Обеспечение и профилактика информационной безопасности детей и подростков

Баранова Мария Вячеславовна
старший методист
Центра информационных технологий
ГАУ ДПО ЯО ИРО
baranova@iro.yar.ru
RIBC76@yandex.ru

Вопросы

1. Риски информационной социализации.
2. Информация, охраняемая законом. Защита персональных данных.
3. Формы повышения кибербезопасности во внеурочной деятельности школьников.
4. Общение в мессенджерах как элемент коммуникации в образовательной среде.

VUCA-мир

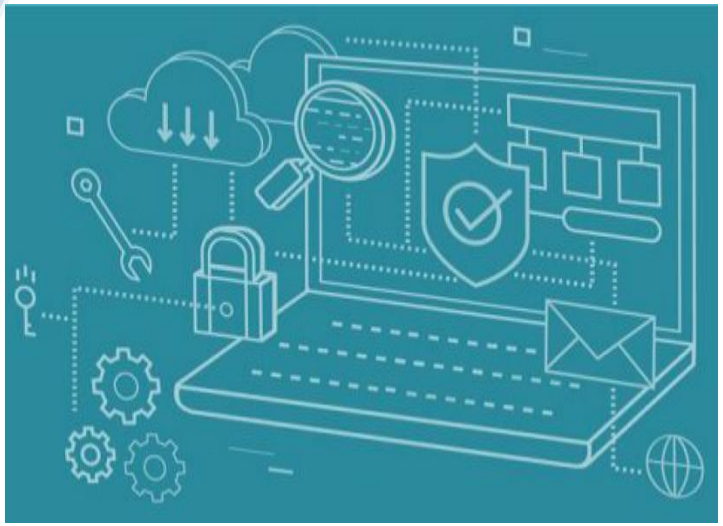
Изменчивость

Неопределенность

Сложность

Неоднозначность

Возможности технологий и интернета



- Быстрый доступ к неограниченному объёму информации.
- Дистанционное образование.
- Интенсификация общения и горизонтальные социальные связи.
- Улучшение качества жизни.
- Возможности для развития и саморазвития личности.
- и т.п.

Новые возможности – НОВЫЕ РИСКИ – новые практики совладания

Контентные риски. Возникают в процессе использования материалов, содержащих противозаконную, неэтичную и вредоносную информацию - насилие, агрессию, эротику и порнографию, нецензурную лексику, пропаганду суицида, наркотических веществ и т.д.

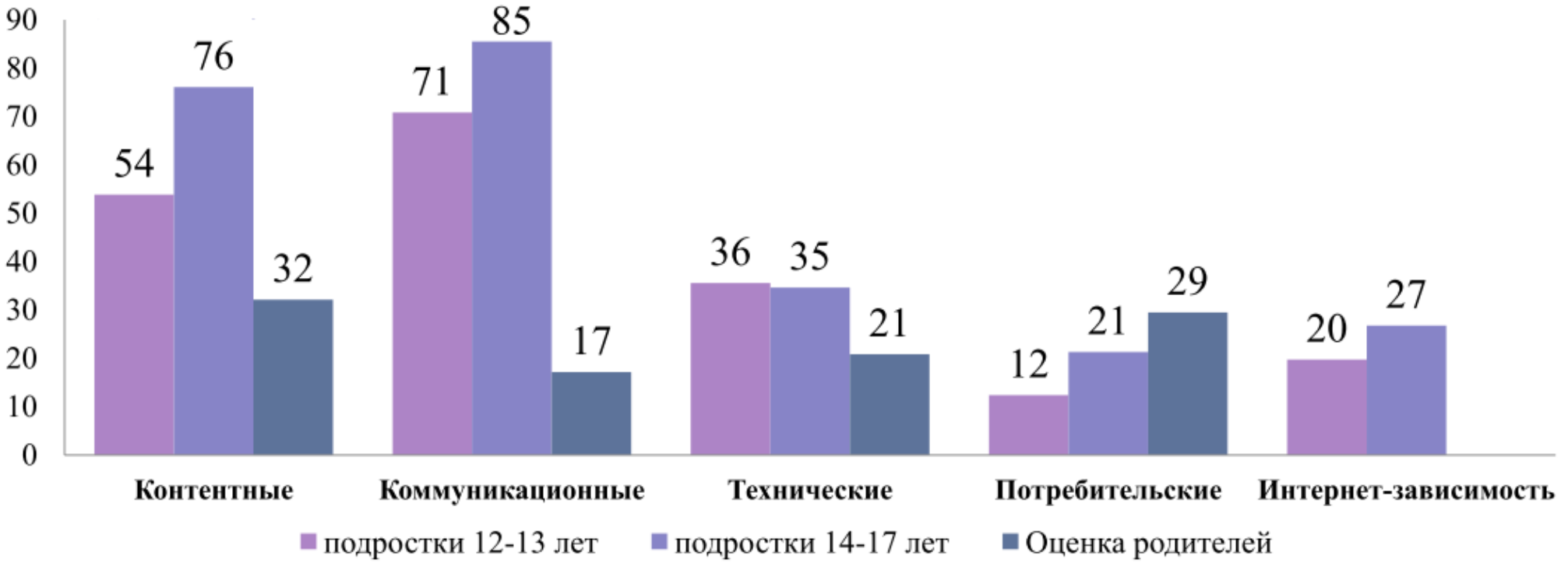
Коммуникационные риски. Связаны с межличностными отношениями Интернет-пользователей и включают в себя незаконные контакты (например с целью встречи), киберпреследования, кибернижения, груминг и др.

Потребительские риски . Злоупотребление правами потребителя: риск приобретения товара низкого качества, подделок, контрафактной и фальсифицированной продукции, хищение денежных средств злоумышленником через онлайн-банкинг и т.д.

Технические риски. Возможность повреждения ПО, информации, нарушение ее конфиденциальности или взлома аккаунта, хищения паролей и персональной информации злоумышленниками посредством вредоносного ПО и др. угроз.

Интернет-зависимость. Непреодолимая тяга к чрезмерному использованию Интернета. В подростковой среде проявляется в форме увлечения видео-играми, навязчивой потребности к общению в чатах, круглосуточном просмотре фильмов и сериалов в Сети.

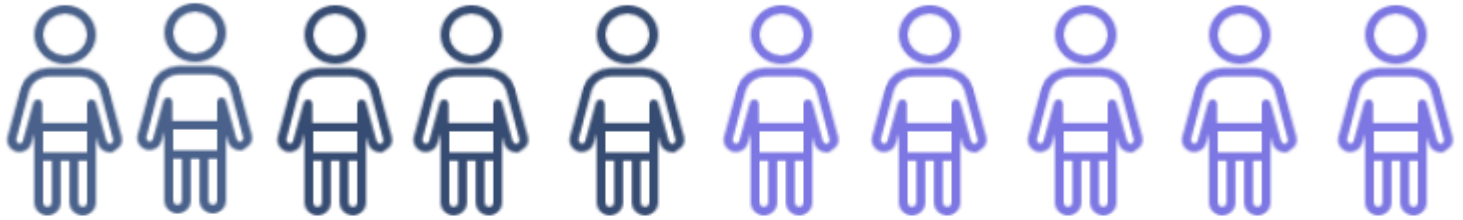
Столкновение с различными видами рисков,



Среди онлайн-рисков наиболее распространенными стали коммуникационные риски. На втором месте – контентные. Каждый третий подросток сталкивался с техническими рисками. Каждый пятый старший подросток – с потребительскими. У пятой части подростков наблюдаются признаки интернет-зависимости. Родители значительно недооценивают опыт подростков в столкновении с коммуникационными и контентными рисками и переоценивают столкновение с потребительскими.

Столкновение с ситуациями в сети, которые расстраивают или беспокоят

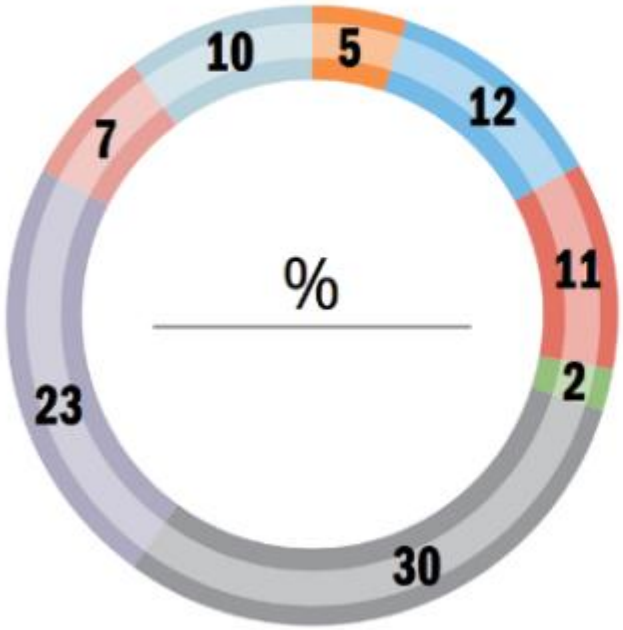
Каждый второй подросток признается, что сталкивался с такими ситуациями за последний год



Только **каждый третий** родитель считает, что его ребенок сталкивался с такими ситуациями за последний год

~80% детей от 4 до 6 лет пользуются сетью Интернет

Ответы подростков 12-17 лет на вопрос: "Что ты будешь делать, если незнакомец из Сети предлагает тебе встречу?"

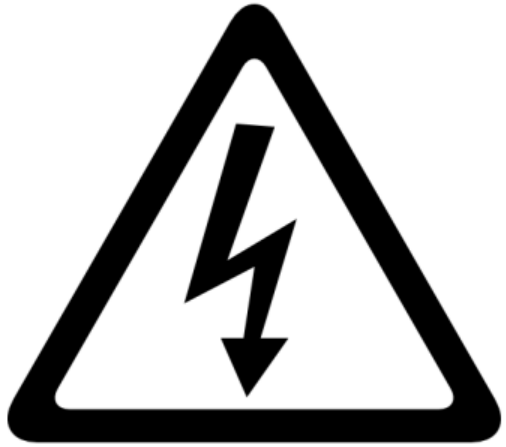


- Никому не скажу и пойду на встречу один
- Расскажу об этом друзьям и пойду на встречу один
- Расскажу об этом родителям и пойду на встречу один
- Пойду на встречу с родителями
- Пойду на встречу с другом
- Откажусь и не пойду на встречу
- Откажусь и удалю его из списка друзей
- Затрудняюсь ответить

Возможные показатели психологического неблагополучия вследствие столкновения с онлайн-рисками

- Отрицательные эмоциональные переживания
- Психологический стресс
- Развитие девиантного поведения
- Деформация морально-нравственной основы поведения
- Деформация эмоционально-волевой сферы
- Проблемы с формированием идентичности
- Негативное влияние на психосексуальное развитие
- Социальная изоляция
- Развитие интернет-зависимого поведения

Контентные риски



Столкновение с различными видами негативных и противоправных материалов
Вредоносная и потенциально опасная информация (насилие, агрессия, жестокость, порнография, ненавистничество, нецензурная лексика, межнациональная ненависть, пропаганда анероксии, булимии, суицида, азартных игр, наркотиков….)

ГДЕ?

Соцсети, блоги, торрент-сайты, персональные сайты, видеохостинги…

Виды деструктивного контента

Неэтичный

- агрессивные онлайн-игры;
- пропаганда аутодеструктивного поведения (селфхарм, булимия, анорексия, употребление алкоголя и табака);
- порнография
- оскорбления, использование нецензурных выражений;
- манипулирование сознанием и действиями отдельных людей и групп.

Незаконный

- информация о производстве, распространении, хранении и употреблении наркотических средств;
- детская порнография;
- разжигание расовой, межнациональной или религиозной ненависти (терроризм, экстремизм, национализм и др.);
- ненависть и агрессивные высказывания или призывы к действиям по отношению к конкретной группе.

Неэтичный контент может граничить с незаконным.

Столкновение с деструктивным контентом

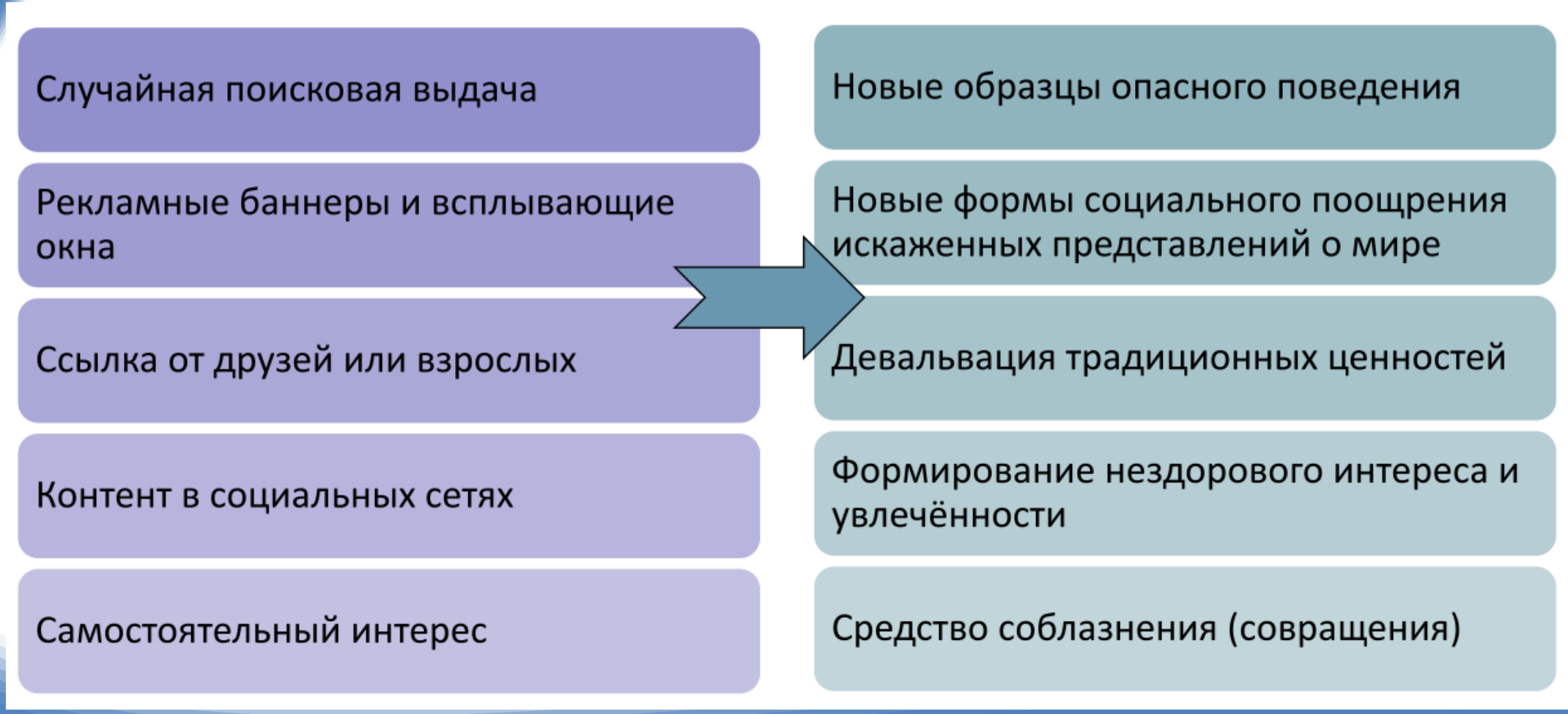
93%	**Фейковая информация**
90%	**Оскорбительный контент**
82%	**Картинки или видео с насилием и жестокостью**
73%	Информация о способах причинения себе физического вреда или боли
72%	Призыв к несанкционированным действиям
72%	Информация о способах употребления или распространения наркотиков и психоактивных веществ
68%	Пропаганда экстремизма и терроризма
37%	Информация о способах совершения самоубийства

Наиболее распространённый деструктивный контент в сети — это фейковая информация и оскорбительный контент.

Контентно-коммуникационные риски смешанной реальности

- Рекрутинг в экстремистские сообщества и распространение радикальных идей.
- Колумбайн или «школьный шутинг».
- Пропаганда употребления психоактивных веществ.
- Рекрутинг в наркокурьеры.
- Распространение фейковой информации.
- Риски, связанные с неосторожным обращением с персональными данными в процессе обмена контентом и коммуникации.
- Обмен детьми личными данными с незнакомыми пользователями, встречи с ними без информирования взрослых.

Как дети сталкиваются с негативным контентом и как он влияет на них



Наиболее опасные деструктивные тенденции

«Убивая людей, я делаю правильно!»

Разнузданная реклама психоактивных веществ

Формирование моды на «психические расстройства», на ЛГБТ-тематику, треш и шок-контент и т.д.

Рост объема депрессивно-суицидального контента и числа подписчиков на такие паблики

Популяризация в молодежной среде немотивированной агрессии и ненависти к людям/обществу в целом

Омоложение деструктивных сообществ, вовлечение в них лиц младшего подросткового и детского возраста

Как защитить детей от негативного контента

- Единый реестр запрещённых сайтов
- «Белые списки»
- Контентная фильтрация на уровне провайдера
- Программы «родительского контроля»
- Настройки браузера (детский режим)
- Настройки на сайтах (например, безопасный поиск)
- Доверительные отношения с ребёнком
- ПОВЫШЕНИЕ ЦИФРОВОЙ КОМПЕТЕНТНОСТИ

Коммуникационные риски

Киберагрессия

- Флейминг
- Хейтинг
- Троллинг
- Киберсталкинг
- Кибербуллинг
- Шейминг

Кибернасилие

- Онлайн-груминг
- Порноместь
- Секс-шантаж
- Доксинг
- Домогательства

– Секстинг

– Знакомства и встречи с онлайн-знакомыми

Шерентинг

Агрессия в сети – наиболее распространённый коммуникационный риск

Наиболее распространенным коммуникационным риском стала агрессивная коммуникация.
Младшие подростки сталкиваются с коммуникационными рисками реже старших.
Каждый второй старший подросток становится свидетелем или участником ситуации с элементами киберагрессии.

Киберагрессия

1. • Киберагрессия – нередко продолжение офлайн-агрессии. По распространенности она уступает агрессии в школе.
2. • Основные причины, почему предпочитают агрессию в онлайн, а не офлайн: **анонимность, безнаказанность, простота и скорость,** а также **невидимость реакции жертвы**
3. • **Внешность, личностные особенности и особенности здоровья и развития** – лидируют в качестве поводов для киберагрессии у всех поколений.
4. • Человек **сильнее переживает** неприятные, болезненные или враждебные ситуации **в реальной жизни** по сравнению с онлайн
5. • **Публичность киберагрессии:** мало жертв и агрессоров, много наблюдателей или свидетелей.

Виды киберагрессии (в интернете)

ФЛЕЙМИНГ – разжигание спора, публичные оскорбления и эмоциональный обмен репликами в интернете между участниками в равных позициях.

ТРОЛЛИНГ – размещение в интернете провокационных сообщений с целью вызвать негативную эмоциональную реакцию или конфликты между участниками.

ХЕЙТИНГ – негативные комментарии и сообщения, иррациональная критика в адрес конкретного человека или явления, часто без обоснования своей позиции.

ШЕЙМИНГ — публичное унижение или пристыжение человека или группы лиц в сети.

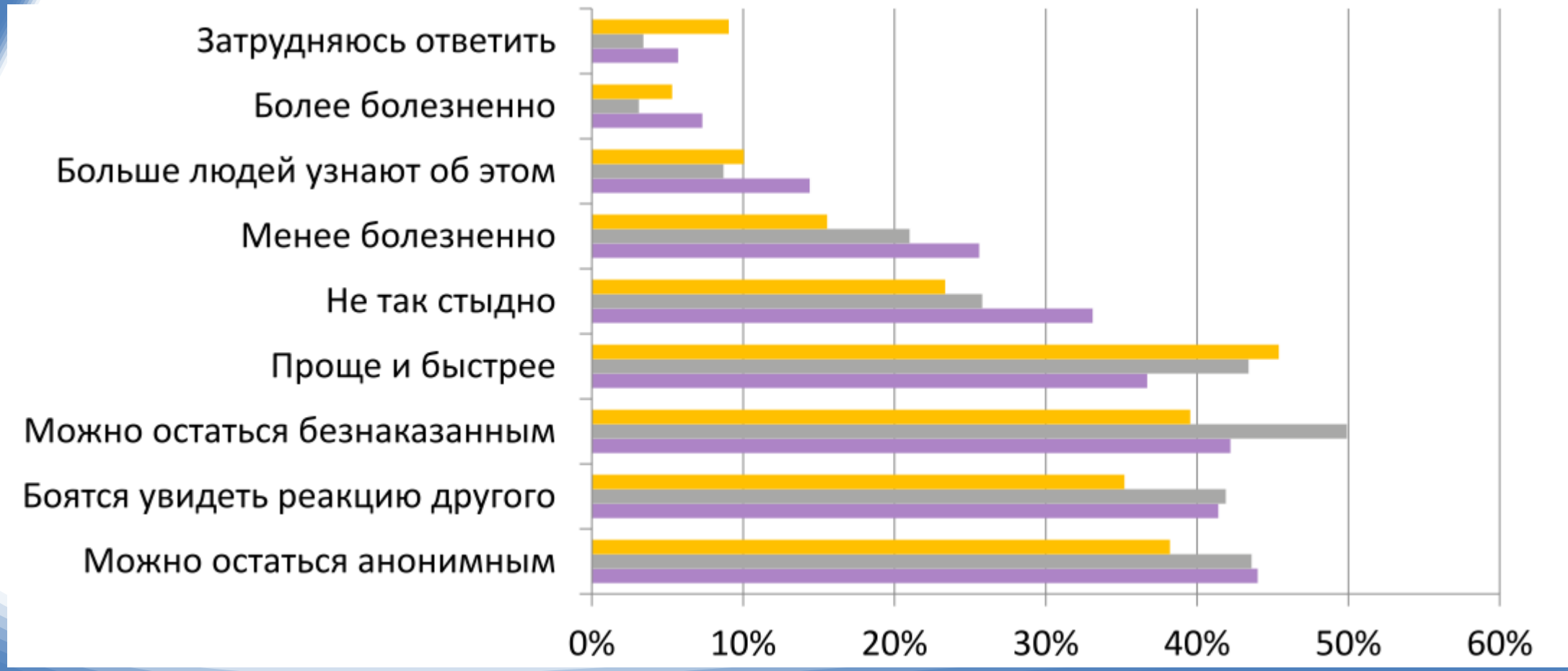
КИБЕРСТАЛКИНГ – использование электронных средств для преследования жертвы через повторяющиеся сообщения, вызывающие тревогу и раздражение.

КИБЕРБУЛЛИНГ - агрессивные, умышленные, продолжительные во времени действия, совершаемые группой лиц или одним лицом с использованием электронных форм контакта и повторяющееся неоднократно в отношении жертвы, которой трудно защитить себя.

В ситуациях киберагрессии подростки чаще наблюдатели

Наиболее распространенная роль в ситуации столкновения с киберагрессией – наблюдатель. Вторая по распространенности роль – поддерживающий жертву. 9 % подростков оказывались жертвами в ситуациях киберагрессии. Наиболее редко в сети подростки оказываются агрессорами или их поддерживающими, их насчитываются единицы. При условии, что каждый респондент мог выбрать несколько вариантов ответа, каждый второй не участвовал ни в какой роли в рассматриваемых ситуациях киберагрессии.

Почему предпочитают вести себя агрессивно чаще онлайн, чем оффлайн?



Булинг и кибербулинг – общие характеристики

Буллинг - агрессивное поведение против сверстников, отличающееся умышленностью, повторяемостью и дисбалансом сил между агрессором и жертвой (Д. Ольвеус)

Кибербуллинг - агрессивное, умышленное действие, совершаемое группой лиц или одним лицом с использованием электронных форм контакта, повторяющееся неоднократно и продолжительное во времени в отношении жертвы, которой трудно защитить себя (Г.В. Солдатова, Е.Ю. Зотова)

- Преднамеренность
- Регулярность
- Неравенство сил
- Групповой процесс с заданной ролевой структурой (агрессор, жертва, «хамелеон», свидетели или наблюдатели)
- Не заканчивается сам по себе
- Негативное психологическое воздействие ситуации на всех участников

Особенности кибербулинга

- Анонимность и дистантность агрессора, агрессор чувствует себя менее уязвимым и ответстсвенным.
- В качестве агрессора могут выступать и знакомые, и незнакомцы.
- Не видна эмоциональная реакция жертвы.
- Возможность травли 24/7, независимости от времени и места.
- Один источник (фото, пост, …)может использоваться множество раз.
- Увеличение аудитории наблюдателей.
- Жертвой кибербулинга может стать каждый вне зависимости от статуса.
- Не оставляет физических следов, незаметность для родителей, учителей.
- Жертва скрывает факт травли.
- Кибербуллингу нельзя противостоять в одиночку

Последствия кибербулинга

ДЛЯ АГРЕССОРА

- Закрепление насилия как способа коммуникации
- Отвержение группой
- Развитие проблемного поведения (правонарушения, аддикции)
- Трудности с успеваемостью и получением образования

ДЛЯ ЖЕРТВЫ

- Социальная изоляция
- Развитие форм асоциального поведения
- Тревожные расстройства
- Депрессивные состояния
- Психосоматические симптомы (нарушение сна, плохой аппетит, головная боль и т.д.)
- Каждый второй продолжает думать об опыте школьного буллинга во взрослой жизни
- ПТСР- Посттравматическое стрессовое расстройство
- Риск суицидального поведения

Негативная психодинамика свидетелей агрессии

1. Необходимость выбора между фигурами сильного и слабого, как правило, в пользу первой
2. Диффузия личной ответственности и повторение групповых, а не выработка индивидуальных траекторий поведения
3. Ослабление чувства сострадания по причине как частоты таких ситуаций, так и по причине отсутствия непосредственного наблюдения за реакцией жертвы; блокирование механизмов восприятия многообразия как нормы.
4. Мало того, что свидетели киберагрессии в силу своего равнодушия и молчаливого согласия – главные союзники агрессора, на них также оказывается значительное негативное психологическое воздействие.

КИБЕРБУЛЛИНГ: ЧТО ДЕЛАТЬ РОДИТЕЛЯМ?

КИБЕРБУЛЛИНГ – ЭТО ТРАВЛЯ ЧЕЛОВЕКА ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ. ЗАЧАСТУЮ ОСУЩЕСТВЛЯЕТСЯ В СОЦИАЛЬНЫХ СЕТЯХ И РАСПРОСТРАНЕНА В ПОДРОСТКОВОЙ СРЕДЕ

ПРОФИЛАКТИКА:

УЧИТЕ ДОВЕРИЮ В СЕМЬЕ

Установите в семье правила доверительного общения, когда каждый из членов делится тем, что его беспокоит. Чтобы ребенок видел, быть слабым – не стыдно, и любые вещи можно обсудить с родителями. Будьте всегда открыты для ребенка.

ОБСУДИТЕ ТЕМУ С РЕБЕНКОМ

Объясните, что агрессивные сообщения в сети и клевета попадают под определения кибербуллинг. Ребенок может попросту не распознать кибербуллинг. Скажите, что вне зависимости от правдивости содержания, обидные письма – одна из его форм. Также, объясните ребенку, что не стоит публиковать в сети личную информацию о себе, которую он не хотел рассказывать всем.

УСТАНОВИТЕ НАСТРОЙКИ ПРИВАТНОСТИ

В каждой социальной сети доступен такой функционал. Например, можно запретить, чтобы вас отмечали в комментариях, постах и фотографиях (проследите, чтобы на странице ребенка такие ограничения были подключены).

РАЗВИВАЙТЕ САМОСТОЯТЕЛЬНОСТЬ РЕБЕНКА

Учите ребенка защищать себя. Согласно исследованиям, дети, оказывающиеся в роли жертв, зачастую сильно привязаны к кому-то из родителей. Поэтому гиперопека способствует тому, что в будущем ребенок может превратиться в жертву. Покажите, что можно вести себя по-другому.

РАЗВИВАЙТЕ У РЕБЕНКА УМЕНИЕ ПОНИМАТЬ ЭМОЦИИ

Если родители учат ребенка понимать, признавать и уважать собственные эмоции, не обращая внимания на устойчивые гендерные предрассудки, то шанс стать жертвой или агрессором у ребенка снижается.

РЕАГИРОВАНИЕ:

ПОДДЕРЖИТЕ РЕБЕНКА

Если ребенок поделился проблемой, не ругайте его, примите ситуацию и дайте понять, что вы на его стороне. Похвалите ребенка за высказанное, узнайте его чувства. Не стоит придерживаться принципа «если не обращать внимания на обидчиков, то они сами отстанут» – нужно выяснить все обстоятельства.

СОХРАНИТЕ УЛИКИ

Сохраняйте доказательства кибербуллинга – все сообщения, картинки и другую оскорбительную информацию, полученную ребенком в виде скриншотов. Эту информацию следует передать в полицию.

РАЗРАБОТАЙТЕ СТРАТЕГИЮ РЕАГИРОВАНИЯ

Объясните ребенку, что не надо отвечать на получаемые оскорбления, это может еще больше активизировать агрессора. Лучше добавить обидчика в «черный список» в сети. Также, сообщите о факте кибербуллинга провайдерам услуг (администрации социальной сети).

ОБРАТИТЕСЬ К КЛАССНОМУ РУКОВОДИТЕЛЮ

Разговор с классным руководителем поможет понять, в курсе ли он сложившейся ситуации и как собирается действовать. Проверьте, есть ли какие-то механизмы на уровне школы, которые должны срабатывать при возникновении травли (служба медиации, иные механизмы).

ОБРАТИТЕСЬ К СПЕЦИАЛИСТУ

Работа с психологом, социальным педагогом или советы других взрослых, которым ребенок доверяет, улучшит ситуацию и поднимет уровень поддержки в глазах ребенка.

Шерентинг – новые практики цифрового родительства или новая зона риска?

Приобретает значение вопрос о распространении персональных данных в сети без ведома детей и подростков. Каждый четвёртый подросток отмечает, что кто-то из родителей опубликовал в интернете
информацию о нём без его согласия, а каждый пятый просил удалить эту информацию.

Не только шерентинг

Травмирующие цифровые следы

«Стратегия комплексной безопасности детей на период до 2027 г.»

«Защита детского населения от деструктивного информационно-психологического воздействия».

Участились случаи вооруженных нападений подростков и молодых людей (вчерашних выпускников школ) на образовательные учреждения

Наблюдается гиперподключенность школьников к сетям

Рост зависимости от цифровых технологий, пандемия ускорила эти процессы

Остро стоит проблема психологической и физической внутренней безопасности личности

Необходима системная работа по противостоянию угрозам :

- Система подготовки кадров в области кибербезопасности
- Серьезные программы по цифровой гигиене
- Работа с родителями
- Современная качественная учебно-методическая литература
- Вовлечение школьников в детско-юношеские организации, в социально значимые воспитательные практики, волонтерские проекты в добрые и полезные дела

Цифровое детство как особый исторический тип детства: культурно-исторический подход

ИКТ **изменяют** пространство жизнедеятельности ребенка и **влияют на всю структуру его деятельности как в офлайне, так и в онлайне**

Другая социальная ситуация развития современного ребенка - важнейшая координата ИКТ и, в первую очередь, интернета

Интернет не просто технологии, это – **среда обитания**, которая выступает **источником развития и фактором социализации. Зона ближайшего развития задается не только значимыми взрослыми, но и онлайн-средой.**

Интернет – культурное орудие, способствующее порождению новых форм деятельности, культурных практик, феноменов, значений и смыслов

Солдатова Г. У. Цифровая социализация в культурно-исторической парадигме: изменяющийся ребенок в изменяющемся мире // Социальная психология и общество. — 2018. — Т. 9, № 3. — С. 71–80.

Цифровая социализация

Цифровая социализация – опосредованный всеми доступными инфокоммуникационными технологиями процесс овладения и присвоения человеком социального опыта, приобретаемого в онлайн-контекстах, воспроизводства этого опыта в смешанной офлайн/онлайн реальности и формирующего его цифровую личность, как часть реальной личности

Новая нормальность: сочетание традиционной и цифровой социализации

Социализация в отличие от воспитания — это стихийный разнонаправленный процесс. В информационном обществе эта стихия опосредуется в том числе техносистемой, становящейся важнейшей частью современной культуры и частью экосистемы формирующейся личности.

Цифровая социализация позволяет учитывать множественную реальность цифрового образа жизни: восприятие и обмен информацией, коммуникацию с живыми и неживыми элементами онлайн-пространства, онлайн-потребление, а также культурные, социальные, психологические и технические аспекты использования электронных устройств

Особая уникальность подрастающего поколения заключается в том, что традиционные формы социализации все чаще соседствуют, совмещаются, вытесняются, а иногда замещаются новыми формами приобретения необходимых знаний и навыков — цифровой социализацией.

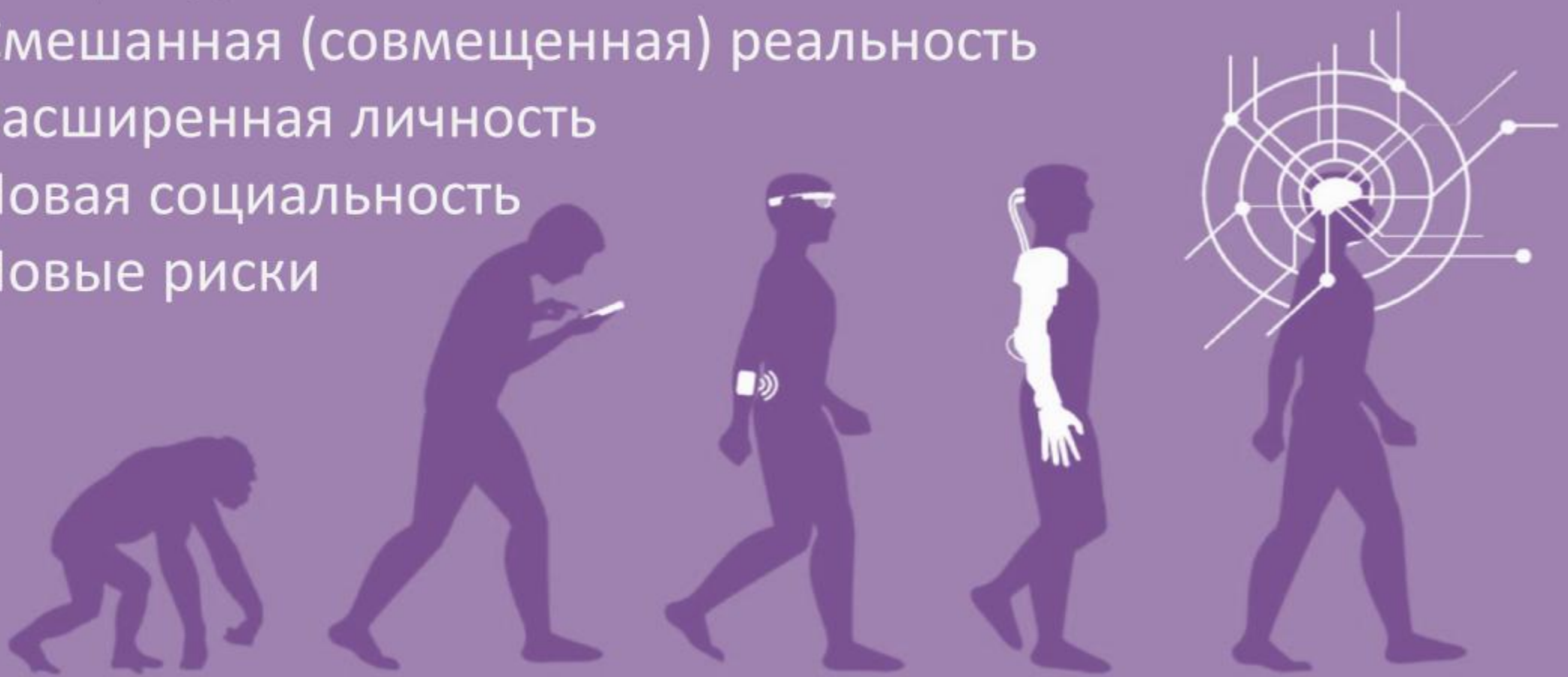
Цифровая социализация – важная часть процесса формирования личности, ее адаптации и интеграции в социальную систему информационного общества

Солдатова Г. У. Цифровая социализация в культурно-исторической парадигме: изменяющийся ребенок в изменяющемся мире // Социальная психология и общество. — 2018. — Т. 9, № 3. — С. 71–80.

Главный гуманитарный вызов XXI века: изменяющийся ребенок в изменяющемся мире

Цифровые измерения новой нормальности

- Гиперподключенность
- Смешанная (совмещенная) реальность
- Расширенная личность
- Новая социальность
- Новые риски

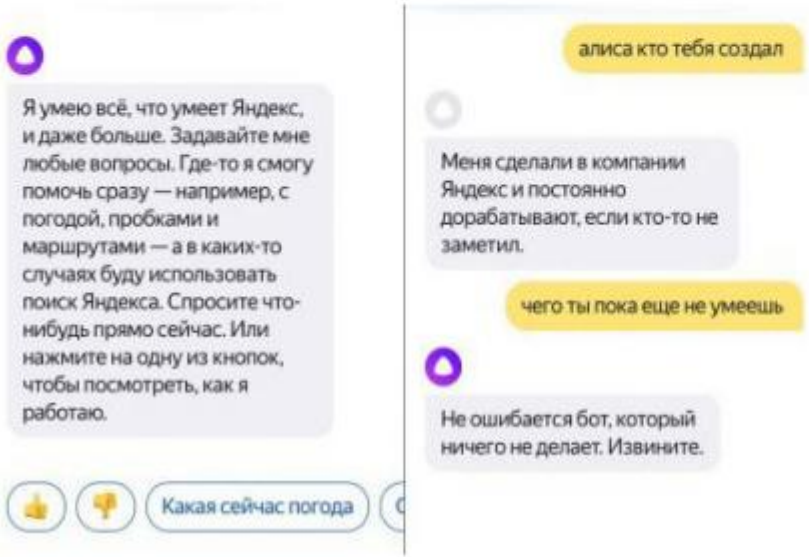


Можем ли мы говорить сегодня только о двух мирах современного ребёнка?

Реальный мир

Онлайн-мир

Множественная реальность



Множественная реальность

Смешанная реальность

Новая смешанная реальность диктует необходимость усвоения новых норм и правил взаимодействия с ней, а также технологий, с помощью которых возможна реализация этого взаимодействия.

Анонимность, предельная открытость, компенсаторность, рекреационность, возможность реализации альтернативных идентичностей, столь привлекательные для первых пользователей социальных сетей, сменяются ответственным авторским контентом, стремлением к обозначению и соблюдению границ своей приватности и других обитателей Сети, выполнением этических норм и правил экологичного взаимодействия (Мороз, 2017).

Риски и безопасность смешанной реальности

В последние годы на первый план в сфере безопасности выходят коммуникационные риски (киберагрессия, злоупотребление персональными данными, опасный и незаконный контент), которые нельзя отнести только к онлайну, они представляют собой продукт смешанной реальности

Контентные риски, вредоносные программы, как специфические для интернета, отходят на второй план. Появляется новая группа онлайн-рисков - распространение личной информации ближайшим окружением

Взгляд на безопасность вновь требует коррекции: нет отдельно безопасности жизнедеятельности и отдельно онлайн-безопасности — есть вопросы безопасности в смешанной реальности

Цифровая компетентность – главный навык XXI века

Цифровая компетентность - готовность и способность личности применять инфокоммуникационные технологии уверенно, эффективно, критично и безопасно в разных сферах жизнедеятельности (информационная среда, коммуникации, потребление, техносфера) на основе овладения соответствующими компетенциями, как системой знаний, умений, ответственности и мотивации.

Солдатова Г. У. Нестик, Т. А., Рассказова, Е. И., Зотова, Е. Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования //М.: Фонд Развития Интернет. – 2013.

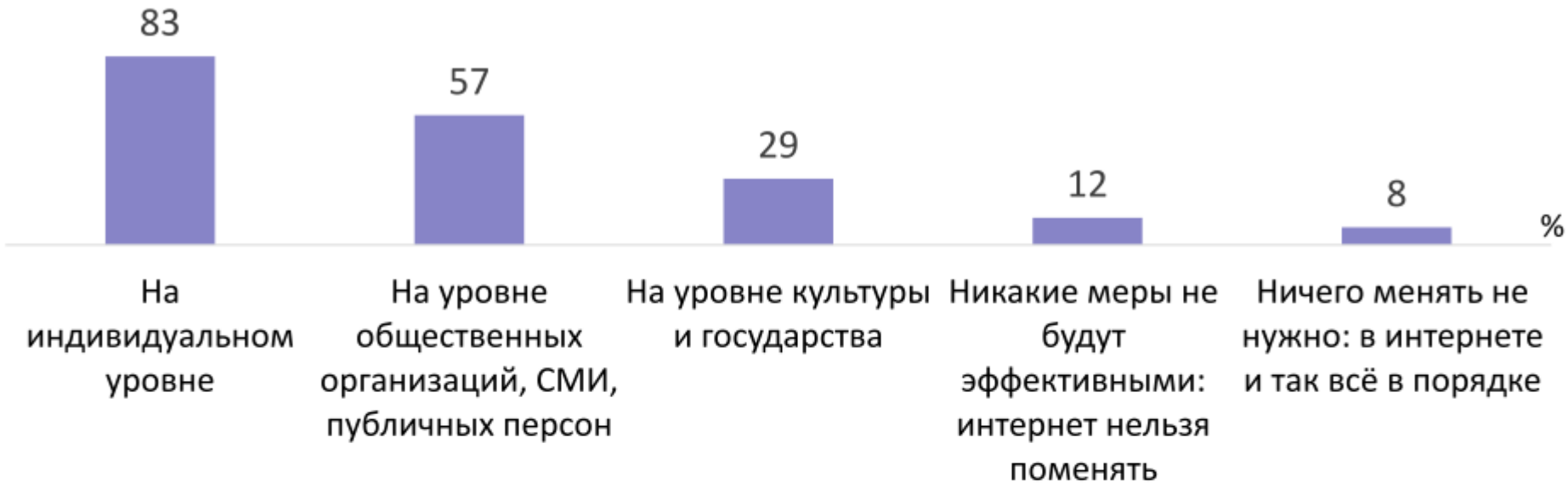
Иллюзия цифровой компетентности

Современные школьники не обладают высоким уровнем цифровой компетентности!
Иллюзорность – искажение оценки своих конкретных знаний и навыков; «перенос» действительных знаний в другие сферы.

Педагоги могут стать проводниками в мир интернета и технологий

- «Цифровой разрыв» между учениками и учителями существенно меньше, чем между родителями и детьми.
- Уверенными пользователя себя называют более 75% учителей. За уверенностью стоят реальные ИКТ-компетенции.
- Подавляющее число педагогов научились пользоваться интернетом самостоятельно (82,5%).

Как повысить уровень цифровой культуры в интернете?



Большинство считают, что повысить уровень цифровой культуры возможно, и сделать это необходимо на индивидуальном уровне (82%) с помощью воспитания в семье (52%) и работы над собой (44%)

Подростки и молодёжь называют родительскую медиацию одним из ключевых факторов.

- 52 % — Воспитание в семье и в образовательных организациях
- 44 % — Работа над собой и личностное развитие
- 31 % — Введение в школах обязательного предмета по цифровой грамотности

Цифровизация школы

Уже с первого класса школьники взаимодействуют с цифровыми устройствами (интерактивные доски, онлайн-уроки)

Возраст начала использования детьми интернета и цифровых устройств постоянно снижается

Однако овладение технологиями чаще происходит стихийно

Важно, чтобы это происходило не бесконтрольным (полевым) путём, а было структурированным и направленным.

Группы информации, охраняемые законом

- Персональные сведения, касающиеся учащихся и преподавателей, оцифрованные архивы.
- Инновационные педагогические и образовательные ресурсы, носящие характер интеллектуальной собственности и защищённые законом.
- Структурированная учебная информация, обеспечивающая образовательный процесс (***библиотеки***, базы данных, обучающие программы).

Изменения в законодательстве

Изменения вступили в силу с **1 марта 2021 г. (ФЗ №519)**
Введение понятия «персональные данные, ***разрешённые субъектом для распространения***» (ранее – «сделанные общедоступными субъектом»)
– это персональные данные, к которым ***предоставлен доступ*** неограниченного круга лиц ***путём дачи соответствующего согласия***.

ФЗ «О персональных данных» от 27.07.2006 №152
(последняя редакция от 30.12.2022)

Категории персональных данных

Общие: фамилия, имя, отчество (при наличии), год, месяц рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, другая информация, относящаяся к субъекту.

Специальные: расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь, сведения о судимости.

Биометрические: ДНК, радужная оболочка глаз, дактилоскопическая информация, цветное фотографическое изображение лица, голос, фотоизображение рисунка вен ладони, иные сведения.

Особенности обработки персональных данных

- Согласие ***оформляется отдельно*** от иных согласий. Требования определены ***Роскомнадзором*** (с 01.07.2021 г. согласие предоставлено с использованием специализированной информационной системы Роскомнадзора).
- Молчание и бездействие субъекта не может считаться согласием на обработку данных.
- Субъект вправе определить категории и перечень персональных данных, условий и запретов для обработки.

Согласие на обработку персональных данных должно включать

- Фамилию, имя, отчество субъекта и его контактную информацию.
- Наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта.
- Цель обработки персональных данных.
- Категории и перечень персональных данных, на обработку которых даётся согласие.
- Категории и перечень персональных данных, для обработки которых субъект устанавливает условия и запреты, перечень устанавливаемых условий и запретов.
- Срок, в течение которого действует согласие.
- Сведения об информационных ресурсах оператора, посредством которых будет осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта.

Документы в сфере обеспечения информационной безопасности

- Положение о работе в сети Интернет в ОО.
- Положение о системе контентной фильтрации (СКФ) ресурсов сети Интернет.
- Правила пользования ресурсов сети Интернет.
- Программа информатизации 2020 – 2025 гг.
- Список разрешённых и проверенных сайтов (регулярно актуализировать информацию).
- Список запрещённых сайтов (всё время пополняется).

Условия обеспечения информационной безопасности обучающихся

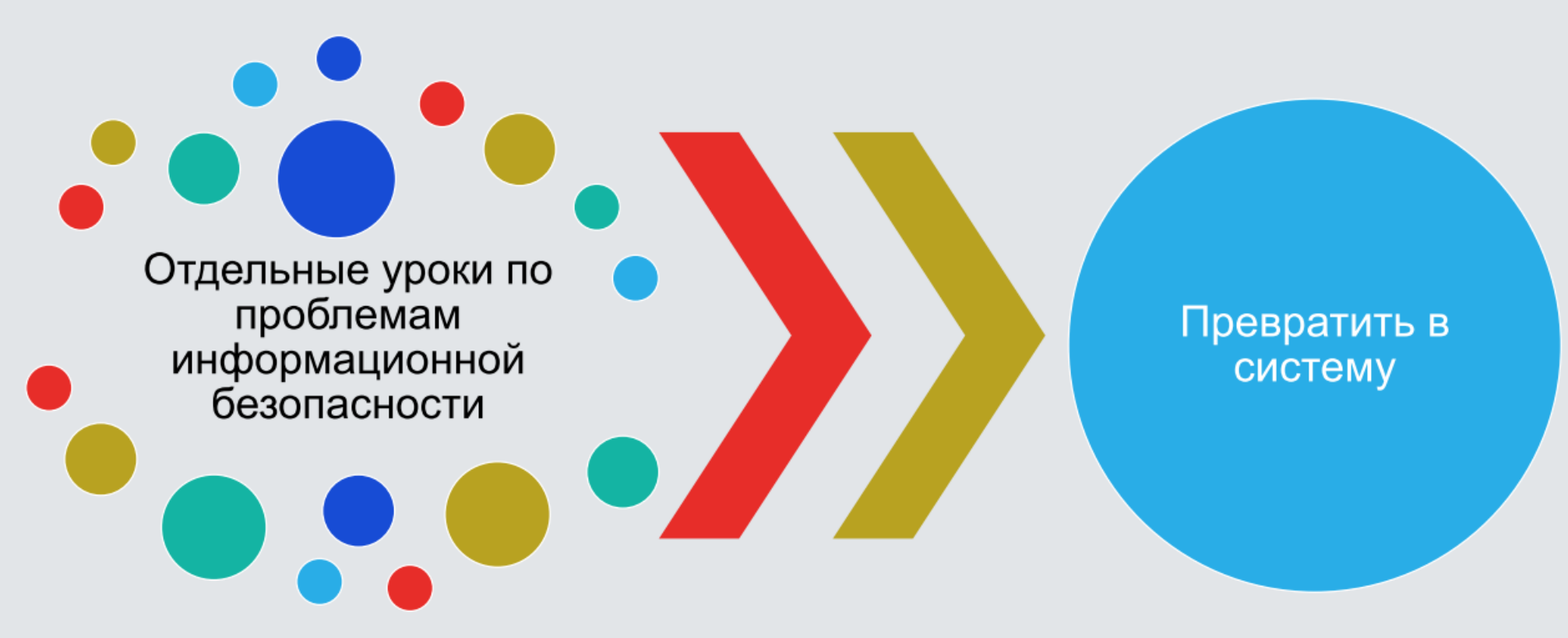
- Осознание важности обеспечения информационной безопасности.
- Создание и постоянное совершенствование методической работы в школе в сфере обеспечения информационной безопасности.
- Привлечение к работе специалистов в вопросах обеспечения информационной безопасности.
- Формирование творческих групп из разновозрастных участников (привлечение увлечённых творческих педагогов, школьников и родителей).
- Создание атмосферы творчества и конструктивного сотрудничества.

Цифровая образовательная система школы

Формирование цифровой грамотности как социальной характеристики личности

- Формирование понятийного аппарата (тезауруса).
- Формирование ценностного отношения к информационным продуктам, цифровым объектам и деятельности в интернете.
- Владение культурой поведения в сети Интернет.

Преобразование содержания



Модели внедрения курса «Информационная безопасность»

- Учебный курс «Информационная безопасность» по выбору школы в вариативной части учебного плана.
- Учебный курс во внеурочной деятельности.
- Тематические разделы и модули курса при изучении школьных предметов: ОБЖ, информатика, технология, обществознание.
- Классные часы.
- Родительские собрания.
- Участие в акциях, конкурсах и т.п.

Учебники по курсу «Информационная безопасность»

Порядковый номер учебника	Наименование учебника	Автор (авторский коллектив)	Класс	Наименование издательства
1.1.1.3.2.3.1	Информационная безопасность. Правила безопасного Интернета.	Цветкова М.С., Якушина Е.В.	2-4	«Издательство «Просвещение»
1.1.2.4.4.6.1	Информационная безопасность. Безопасное поведение в сети Интернет.	Цветкова М.С., Якушина Е.В.	5–6	«Издательство «Просвещение»
1.1.2.4.4.6.2	Информационная безопасность. Кибербезопасность.	Цветкова М.С., Хлобыстова И.Ю	7–9	«Издательство «Просвещение»
1.1.3.4.2.12.1	Информационная безопасность. Правовые основы информационной безопасности	Цветкова М.С.; под редакцией Цветковой М.С.	10–11	«Издательство «Просвещение»

https://fpu.edu.ru/textbook/53

М.С. Цветкова «Информационная безопасность. 2-11 классы. Методическое пособие для учителя» https://lbz.ru/metodist/authors/ib/ib-mp-tsvetkova.pdf

УМК ПО ФОРМИРОВАНИЮ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «КИБЕРБЕЗОПАСНОСТЬ»

Галина Солдатова – член-корреспондент РАО, профессор МГУ им. М.В. Ломоносова. Главный редактор журнала «Дети в информационном обществе». Лауреат Премии Российской Федерации в области образования. Автор около 250 публикаций. Директор Фонда «Развития Интернет»

Учебные пособия по курсу информационной безопасности (5-9 класс)

Методические рекомендации курса по культуре поведения в информационном пространстве

УМК «Кибербезопасность» учит школьников и их родителей правильно ориентироваться в мире цифровых технологий

Курс Кибербезопасность. 5-9 классы (под ред. Г.У. Солдатовой, издательство «Русское слово»)

Цель – повышение цифровой компетентности школьников и расширение возможностей полезного, критичного, ответственного и безопасного использования Интернета.

- расширение представлений о возможностях использования цифровых технологий
- расширение представлений о возможностях Интернета как источника информации
- знакомство с онлайн-рисками и формирование стратегий их предотвращения
- помощь в осознании влияния цифровых технологий на образ жизни
- формирование критического мышления

Курс Кибербезопасность. 5-9 классы (под ред. Г.У. Солдатовой, издательство «Русское слово»)

Занятия – аудиторная и самостоятельная работа.

Тематический модуль –

Вступительная лекционная часть (сам учитель + методические рекомендации + источники)

Учебные пособия – тренажёры.

Задания рассчитаны на разные формы работы – индивидуальную, в парах, в малых и больших группах. При работе в тетрадях предполагается использование цифровых устройств и интерактивных форм деятельности.

Мероприятия по формированию ответственного и безопасного поведения

- 2 классы. Классный час «Правила этикета в интернете».
- 3 классы. Урок-игра «Путешествие по Всемирной паутине».
- 4 классы. Брейн-ринг «Цифровая безопасность».
- 5 классы. Классный час «Урок медиабезопасности».
- 6 классы. Родительское собрание «Безопасность в виртуальном мире. Что могут сделать взрослые».
- 7 классы. Урок-квест «Как защититься от интернет-угроз».
- 7-8 классы. Классный час «Кибербулинг или виртуальное издевательство».
- 8 классы. Классный час «Кибербезопасность в социальных сетях».
- 8 классы. Дебаты «Социальные сети – зло или благо».
- 9-10 классы. Урок-квест «Актуальные проблемы безопасного интернета».
- Участие во Всероссийском онлайн-чемпионате «Изучи Интернет-управляй им!» (при поддержке компании «Ростелеком»)
- Участие во Всероссийском проекте «Информационная культура и безопасность» с проектом «Моя безопасная школа»
- и т.п.

Классные часы

- Правила поведения в цифровом пространстве
- Личное и публичное
- Социальные сети
- Кибербулинг

Уроки технологии

- Блок «Социальные технологии»
- Помощь бабушкам и дедушкам в освоении информационного пространства
- Занятия с младшими братьями и сёстрами «Будь осторожен, малыш!»
- Волонтёрское движение «Цифровые помощники»
- Проведение опросов, интервью

Проектная деятельность (9 – 11 классы)

- Большие данные
- Исследования поведения людей
- Социальные сети

Волонтёрская деятельность – основная школа для начальной

- Обучающие игры
- Проведение классных часов
- Исследование моделей поведения в цифровом пространстве

Медиаволонтёрство

Информационно-медийное направление волонтёрской деятельности – актуальный ресурс для гражданского воспитания школьников

направленно на формирование информационного поля вокруг общественно значимых событий социальных проектов

оказывает информационную поддержку социальным проектам, инициирует проведение полезных, добрых дел, разрабатывает контент и распространяет его в СМИ и социальных сетях

медиаволонтёры на добровольных началах выступают в качестве фотографов, журналистов, SMM-специалистов, блогеров, видеооператоров, дизайнеров и т.д.

УМК «Дорогою добра» (авт. Х.Заладина, И.Шульгина)

КАК направит энергию детей в позитивное русло? Как научить подростков критически мыслить?

КАК мотивировать детей на социальную активность?

КАК объединить подростков вокруг интересной идеи или социального проекта?

КАК нейтрализовать негативный контент среды?

УМК «Дорогою добра» (авт. Х.Загладина, И.Шульгина)

Курс по развитию добровольчества поможет формированию важных качеств, необходимых для работы в команде: коммуникативность, ответственность, инициативность и т.д.
Дети получат знания об истории добровольчества, сведения о благотворительности, меценатстве, филантропии, узнают как реализовать добровольческие проекты.

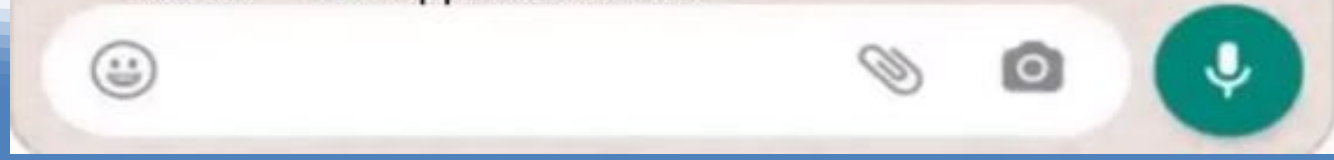
Мессенджер (от англ. message — сообщение) — приложение или онлайн-система, позволяющие мгновенно обмениваться информацией через интернет.

В России WhatsApp входит в тройку самых популярных мессенджеров — вместе с Telegram и Viber. Занимает 1е место по использованию.

Возможности и удобство мессенджеров:

✓ мгновенная отправка текстовых сообщений,
✓отправка фото, аудио, видео,
✓отправка документов,
✓поделиться геолокацией,
✓создавать публичные каналы и обсуждения (чаты),
✓анимированная передача эмоций,
✓наличие web-версии (компьютерной);

✓отсутствие оплаты (достаточно wi-fi или мобильного интернета),
✓мгновенное подтверждение доставки/прочтения, в том числе в групповых чатах – «всегда на связи».



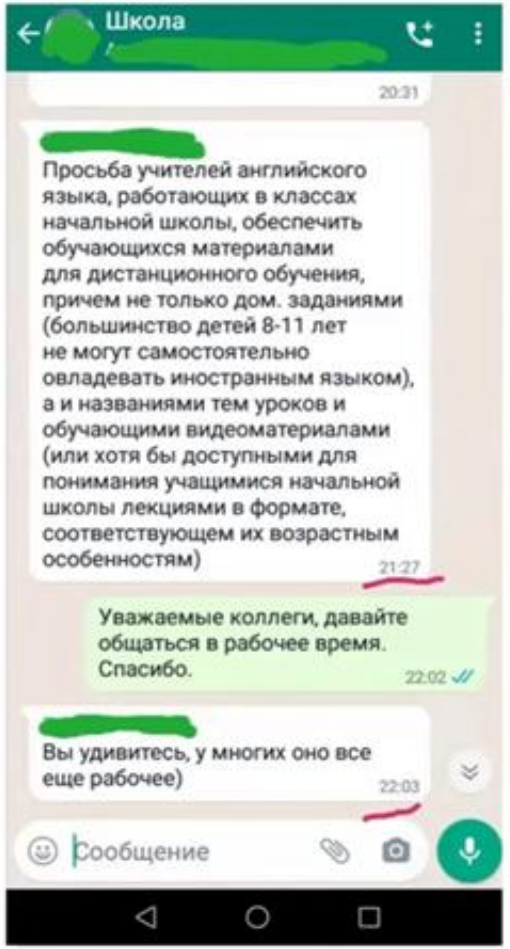
Обилие мессенджеров + других информационных каналов: WhatsApp, Telegram, Viber и др. + электронная почта, соцсети, телефон.

Обилие чатов в мессенджерах (на примере педагогов):

Обилие не соответствующей содержанию чата информации, спам:

- ✓видео- «приколы»
- ✓поздравления-картинки, поздравления-ролики
- ✓обсуждение личных вопросов
- ✓«реклама»
- ✓изобилие слов-подтверждений (понял, принял, ок - от всех участников чата)
- ✓предоставление излишней информации (демонстрация активности/непонимание правил и целей чата)

Неструктурированность времени получения сообщений, а также их выход за рамки рабочего времени («всегда на связи»)



Стресс - особое психическое состояние, проявляющееся в психологических и поведенческих реакциях, которые отражают внутреннее беспокойство или его подавление (N.H. Rizvi). Стресс является своеобразной формой отражения субъектом сложной ситуации, в которой он находится.

Информационный стресс - состояние, формирующееся под воздействием экстремальных (сложных) значений информационных факторов (В.А. Бодров).

Факторы информационного стресса

Факторы информационного стресса и их проявление при общении в чатах:

- неопределенность ситуации (непредсказуемость развития ситуации, ощущение отсутствия контроля за ситуацией) – *сообщение с новой задачей может придти в любой момент;*
- дефекты информационных потоков (противоречивость информации, дефицит информации, избыточность и большой объем информации) – *разнообразная неструктурированная информация (рабочая и личная), дефицит информации по задаче;*
- фактор сложности (высокая субъективная сложность задачи, частичный или полный неуспех в деятельности, большая длительность воздействия учебной/рабочей нагрузки) – *дефекты постановки задач коммуникатором;*
- фактор дефицита времени (дефицит времени, высокий темп предъявления информации) – *нехватка времени на выполнение, позднее прочтение, санкции.*

Эмоциональные признаки информационной перегрузки:

- опустошенность, усталость,
- напряжение, беспокойство,
- страх от негативных новостей,
- страх не успеть вовремя выполнить поручение/задание,
- страх пропустить важное и «быть в отстающих»,
- просматривание чатов как навязчивость.

Признаки стресса на поведенческом уровне: рассеянность, забывчивость; безразличие к поведению окружающих людей; затруднения сосредоточиться на важных вещах; невозможность объективно оценивать себя и окружающих; тяга к вредным привычкам; скованность движений. В условиях информационного перенапряжения трудно сконцентрироваться и принять правильное решение.

Причины неэффективности и «стрессовости» чата:

✓отсутствие модератора/руководителя чата, его пассивность в управлении групповыми процессами в чате

✓отсутствие оговоренных правил общения в чате

✓низкая компетентность коммуникаторов в области деловой переписки. Частые ошибки:

– большой объем сообщений,

- отсутствие структуры,

- изобилие интонационных знаков («срочно всем!!!!!!», «когда????») как проявление неконтролируемых эмоций

- отправка голосовых сообщений в общий чат,

- временная непоследовательность и выход за рамки рабочего времени

✓отсутствие контроля эффектов «коллективного распределения ответственности», «социальной лености», эффекта «невидимки»

Этикет в мессенджерах

Связывайтесь по рабочим вопросам

С 9:00 до 19:00

Связывайтесь по личным вопросам

С 12:00 до 21:00
в крупных городах

С 12:00 до 20:00
в маленьких городах

Убедитесь, что ваш вопрос стоит чужого времени

Здоровайтесь, начиная переписку

Обращайтесь к собеседнику по имени

Пишите без ошибок

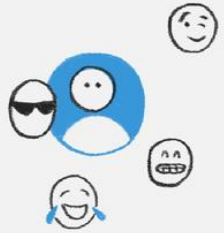
Если собеседник не отвечает, напомнить о себе можно только на следующие сутки

Не спешите
Лучше пропустить обращение, чем перепутать имя

Не пишите капслоком
Некоторые вопринимают это как крик

Не обращайтесь к незнакомым людям на "ты"
В деловой среде предложить перейти на "ты" может вышестоящий, в светской — женщина

Никогда не отправляйте голосовые сообщения
Только если собеседник не прислал их первым



Не используйте смайлики
При переписке с малознакомыми людьми

Если не можете ответить сразу
Прочитав сообщение, сообщите

Мемы
Не присылайте их в рабочее время

Не злоупотребляйте сообщениями

Не звоните без предупреждения
В соцсети и мессенджере

 ТАСС выражает благодарность Альбине Холговой, президенту Национальной ассоциации экспертов по деловой этике, этикету и протоколу, за помощь в подготовке материала.

Спасибо за внимание!

Баранова Мария Вячеславовна
старший методист
Центра информационных технологий
ГАУ ДПО ЯО ИРО
baranova@iro.yar.ru
RIBC76@yandex.ru