это достигается путем отслеживания ваших действий, причем как внутри самих сервисов, так и за их пределами. Лайки, репосты, просмотры, клики, поисковые запросы, открытые вкладки, поведение на внешних сайтах – все это мазки к вашему цифровому «портрету».

**ЕСЛИ ВЫ ХОТИТЕ
ОБЛАДАТЬ
МАКСИМАЛЬНО
ОБЪЕКТИВНОЙ
ИНФОРМАЦИЕЙ О
МИРЕ, ВАМ
ПРИДЕТСЯ
ВЫБРАТЬСЯ ИЗ
ЭТОГО ПУЗЫРЯ**

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Информационный_пузырь

Персональные_данные

Информационная_гигиена

Контент_фильтр

Родительский_контроль

Фишинг

Информационный пузырь

Google – зайдите в Учетную запись и отключите все отслеживающие активности.

Yandex – зайдите в Настройки и снимите галочку с «Учитывать мою историю поиска в результатах».

Пользуйтесь режимом “Инкогнито”, в котором не сохраняется история поиска и посещений. При этом выйдите из аккаунтов Google или Yandex.

Обманываем алгоритмы в соцсетях

А еще вы можете отключить персонализированную выдачу:

Facebook – нажмите на кнопку «Лента новостей» в боковой панели и поставьте галочку на «Новейшее».

«ВКонтакте» – в правой панели отключите функцию «Сначала интересные».

После этого разного мусора или просто ненужной информации до вашего сознания будет доходить намного меньше.

Интернет-гиганты хотят максимально удовлетворить наше эго. И этому способствует наше желание потреблять только комплементарную информацию.

Это ограничивает наше видение реальности и отключает критическое мышление.

Анонимизируйте свое присутствие в сети и сознательно ищите неприятную информацию, чтобы выйти из пузыря фильтров.

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

- 1. Не реагируйте на тревожные звонки, письма, SMS или сообщения в соцсетях о том, что вашему родственнику или знакомому нужны деньги. В этом случае стоит попытаться связаться с этим родственником или знакомым и сообщить, от их имени рассылаются такие сообщения, — возможно их аккаунт взломали.**
- 2. Не переходите по ссылкам в письмах о выигрыше денег, гаджета или другого приза. Скорее всего, по ссылке вы получите только вирус.**
- 3. Вообще не переходите по неизвестным ссылкам, не отвечайте и не перезванивайте по сомнительным номерам.**
- 4. Никому никогда не сообщайте коды подтверждения из SMS-сообщений.**
- 5. Не передавайте банковскую карту посторонним. Требуйте проведения операций с ней только в личном присутствии и старайтесь никогда не терять ее из виду.**

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

6. Никому не сообщайте пин-код от банковской карты, не пишите его на карте и храните отдельно. Набирая пин-код, всегда прикрывайте клавиатуру рукой. В том числе, при расчете в кафе и магазинах.

7. Не делайте покупки и не вводите код CCV/CVC на сомнительных сайтах.

8. Если банковская карта потерялась, немедленно сообщите в банк и заблокируйте ее. То же самое — если вам пришло SMS-сообщение о покупке или снятии денег в банкомате, а вы этого не делали. Для этого полезно иметь телефон службы поддержки банка под рукой.

9. Всегда осматривайте банкомат перед использованием. Необходимо убедиться, что над клавиатурой и на картоприемнике нет посторонних прикрепленных предметов, а клавиатура не шатается.

10. Не используйте открытые точки Wi-Fi (интернет в общественных местах: транспорте, кафе, кинотеатрах), когда заходите в интернет-банк или пользуетесь мобильным банковским приложением.

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

Убедитесь в наличии HTTPS

В соответствии со стандартами VISA и MasterCard, данные платёжных карт должны передаваться с помощью защищённого соединения, о чём говорит наличие в адресной строке браузера иконки замочка и префикса `https` в адресе сайта, где `s` означает `secure`, то есть безопасный

