

**Методические рекомендации по организации и проведению
в государственных и муниципальных общеобразовательных организациях
Республики Башкортостан уроков «цифровой гигиены»**

В методических рекомендациях рассмотрен понятийно- категориальный аппарат цифровой гигиены, обозначены основные стратегии воспитания личности в условиях цифровой трансформации образования. Методические рекомендации содержат теоретическую часть, в которой даётся общее представление о цифровой гигиене, её научном аппарате.

Методические рекомендации подготовлены в соответствии со «Стратегией развития информационного общества в Российской Федерации на 2017-2030 годы», цифровой трансформацией постиндустриального общества – обозначенной как цель в «Указе Президента РФ О национальных целях развития Российской Федерации на период до 2030 года».

Методические рекомендации включают конкретные алгоритмы, направленные на обеспечение безопасности человека в информационной среде и формирование у обучающихся умений и навыков по предупреждению потенциальных угроз в гиперинформационном обществе.

Методические рекомендации предназначены для учителей общеобразовательных школ, педагогов-психологов, социальных педагогов и классных руководителей. Разработаны в целях оказания содействия учителям общеобразовательных школ в организации и проведении уроков по цифровой гигиене.

СОДЕРЖАНИЕ

1. Введение.....	3
2. Понятийно-категориальный аппарат цифровой гигиены.....	4
3. Концептуальные подходы к реализации содержания внеурочного курса «Цифровая гигиена» в современной школе.....	9
4. Специфика ценностей цифрового мира. Ценности цифрового мира.....	10
5. Психологический портрет поколения Z.....	12
6. Основные принципы воспитания в области цифровой гигиены.....	21
7. Темы уроков по цифровой гигиене в школе и методические рекомендации к их проведению.....	22
8. Заключение.....	36
9. Рекомендуемый список источников и литературы.....	40
10. Глоссарий основных понятий и терминов.....	45

1. Введение

В современном мире цифровая гигиена становится не менее важной, чем личная гигиена. Каждый день мы пользуемся множеством устройств и онлайн-сервисов, что сопровождается рисками потери данных, кражи личной информации и иных угроз.

Цифровая гигиена включает в себя набор мер по защите устройств, информации и данных от различных угроз.

Цифровая революция полностью изменила мир, в котором мы живем. От взаимодействия с социальными сетями до работы с массивами данных – цифровая среда охватила все аспекты нашей жизни. От взаимодействия с социальными сетями до работы с массивами данных – цифровая среда охватила все аспекты нашей жизни. Особое значение она приобретает для подрастающего поколения, которое практически с первых лет своей жизни сталкивается с интернетом и электронными устройствами. Однако вместе с преимуществами цифровизации и доступности знаний встает новая серьёзная проблема: способность критически воспринимать информацию и защищать себя от негативных последствий онлайн-среды.

Цифровая (информационная) гигиена – это совокупность навыков, знаний и умений, которые позволяют человеку эффективно работать с информацией в условиях цифровой среды.

Важно отметить, что информационная гигиена также включает в себя контроль над собственным присутствием в онлайн-среде. Дети должны понимать, что их цифровой след – это реальная проекция их деятельности, которая может повлиять на их будущее в профессиональной и личной жизни. Это подводит нас к необходимости формирования так называемой «цифровой осознанности», которая становится важным аспектом образовательной политики во многих странах.

Наряду с этим, актуальность представляемой темы определена вызовами цифровизации образования и поисками ресурсов повышения цифровой гигиены и безопасности воспитания детей и подростков.

Введение цифровой гигиены в школьную программу актуально, так как в условиях цифровизации знаний способность критически воспринимать информацию, защищать свои данные и выстраивать здоровое взаимодействие с технологиями становится неотъемлемой частью успешного будущего каждого ребёнка.

Обозначим ряд причин актуальности введения цифровой гигиены в образовательные программы:

Поток данных. Школьники сталкиваются с огромным количеством новостей, статей, видео и соцсетей, которые влияют на их восприятие мира. Умение эффективно фильтровать и перерабатывать эту информацию во многом остаётся вне традиционной образовательной программы.

Кибербезопасность. Среди ключевых навыков – защита персональных данных, умение распознавать фишинговые атаки, избегать подозрительных ссылок и понимать важность сложных паролей.

Управление цифровым временем. Это умение предотвращать цифровую зависимость, ограничивать время, проводимое за экраном, и балансировать между онлайн и оффлайн.

Защита от кибербуллинга, утечки личной информации и других киберпреступлений.

Однако внедрение концепции цифровой гигиены в школьное образование сопровождается рядом трудностей, среди которых недостаточная подготовленность учителей к преподаванию подобных дисциплин, отсутствие унифицированной программы, охватывающей все аспекты цифровой грамотности и другие.

Представленные методические рекомендации предназначены для учителей общеобразовательных школ и направлены на определение того, что такое цифровая гигиена, почему она важна в условиях тотальной цифровизации, а также на ознакомление учителей с основными темами уроков по внеурочному курсу «Цифровая гигиена».

2. Понятийно-категориальный аппарат цифровой гигиены

Что такое цифровая гигиена?

1. Цифровая гигиена – это комплекс мер направленный на безопасное формирование цифрового профиля человека, предупреждение вероятных последствий цифрового следа, являющийся превентивной защитой при взаимодействии с цифровым пространством. Обеспечивает оптимальные условия существования в онлайн и оффлайн режиме.

2. Цифровая гигиена (кибергигиена) – комплекс мер, направленных на обеспечение безопасности и защиты личных данных при использовании цифровых технологий. Цели — минимизировать риски кибератак, фишинга, вирусов и утечки данных, а также сформировать полезные привычки в использовании интернета и устройств.

3. Цифровая гигиена — это свод правил, следуя которым, человек обеспечивает себе информационную безопасность в сети Интернет. Относится к сфере знаний о цифровой безопасности. Цифровая гигиена (кибергигиена) подразумевает формирование полезных привычек у любого человека для защиты от сетевых угроз.

4. Цифровая гигиена – это знания и правила потребления информации в современном мире ТВ и интернета, позволяющие сохранить ментальное здоровье, финансы и собственную идентичность (на сайте habr.com).

5. Цифровая гигиена – это комплекс правил и практик, направленных на поддержание здорового баланса между использованием технологий и сохранением психологического благополучия (на сайте b17.ru)

6. Цифровая гигиена – это комплекс мер, направленных на обеспечение безопасности и защиты личных данных при использовании современных технологий и интернета.

Как вести себя в интернете, чтобы обеспечить безопасность данных, защитить личную жизнь и сохранить эмоциональное равновесие в эпоху

информационных технологий? На эти главные вопросы эпохи цифровизации, позволяет дать мотивированный ответ учителю цифровая гигиена.

Цифровая гигиена охватывает не только технические аспекты безопасности, но и психоэмоциональное состояние: установление временных ограничений на использование устройств, грамотное управление уведомлениями и осознанный выбор контента.

Цифровая гигиена как концепция начала активно развиваться в последние десятилетия, поскольку технологии, связанные с обработкой и хранением данных, приобрели колоссальное значение в личной и профессиональной жизни.

Таким образом, **цифровая гигиена – это комплекс мер, направленных на защиту персональных данных, безопасности устройств и информации при использовании цифровых технологий.**

В рамках изучения цифровой гигиены обучающиеся знакомятся с ключевыми понятиями «цифровой след» и «цифровой профиль».

Цифровой след – это совокупность данных, которые человек оставляет в процессе использования цифровых технологий и интернета. Эти данные могут быть как предоставленными самим пользователем, так и собранными автоматически.

Существуют два типа цифрового следа:

Активный – информация, которую пользователь оставляет намеренно. Примеры: публикации и фотографии в социальных сетях, комментарии на форумах и статьях, заполненные анкеты и регистрационные формы.

Пассивный – данные, которые собираются автоматически, часто без ведома пользователя. К ним относятся, например, файлы cookie, IP-адреса, данные, фиксируемые мобильными устройствами.

Некоторые источники формирования цифрового следа:

- **Социальные сети.** Даже если человек просто просматривает новости или чужие публикации, платформа может собирать информацию о его интересах для создания персонализированных рекомендаций.
- **Поисковые системы.** Каждый запрос, введённый в строку поиска, сохраняется.
- **Гаджеты и мобильные приложения.** Любой смартфон может фиксировать местоположение, время использования приложений, а также взаимодействие с ними.
- **Покупки в интернете.** История заказов, предпочтения по категориям товаров, отзывы, данные о платежах – всё это оставляет цифровой след.
- **«Умные» устройства.** Голосовые ИИ-помощники постоянно слушают команды и могут записывать разговоры, а «умные» камеры и другие устройства «интернета вещей» собирают данные о домах пользователей и о них самих.

Цифровой след может не только приносить пользу, но и нести в себе серьёзные риски. Некоторые из них: утечка личных данных, репутационные проблемы, мошеннические схемы.

Цифровой профиль влияет на различные аспекты жизни, поскольку цифровой след (ЦС) уже используется в качестве основы для оценки реальной личности.

- ЦС является источником информации, предметом сбора, накопления, исследования и социальной инженерии в организациях различных целеполаганий.

- Используя цифровой след, злоумышленники могут взломать личные аккаунты пользователей, получить доступ к банковским счетам, личной переписке и рабочим данным.

Цифровой профиль гражданина (ЦПГ) – это совокупность информации о физлице, собранной из различных государственных систем в одном месте – Единой системе идентификации и аутентификации (ЕСИА).

Некоторые виды информации, которые может содержать ЦПГ:

- **Персональная.** ФИО, дата и место рождения, паспорт, ИНН, СНИЛС, место регистрации/проживания, телефоны, e-mail, сведения о заключении и расторжении брака и другие.
- **Финансовая.** Сведения о трудовой занятости, самозанятости, доходах, взносах, 2-НДФЛ, данные из ЕГРИП/ЕГРЮЛ, о соцвыплатах, пенсиях, мерах соцподдержки, маткапитале и другие.
- **Имущественная.** Недвижимость, транспорт в собственности, действующие обременения, водительские права и другие.
- **Медицинская.** Полис медстрахования, данные об инвалидности, прикрепление к медучреждению и другие.

Как работает ЦПГ? Профиль формируется автоматически, собирая данные из ЕСИА и других государственных информационных систем (ГИС). Гражданин сам управляет согласиями на доступ к данным – предоставляет их и отзывает.

До конца 2025 года разработка и использование инфраструктуры ЦПГ – часть эксперимента для повышения качества и связанности данных в государственных системах

Профиль формируется автоматически, собирая данные из ЕСИА и других государственных информационных систем (ГИС). При изменении сведений они автоматически корректируются в профиле гражданина.

Гражданин сам управляет согласиями на доступ к данным – предоставляет их и отзывает. Поэтому без разрешения физлица банк или страховая компания получить информацию не может.

Что необходимо знать каждому в области цифровой гигиены?

Каждому человеку необходимы:

- 1) Периодическая смена паролей
- 2) Использование виртуальных банковских карт
- 3) Ответственное поведение в соцсетях
- 4) Не все «друзья» нам друзья
- 5) Регулярная очистка кэшей, историй и корзины
- 6) В цифре ничего не исчезает и не удаляется, поэтому не стоит порождать «глупую веселость»
- 7) Цифровые вирусы жестче, трансграничнее и бесконечнее коронавируса. Антивирусы бьются только с цифровой частью.
- 8) Основная цель цифрового вируса – человек. Основная уязвимость человека – его собственное легкомыслие.

9) Помыть руки, надеть повязку, почистить кэш и историю – обязательные привычки.

10) Цифровой профиль вещь изменяемая, но «Цифра помнит все»

11) Понимание и использование цифрового следа является заботой человека и организации.

Принципы цифровой гигиены, которые важно соблюдать каждому:

- **Осторожность при работе с личными данными.** Не стоит выкладывать в открытый доступ паспортные данные, адреса и другую личную информацию – злоумышленники могут использовать их для мошенничества.
- **Осторожность с подозрительными ссылками и вложениями.** Фишинговые атаки часто используют письма с вредоносными ссылками – перед открытием нужно убедиться, что отправитель – надёжный источник.
- **Контроль конфиденциальности в соцсетях.** Настроив приватность, можно ограничить доступ посторонних к личной информации. Желательно отключать геолокацию и не публиковать избыточные сведения о себе.

Меры, которые необходимо соблюдать каждому в области цифровой гигиены:

- **Использование надёжных паролей.** Пароли должны быть сложными, уникальными для каждого аккаунта и содержать не менее 12 символов, включая буквы, цифры и специальные знаки. Рекомендуется использовать менеджер паролей.
- **Двухфакторная аутентификация.** Дополнительный уровень защиты – подтверждение входа через SMS, почту или приложение-аутентификатор.
- **Регулярные обновления программ и антивирусной защиты.** Обновления закрывают уязвимости, которые могут использовать хакеры.
- **Создание резервных копий данных.** Это защита от потери данных при взломе, заражении вирусами-шифровальщиками или технических сбоях.
- **Контроль приложений и их доступ к данным.** Многие приложения запрашивают доступ к контактам, местоположению, файлам, камере и микрофону – нужно регулярно проверять и пересматривать разрешения, которые предоставлены.

Инструменты, которые должен использовать каждый в области цифровой гигиены:

Для обеспечения цифровой гигиены используются:

- **Антивирусное программное обеспечение** – выполняет регулярную автоматическую проверку устройства по расписанию, обнаруживает и удаляет вредоносные программы.
- **Сетевой экран** – предотвращает несанкционированный доступ пользователей к веб-сайтам, почтовым серверам и другим источникам информации.

Некоторые задачи, которые входят в сферу цифровой гигиены:

- **Обновление программного обеспечения.** Регулярные обновления операционных систем, приложений и антивирусных программ помогают защититься от новых угроз.
- **Использование двухфакторной аутентификации.** Дополнительный уровень защиты предотвращает несанкционированный доступ к аккаунтам.

- **Создание сложных паролей.** Использование уникальных и сложных паролей для каждого аккаунта значительно снижает риски взлома.
- **Использование антивирусных программ и шифрования данных.** Это помогает защитить устройства от вирусов и предотвратить утечку информации.
- **Осторожность при использовании публичных сетей.** Подключение к незащищённым Wi-Fi-сетям может привести к утечке данных, если не использовать VPN.
- **Создание регулярных резервных копий данных.** Также важно быть осторожным при открытии сомнительных ссылок или загрузке файлов.

Соблюдение цифровой гигиены важно для защиты личных данных, предотвращения кибератак и мошенничества, а также для сохранения конфиденциальности.

3. Концептуальные подходы и принципы к реализации содержания внеурочного курса «Цифровая гигиена» в современной школе»

- **Принцип дидактической спирали.** Перечень основных содержательных линий школьной информатики практически инвариантен к этапу обучения, но уровень их изучения должен быть разным: в старшей школе он выше, чем в основной школе.
- **Принцип системности и структурированности материала.** Важным дидактическим средством, поддерживающим этот принцип, являются структурограммы системы основных понятий, присутствующие в конце каждой темы.
- **Деятельностный подход к обучению.** Каждая тема курса, относящаяся либо к теоретическим вопросам информатики, либо к ИКТ, поддерживается практическими заданиями для учащихся, выполняемыми на компьютере.
- **Ориентация на формирование информационно-коммуникационной компетентности учащихся.** Переход от уровня компьютерной грамотности (базовый курс) к уровню информационно-коммуникационной компетентности происходит через комплексность рассматриваемых задач, привлекающих личный жизненный опыт учащихся, знания других школьных предметов.
- **Фокус внимания на развитии человека как личности.** Курс может быть направлен не только на проблемы безопасности в интернете, но и на развитие человека как личности в совокупности её психологических и социальных свойств в условиях активного использования цифровой информационной среды.
В рамках курса «Цифровая гигиена» могут использоваться разнообразные форматы обучения: традиционный урок, тренинги, дистанционное обучение, смешанный формат.

4. Специфика ценностей цифрового мира. Ценности цифрового мира.

Специфика ценностей в цифровом мире проявляется в разных аспектах: личностном, социальном, корпоративном и государственном. Цифровизация влияет на формирование ценностей, трансформируя их в

условиях удалённой работы, онлайн-взаимодействия и изменения бизнес-моделей.

Личностные

- **Трансформация ценностей** в рамках концепции «постматериального». На место прежних «материальных» ценностей адаптации к окружающему миру и стремления к безопасности приходят ценности самореализации, саморазвития, экологического мышления и другие.
- **Значимость когнитивного капитала личности** – он становится главной ценностью, значимым ресурсом развития и самоактуализации личности.
- **Важность осознанности и осмысленности** – важнейшая категория самоопределения человека в цифровом обществе сетевых структур.

Социальные

- **Открытость и доступность информации** как источник социального развития.
- **Ответственность за достоверность передаваемого в информационную среду интеллектуального и эмоционального контента.**
- **Устойчивость digital-среды,** обеспечивающей качество взаимоотношений в социуме.
- **Поддержка разнообразия** – цифровой мир помогает разным группам людей объединяться на основе их ценностей, помогает каждому выражать свою индивидуальность в продуктивных формах активности.

Корпоративные

- **Гибкость и адаптивность** – компании должны быть готовы к постоянным изменениям, быстрому принятию решений и гибкости в организации рабочих процессов.
- **Виртуальные команды и удалённая работа** – это требует новых подходов к коммуникации, управлению и созданию общей рабочей атмосферы.
- **Цифровые инструменты для коммуникации и сотрудничества** – использование различных цифровых платформ, приложений для общения, обмена информацией и совместной работы помогает улучшить эффективность бизнес-процессов.
- **Внедрение цифровых ценностей** – важно внедрять инновации, технологический прогресс, кибербезопасность и этику в работу компании и принципы корпоративной культуры.

Государственные

- **Прозрачность и открытость** – благодаря цифровым технологиям обеспечивается более открытое управление, предоставляется доступ гражданам к информации о деятельности государственных органов.
- **Использование данных** для улучшения госполитики, предоставления госуслуг, повышения эффективности деятельности госаппарата.
- **Создание цифровых государственных экосистем** – они должны удовлетворять запросы на социальную и экономическую активность, а также воспроизводить коллективные мировоззренческие смыслы, формировать идентичность принадлежности к стране и её историческому наследию.
- **Ценностное совпадение правительства и населения** – платформы и сайты цифрового государства позволяют декларировать совпадение по

ценностям или транслировать определённые ценности, чтобы они были присвоены населением.

Некоторые ценности цифрового мира:

- **Свобода.** Цифровой мир характеризуется открытым информационным пространством, доступностью ресурсов, потенциалом самовыражения и самореализации.
- **Ценность личности.** В цифровом мире важно учитывать уникальность каждого человека, его жизнь, активность и переживания.
- **Открытость и доступность информации.** Информация считается источником социального развития.
- **Ответственность.** В цифровом мире необходимо обеспечивать достоверность передаваемого в информационную среду интеллектуального и эмоционального контента.
- **Творчество.** Важно проявлять творчество даже в условиях алгоритмичных решений, принятых на основе результатов функционирования искусственного интеллекта.
- **Возможность влиять на изменения социального поведенческого протокола.**

Также к ценностям цифрового мира относят **инновационность**, устойчивость цифровой среды, личностную идентичность и другие.

5. Психологический портрет поколения Z

Яркими представителями аборигенов цифровой эпохи являются зуммеры (Z-поколение) или центиниалы

Зумер – неологизм и сленговое слово заимствованное из английского языка, обозначающее представителей поколения Z из теории поколений американского писателя Уильяма Штрауса и экономиста Нила Хоува (1991).

Годы рождения поколения зумеров условны и могут варьироваться в зависимости от социальных, экономических и технологических факторов в разных странах, а также от методологий, используемых исследователями. Тем не менее, чаще всего выделяют следующие варианты временных границ у поколения зумеров:

1995–2010 – классическая версия Штрауса и Хоува, наиболее популярная, учитывающая начало цифровой эпохи;

1997–2012 – версия Pew Research Center, которая фокусируется на периоде активного внедрения интернета и смартфонов в повседневную жизнь;

2000–2015 – по данным Марка МакКриндла, при этом делается акцент на новом тысячелетии и влиянии цифровых технологий на формирование личности;

2003–2024 – версия российской компании RuGenerations;

1996–2010 – компромиссная версия, сочетающая черты переходного поколения Y (миллениалов) и цифровой зрелости зумеров.

В России [маркетологи](#) и социологи чаще всего называют период 2000-2011 годов, так как в это время активно развивались интернет, мобильные технологии и социальные сети. Кроме того, происходили важные исторические события, которые повлияли на мировоззрение и ценности поколения зумеров.

Временные рамки могут меняться в зависимости от страны. Например:

В США зумерами обычно считают тех, кто появился на свет с 1997 по 2012 год.

В России, по мнению исследователей, к поколению Z относятся люди, рождённые с 2003 по 2015 год.

Поколение Digital, хоумлендеры, центениалы, цифровые аборигены – у зумеров множество наименований, и каждое подчеркивает их уникальность. Они выросли в эпоху технологий, когда интернет и смартфоны стали неотъемлемой частью нашей жизни. Это поколение коренным образом отличается от своих предшественников

Поколение Z (зумеры) – термин, который обозначает **поколение людей, выросших в эпоху развития цифровых технологий**. Название продолжает традицию обозначения поколений буквами после X и Y. Точных временных рамок для поколения Z не существует. По разным классификациям, к зумерам относят людей, родившихся примерно с середины 1990-х до начала 2010-х годов. Некоторые источники указывают конкретный диапазон –1997–2012 годы.

Название «зумеры» происходит от глагола zoom – «увеличивать», «приближать» и характеризует способность быстро воспринимать информацию и адаптироваться к изменениям.

Эта метафора идеально описывает поколение Z, которое с раннего детства осваивает технологии, позволяющие им буквально и фигурально приближаться к миру. Часто можно заметить, как они пытаются «увеличить» бумажный рисунок пальцами, словно экран [смартфона](#), что показывает их привычку воспринимать мир через цифровые интерфейсы.

Зумеры – это первое поколение, выросшее в цифровом мире. Их отличают высокая скорость восприятия информации, ориентация на визуальные форматы, развитое критическое мышление и одновременно – эмоциональная нестабильность из-за постоянного информационного шума. Они ценят гибкость, свободу выбора и индивидуальность. Авторитеты для них – не по должности, а по личной убедительности.

С раннего возраста зумеры погружаются в мир интернета, гаджетов и социальных сетей, который стал для них естественной средой обитания. Общение в онлайн-пространстве, цифровые игры и мультимедиа формируют их восприятие реакции. Это делает их гибкими в использовании новых технологий, но также усиливает [зависимость](#) от цифровых устройств.

Ирина Тебенева в своей книге «Что за X.Y...Z? Как родителям и детям понять друг друга» предлагает новый взгляд на пирамиду Маслоу, где базовые потребности – это заряженный смартфон и Wi-Fi, а уже потом все остальные.

Чем зумеры отличаются от бумеров, миллениалов и поколения альфа?

Представители поколения Z отличаются от бумеров, миллениалов и альфа своим уникальным цифровым опытом.

Бэби-бумеры, родившиеся в 1944-1967 годы, выросли в эпоху послевоенного восстановления. Для них важны стабильность, традиции и долгосрочные цели. В отличие от них, зумеры стремятся к гибкости, индивидуальности и осознанному потреблению.

Миллениалы (1981-1996) застали переход от аналогового мира к цифровому. Зумеры отличаются от них тем, что родились уже в эпоху полной цифровизации. Они привыкли к мгновенному доступу к информации и высоко ценят визуальные форматы.

От поколения альфа зумеры отличаются тем, что их детство проходило в период становления и массового внедрения цифровых технологий. Они застали переход от кнопочных телефонов к смартфонам, от стационарных компьютеров к облачным сервисам. Поколение альфа, напротив, с самого рождения окружено высокими технологиями – голосовыми помощниками, умными устройствами и искусственным интеллектом. Если зумеры осваивали цифровой мир постепенно, то альфа воспринимают его как естественную часть своей жизни, что делает их еще более интегрированными в технологическую среду.

Сленг и язык зумеров

Как и у любого поколения, у зумеров есть свой сленг – слова, которые часто непонятны представителям других возрастных групп. Это неформальный язык, используемый зумерами в общении между собой. Он отражает современные тенденции и формируется под влиянием культуры и социальных сетей

Сленг позволяет зетам сократить время на общение, выразить слова и понятия, которых нет в русском языке. Приведем несколько примеров:

брейнлаг – это когда мозг тормозит и долго соображает, например, когда тебя спросили, а ты не можешь быстро ответить;

бэнч – замечательно, очень хорошо;

тильтовать – находиться в состоянии раздражения и эмоционального упадка, злиться из-за неудачи;

варик – сленговая форма слова «вариант»;

агриться – сердиться, злиться, проявлять агрессию и злобу;

флексить – демонстрировать свою крутость, хвастаться;

быть на чиле – отдыхать, расслабляться.

Анастасия Курникова, HR-менеджер коммуникационного агентства PR Partner, активно взаимодействует с представителями поколения Z. Она отмечает:

– У зумеров есть особенная культура переписки: они предпочитают короткие сообщения без лишних предисловий. Не стоит писать «Привет! Как дела? У меня к тебе вопрос», если можно просто сразу задать его. Деловая переписка для них – не повод для светской беседы, а инструмент для решения задач.

Иногда нам кажется, что быстрее позвонить, записать голосовое сообщение или отправить видеосообщение. Но для зумеров удобнее текст. Эксперт подчеркивает:

– Текстовая информация четкая, понятная, и ее можно обработать в удобный момент. Неожиданные звонки вызывают у зумеров тревожность, а голосовые – раздражение. Поэтому, если срочно нужно передать информацию, можно надиктовать ее и конвертировать в текст.

Политические взгляды и общественная позиция зумеров

Зеты выросли в эпоху глобализации, свободного доступа к информации и социальных сетей, что сильно повлияло на их отношение к политике и общественным вопросам. По словам нашего эксперта Кирилла Сагитова, в политической сфере зумеры обычно занимают умеренно-критическую позицию:

– Они не склонны к радикализму, но очень чувствительны к теме справедливости, экологии и равенства. Они высоко ценят прозрачность, свободу слова и равные права для всех. При этом их общественная активность проявляется больше в онлайне, чем в оффлайне.

Социальные сети и цифровые платформы для зумеров – основной инструмент выражения мнения, участия в петициях, благотворительных проектах и общественных кампаниях. Несмотря на это, зеты могут активно поддерживать инициативы, которые соответствуют их ценностям и в реальной жизни, если они видят в этом возможность изменить мир к лучшему.

Что необходимо знать педагогу о зумерах

Зумеры – это первое поколение, выросшее в эпоху цифровых технологий, интернета и социальных сетей.

1. Зумеры родились примерно в 1995-2012 годах – границы варьируются в зависимости от страны и методологии исследований.

2. Это поколение цифрового мира, для которого технологии – естественная среда.

3. Зумеры быстро воспринимают информацию, ориентируются на визуальные форматы. Они склонны к критическому мышлению, но подвержены эмоциональной перегрузке из-за информационного шума.

4. Поколение Z ценит гибкость, свободу выбора и индивидуальность. Для них важны искренность и личная убедительность авторитетов, а не их должность.

5. Зеты уделяют внимание вопросам экологии, равенства и социальной справедливости.

6. Они стремятся к финансовой независимости с юного возраста, используя цифровые возможности для заработка.

Таким образом, зумеры – это поколение, которое не просто живет в цифровом мире, а активно его создает, меняя привычные устои и формируя будущее здесь и сейчас.

Ценности

Некоторые ценности поколения Z:

- **Свобода самовыражения** – зумеры не боятся быть непохожими на других, экспериментируют со стилем, гендерными ролями и профессиями, отвергая жёсткие рамки.
- **Инклюзивность** – для этого поколения важны толерантность и равноправие, они поддерживают людей с разными взглядами, культурами и особенностями.
- **Экологичность** – забота о планете – не мода, а осознанный выбор, зумеры сортируют мусор, экономят ресурсы и критикуют компании, вредящие окружающей среде.

Поколение Z влияет на общество, культуру и экономику. Например:

Потребности и ценности зумеров формируют новые тренды в маркетинге, образовании и других сферах.

Представители этого поколения активно участвуют в социальных движениях и политических процессах, используя цифровые инструменты для организации и мобилизации.

Однако обобщения о целом поколении всегда неполны – внутри поколения Z существует большое разнообразие взглядов, ценностей и жизненного опыта.

Среди сильных сторон поколения Z – свобода от предрассудков, психологическая гибкость, креативность. Его представителей отличает творческий подход в любом деле, поскольку в любой сфере жизни сегодня наблюдается высокий уровень конкуренции, которого не было ни в одном из предыдущих поколений. Однако эти люди не способны в полной мере к концентрации внимания, они живут в мире быстро сменяющихся друг друга событий, в их жизни нет стабильности.

Поколение Z – это молодёжь, которая выросла в эпоху цифровых технологий и их влияния на общество. На поколение Z влияет то, как они выглядят и как их воспринимают другие люди в онлайн-среде. Этот фактор становится важной составляющей мотивации для молодых людей и влияет на ценности и цели, которые они преследуют в жизни.

Поколение Z (или «зумеры») с раннего детства сильно привязаны к гаджетам, формируют картину мира и взгляды на жизнь на основании рекомендаций друзей и лидеров мнений. Они стараются всегда быть на связи с друзьями. Зумеры считаются вдумчивыми и экономными, бережно относятся к природным ресурсам и следят за собственным ментальным здоровьем.

Поколение Z – это дети, которые родились в информационном обществе. Они более зависимы от цифровых технологий, чем их родители, которые пользовались телевидением как альтернативой книгам и газетам. Они нетерпеливы и сосредоточены в основном на краткосрочных целях, при этом они менее амбициозны, чем дети из предыдущих поколений. Они более ориентированы на потребление и более индивидуалистичны.

Поколение Z – дети мультимедийных технологий, которые родились в информационном обществе. Они более зависимы от цифровых технологий, чем их родители, которые пользовались телевидением как альтернативой книгам и газетам. Они нетерпеливы и сосредоточены в основном на краткосрочных

целях, при этом они менее амбициозны, чем дети из предыдущих поколений. Они более ориентированы на потребление и более индивидуалистичны.

6. Основные принципы воспитания в области цифровой гигиены

Основные принципы воспитания в области цифровой гигиены включают управление экранным временем, защиту личных данных, выбор контента и формирование навыков безопасного общения в сети.

Цель – научить ребёнка осознанно взаимодействовать с онлайн-миром, не теряя связи с реальностью.

Ограничение экранного времени

- **Установить чёткие и понятные временные рамки.** Правила должны быть последовательными и обсуждаться совместно с ребёнком. Важно не просто запретить, а объяснить, почему вводятся ограничения, и предложить привлекательные альтернативы в реальном мире: совместные игры, прогулки, занятия спортом или творчеством.
- **Создать зоны и время без гаджетов** особенно в семье: за столом, перед сном, во время прогулок.
- **Использовать инструменты управления временем** – например, отдельный таймер для каждой онлайн-задачи, который помогает сохранять концентрацию. В зависимости от возраста ребёнка можно выбирать разные отрезки времени: для подростков – 20–25 минут, для младших школьников и дошкольников – 10–15 минут.

Защита личных данных

- **Объяснить ребёнку, какую информацию нельзя публиковать в открытом доступе или передавать незнакомым людям.** К таким данным относятся полное имя, домашний адрес, номер школы, номер телефона, а также пароли от аккаунтов.
- **Научить использовать сложные и разные пароли** для различных сервисов и не делиться ими даже с друзьями.
- **Обсудить настройки конфиденциальности** в социальных сетях, объяснить, как сделать профиль закрытым и ограничить круг лиц, которые могут видеть публикации.

Выбор контента

- **Научить ребёнка выбирать контент, который он смотрит и читает в интернете.** Объяснить, что есть контент, который может быть вредным или опасным для здоровья и развития: насилие, пропаганда наркотиков, экстремизм.
- **Развивать критическое мышление,** чтобы ребёнок учился анализировать информацию из интернета, отличать фейковые новости и не доверять сомнительным источникам.
- **Использовать родительский контроль** на устройства, чтобы блокировать доступ к нежелательным сайтам и приложениям.

Общение в сети

- **Объяснить ребёнку, что виртуальные знакомые в реальной жизни могут оказаться не теми, за кого себя выдают.** Установить запрет на встречи с интернет-друзьями без ведома и присутствия родителей.

- **Научить ребёнка с осторожностью относиться к любым сообщениям от незнакомцев**, особенно если они содержат просьбы личного характера, предложения подарков или угрозы.
- **Объяснить, что о любых подозрительных или пугающих диалогах следует немедленно сообщать взрослым**, которым ребёнок доверяет.
- **Использовать игровые формы обучения** – например, придумать сказку или историю про то, как нужно вести себя в интернете, разыграть с ребёнком разные ситуации, которые могут случиться онлайн.

7. Темы уроков по цифровой гигиене в школе и методические рекомендации к их проведению

Урок 1. История возникновения интернета, понятия интернет-угроз, изменения границ допустимого в контексте цифрового образа жизни.

Интернет-угрозы – это опасности, которые подстерегают людей и компьютерные системы в интернете. Некоторые виды интернет-угроз:

- **Вредоносное ПО.** К нему относятся вирусы, черви, трояны, шпионское ПО и программы-вымогатели. Они предназначены для повреждения, уничтожения или несанкционированного доступа к системам и данным.
- **Фишинг.** Злоумышленники пытаются получить конфиденциальную информацию, маскируя вредоносный файл, сайт или ссылки под надёжный источник.
- **Атаки типа «отказ в обслуживании».** DoS-атаки и DDoS-атаки направлены на перегрузку систем, сайтов, сетей, приложений, что делает их недоступными для пользователей.
- **SQL-инъекции.** Внедрение вредоносного SQL-кода в запросы базы данных с целью получить несанкционированный доступ к данным.
- **Кража данных.** Несанкционированное копирование, передача или использование конфиденциальных данных.
- **Социальная инженерия.** Манипуляции с целью получения конфиденциальной информации путём обмана пользователей.
- **Кибербуллинг.** Психологическое насилие с использованием угроз и преследования.
- **Киберклевета, или кибердиффамация.** Подрыв репутации физического лица или организации с использованием интернета.
- **Финансовые угрозы.** Утрата денег через мошеннические сайты, сервисы сомнительного происхождения. Чтобы обезопасить себя от интернет-угроз, рекомендуется использовать программы родительского контроля, антивирусы, безопасный поиск и настраивать Wi-Fi с паролем и DNS-фильтрацией для блокировки опасных сайтов.

Некоторые методические рекомендации для обучающихся по теме «Понятия интернет-угроз»:

- **Использовать разнообразные форматы обучения.** Это могут быть традиционные уроки (коллективная и групповая формы работы), тренинги, дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение) или смешанный формат.

- **Применять систему учебных заданий.** Задания должны помогать школьникам выявлять информационную угрозу, определять степень её опасности, предвидеть последствия угрозы и противостоять им. Примеры заданий: составление памяток, анализ защищённости собственных аккаунтов в социальных сетях и электронных сервисах, практические работы.
- **Привлекать жизненный опыт обучающихся.** Это позволяет правильно ввести ребёнка в цифровое пространство и корректировать его поведение в виртуальном мире.
- **Формировать навыки работы с информацией.** Это умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и её критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов.
- **Формировать ответственное отношение к взаимодействию в информационно-телекоммуникационной среде.** Это может включать мотивацию к обеспечению личной безопасности, безопасности семьи и друзей.

Урок 2.Изменения нормативных моделей развития и здоровья детей и подростков.

В рамках этой темы необходимо:

- **Учить не накапливать и запоминать информацию,** а уметь самостоятельно её добывать и критически оценивать.
- **Развивать способность действовать в формате многозадачности.** Важно научить, правильно распределять ограниченные когнитивные ресурсы.
- **Учить мышлению в ситуации неопределённости,** в открытых сетевых системах, в рамках широкого диапазона действий и отношений.
- **Мотивировать ответственное отношение** к обеспечению личной безопасности, безопасности семьи и друзей при активном использовании сетевых форм общения (социальные сети, игры и пр.).
- **Формировать навыки своевременного распознавания онлайн-рисков** (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).
- **Преодолевать «цифровой разрыв»** между поколениями и обучать родителей правильной оценке своих возможностей в помощи детям в интернете.
- **Использовать различные формы проведения мероприятий** для родителей: лектории, выступления на родительских собраниях, микрообучение на основе технологий онлайн-обучения, геймификация, создание чек-листов и пр..

Урок 3.Цифровая гигиена: зачем это нужно? Понятие периметра безопасности, обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребёнка, баланс ценностей развития и ценностей безопасности.

Некоторые методические рекомендации для обучающихся по теме «Цифровая гигиена: зачем это нужно?»:

- **Объяснить, что в интернете есть деструктивный контент:** мошенничество, угрозы, фейки, слежка, кибербуллинг, пропаганда наркотиков и алкоголя, инструкции по изготовлению оружия и другой деструктив.

Полностью искоренить такой контент невозможно, но можно противодействовать его влиянию. Для этого нужно, чтобы ребёнок понимал, с чем он столкнулся и что нужно делать.

- **Привить навыки фактчекинга и критического мышления.** Подростки должны знать, что доверять нужно только официальным источникам информации и за распространение фейков предусмотрена ответственность.
- **Уделить внимание таким аспектам, как анонимность и приватность,** целостность цифрового образа, защита репутации, защита от нежелательных знакомств, а также финансовых онлайн-транзакций и счетов.
- **Обсудить с детьми, что они делают и чем делятся в сети.** При необходимости можно искусственно фильтровать контент с помощью приложений или специальных детских аккаунтов.
- **Использовать разнообразные форматы обучения.** Это могут быть традиционный урок (коллективная и групповая формы работы), тренинги, дистанционное обучение (электронные курсы, видеоролики, почтовые рассылки, микрообучение), смешанный формат.

Урок 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией, способы выявления наличия вредоносных кодов на устройствах, действия при их обнаружении.

Для выявления вредоносных кодов можно использовать следующие подходы:

- **Статический анализ.** Выявляет угрозы путём изучения структуры файлов без их выполнения. Антивирус сканирует бинарные инструкции, строки кода, импортируемые библиотеки и другие элементы, сопоставляя их с базами сигнатур и хешей.
- **Динамический анализ.** Образец оценивают по его поведению – в действующей системе или в изолированной среде. Этот метод используют против сложных угроз, при реализации которых применяются обфускация, полиморфизм и другие техники маскировки.
- **Эвристический анализ.** Выявляет вредоносные объекты по их поведению и структуре файла. Средства защиты отслеживают характерные признаки подозрительной активности: попытки скрыть присутствие вредоноса в системе, внедрение в другие процессы и получение несанкционированного доступа к защищённым ресурсам.
- **Анализ трафика.** Когда система обнаруживает подозрительный файл, она может быстро проверить его через облачный сервис, который анализирует объект с учётом последних обновлений и данных от других пользователей.

Некоторые действия при обнаружении вредоносных кодов:

- **Отключить устройство от интернета.** Это предотвратит отправку большего количества личных данных хакерам.
- **Просканировать устройство с помощью антивирусного программного обеспечения.** Антивирусное программное обеспечение сканирует устройство, чтобы найти совпадения между кодом известных вирусов и кодом устройства.

- **Удалить необычные файлы и приложения.** Эти подозрительные файлы или приложения могут быть замаскированным вредоносным ПО.
- **Включить безопасный режим.** На большинстве устройств есть функция безопасного режима, которая позволяет загружать только минимально необходимое программное обеспечение.
- **Сбросить устройство к заводским настройкам.** Прежде чем прибегнуть к этому действию, нужно убедиться, что все данные сохранены в резервной копии, иначе они будут утеряны.
- **Поменять пароли от учётных записей,** если есть подозрение на то, что они могли быть украдены.
- **Регулярно делать резервные копии важных данных** и проверять их работоспособность, чтобы информацию можно было восстановить в случае заражения устройства.
- **Урок 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией, груминг, кибербуллинг, профилактика насилия в Сети.**

Груминг в психологии — это процесс, при котором взрослый человек целенаправленно завоевывает доверие ребёнка или взрослого, чтобы впоследствии вступить с ним в сексуальные отношения. Груминг — это систематический процесс, в котором взрослый устанавливает доверительные отношения с ребёнком или подростком с целью последующей сексуализированной эксплуатации.

Термин происходит от английского слова grooming — «ухаживающий». Груминг может происходить как в виртуальном пространстве, так и при реальной, физической коммуникации.

Некоторые формы

- **Онлайн-груминг (кибергруминг)** — манипуляция в интернете, где злоумышленник может выдавать себя за любое лицо, в том числе за сверстника, чтобы жертва больше ему доверяла.
- **Груминг в закрытых сообществах** — преступники часто используют авторитетные позиции в закрытых группах, таких как спортивные клубы, школы, религиозные организации или творческие коллективы.
- **Груминг в семье** — родственники или близкие друзья семьи используют доверие и зависимость ребёнка для манипуляции.

Опасность груминга в том, что действия злоумышленника изначально выглядят невинными: он постепенно входит в доверие к жертве, а затем склоняет к сексуальным отношениям. При этом жертва может не понимать, что подвергается насилию, — иногда ей может казаться, что она сама спровоцировала эти отношения, на деле же ответственность всегда несёт взрослый.

Некоторые признаки, указывающие на груминг:

- **Чрезмерная дружелюбность** взрослого, предложение подарков и/или денег.
- **Приглашение в «особенный» круг общения.**
- **Поощрение секретности:** «Никому не говори, это только между нами».

- **Постепенно нарушаются границы личного пространства:** сначала это дружеские объятия, затем — интимные прикосновения.

Меры защиты

Взрослым важно уметь распознавать манипуляции и чётко определять границы профессиональных отношений. В случае подозрительной коммуникации нужно её прекратить и обратиться за поддержкой.

Родителям рекомендуется:

- **Выстраивать доверительные отношения с ребёнком** — важно, чтобы он не боялся сообщить о любом случае, который его смутил или напугал.
- **Объяснить ребёнку, что следует насторожиться,** если какой-то друг просит никому не говорить об их общении.
- **Научить блокировать подозрительных собеседников** и сохранять скриншоты странных переписок.

Некоторые методические рекомендации для обучающихся по теме «Атаки, связанные с социальной инженерией, груминг, кибербуллинг, профилактика насилия в Сети»:

- **Объяснить, что в интернете люди часто оказываются не теми, за кого себя выдают.** Подросткам нужно научить проверять запросы от знакомых, чтобы убедиться, что аккаунт настоящий. Также важно рассказать о рисках общения с незнакомцами онлайн и в приватных чатах.
- **Объяснить, что нельзя называть своё полное имя, домашний адрес, электронную почту, номер телефона или номер школы людям, которых нет в реальной жизни.** Нужно научить подростков не публиковать личную информацию, которую они не хотели бы рассказывать всем.
- **Научить правильно реагировать на обидные слова или действия других пользователей.** Подросткам важно сформировать понимание, что соцсети и мессенджеры — часть не виртуальной, а реальной жизни, и любые действия в них имеют последствия.
- **Объяснить, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.**
- **Информировать о возможности получения психологической помощи.** Можно рассказать об адресах, телефонах доверия и времени консультаций.
- **Провести тренинги, классные часы, квесты,** направленные на отработку навыков бесконфликтного поведения в сети, решения межличностных конфликтов, эффективной коммуникации.
- **Информировать о возможности вступления в школьное объединение,** которое отвечает за бесконфликтное разрешение сложных ситуаций взаимодействия подростков в сети.

Кибербуллинг – это преднамеренные действия, направленные на причинение вреда человеку через интернет или цифровые устройства. Его цель – причинить вред, запугать, разозлить или унижить человека в интернете.

Некоторые формы кибербуллинга:

- **Оскорбления и угрозы.** Грубые высказывания, дискриминационные комментарии, угрозы физического насилия и многое другое.
- **Аутинг.** Вопреки желанию человека в Сеть выкладывают компрометирующую информацию, личные переписки, секреты, фото или видео, порой интимного характера.
- **Троллинг.** Обычно это провокационные высказывания с долей сарказма.
- **Имитация личности.** Создание фейкового аккаунта с помощью данных и фото реального человека.
- **Доксинг.** Публикация в открытом доступе персональных данных человека — адреса места жительства, номера телефона, места работы или учёбы — без его согласия и с целью травли.
- **Массовые бот-атаки.** Когда под публикациями человека появляются сотни или даже тысячи однотипных сообщений с фальшивых аккаунтов с оскорблениями и угрозами.
- **Грифинг.** Этот вид травли встречается в онлайн-играх. «Гриферы» намеренно мешают другим игрокам: блокируют прохождение испытания, нападают на союзников, спамят в чате оскорблениями.
- **Флейминг.** Сознательное провоцирование публичного конфликта в сети с переходом на оскорбления.

Некоторые методические рекомендации для обучающихся по теме «Кибербуллинг»:

- **Не сообщать свои данные агрессору** (реальное имя, фамилию, адрес, телефон, номер школы и т. п.).
- **Не открывать доступ к своей страничке** незнакомым людям.
- **Следить за информацией**, которую выкладывается в интернете.
- **Придерживаться правил сетевой этики**, не отвечать грубо на сообщения, чтобы не спровоцировать собеседника.
- **Игнорировать сообщения от незнакомых, агрессивных и подозрительных личностей.**
- **Фиксировать угрозы и факты кибербуллинга.** Если расстроило сообщение (картинка, видео), нужно обратиться за помощью к администратору ресурса, сохранить или распечатать страницу.
- **Обращаться за помощью к взрослым.** Например, к родителям, учителям, администраторам интернет-ресурсов.

- **Соблюдать корректность при общении в сети.** Не стоит вести хулиганский образ виртуальной жизни, так как интернет фиксирует все действия и сохраняет их.
- **Не размещать информацию,** которая может кого-либо оскорбить или обидеть.

Некоторые методические рекомендации для обучающихся по теме «Профилактика насилия в Сети»:

- **Объяснить, что при общении в интернете нужно быть дружелюбным с другими пользователями.** Не стоит писать резкие и оскорбительные слова.
- **Научить правильно реагировать на обидные слова или действия других пользователей.** Не нужно общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит покинуть ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путём.
- **Объяснить, что нельзя разглашать в интернете информацию личного характера** (номер телефона, домашний адрес, номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии и видео.
- **Объяснить опасность встречи с незнакомыми людьми из интернета.** В сети человек может представиться кем угодно, поэтому на реальную встречу с интернет-другом надо обязательно ходить в сопровождении взрослых или подруги/друга.
- **Объяснить, что при общении на ресурсах, требующих регистрации** (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя. Можно выбрать ник, не содержащий никакой личной информации.
- **Объяснить, что цель сообщения о случае насилия** — своевременное вмешательство для предупреждения вреда, а не наказание и преследование обидчика.
- Для обучающихся разных возрастов можно использовать различные формы работы, например, круглые столы и интернет-батлы, открытые обсуждения и дискуссии, тренинговые занятия.

Урок 6. Обращение с деньгами в сети интернет, использование детской пластиковой карты.

Некоторые методические рекомендации по обучению обращению с деньгами в интернете и использованию детской пластиковой карты:

- **Объяснить основы финансовой безопасности.** Важно, чтобы ребёнок усвоил: ПИН-код и CVV-код – секретная информация, сообщать которую нельзя никому, эту информацию лучше выучить наизусть. Также нужно напомнить, что нельзя давать свою карту незнакомым или малознакомым людям.

- **Обсудить с ребёнком, на что он может тратить деньги в сети.** Лучше, если он решит что-то купить, например интернет-игру, то сделает это вместе с родителями.
- **Предупредить об опасностях участия в онлайн-викторинах, лотереях, распродажах.** Нужно объяснить ребёнку, что такие заработки в интернете нереальны. Также важно научить отличать надёжные сайты от фальшивок.
- **Остерегаться телефонных мошенников.** Нужно объяснить детям, что личные данные и персональную информацию можно сообщать только близким родственникам, а с незнакомцами по телефону общаться не стоит, кем бы они ни представлялись.
- **Установить средства защиты от воздействия вредоносного кода** на все устройства, имеющие выход в интернет. Нужно контролировать актуальность антивирусных баз и использовать все возможные настройки безопасности, которые предоставляются интернет-порталом.
- **Объяснить ребёнку, что для покупок предметов и дополнительных опций в игре нужно использовать официальные внутриигровые магазины и игровые порталы,** что нельзя вводить данные банковских карт на сторонних ресурсах.
- **Установить лимит на переводы и снятие наличных по детской карте.** Нужно напомнить, что нельзя сообщать данные банковской карты и передавать её кому-либо, так же как логин и пароль от личного кабинета банка и проверочный код из СМС.
Некоторые методические рекомендации по теме «Использование детской пластиковой карты»:
- **Формирование финансовой грамотности.** Нужно объяснить детям основы управления финансами, научить планировать расходы и осознавать ценность денег.
- **Обеспечение безопасности.** Можно рассказать о том, что пластиковая карта безопаснее наличных, а родители могут контролировать расходы ребёнка и устанавливать лимиты.
- **Развитие независимости.** Можно объяснить, что карта позволяет детям свободно расплачиваться за покупки, что формирует уверенность в своих силах.
- **Обучение онлайн-транзакциям.** Можно рассказать о том, что с помощью детской карты можно учить детей пользоваться интернет-банкингом.
- **Развитие ответственности.** Можно объяснить, что детская карта может научить ребёнка принимать решения о финансах, заботиться об их сохранности и использовать деньги с умом.
- **Привитие навыков накопления.** Можно рассказать о том, что некоторые финансовые учреждения предлагают специальные условия для накоплений, что может вдохновить детей начать сбережения.

Урок 7. Контентные риски, настройка и безопасное использование смартфона или планшета, семейный доступ.

Контентные риски в интернете – это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие **противозаконную, неэтичную или вредоносную информацию**. Столкнуться с такими рисками можно практически везде: в социальных сетях, блогах, торрентах, персональных сайтах, видеохостингах и других ресурсах.

Виды

Контент, создающий контентные риски, может быть:

- **Противозаконным** – например, распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.
- **Неэтичным** – контент не запрещён к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, «только для взрослых»).
- **Вредоносным** – контент может нанести прямой вред психическому и физическому здоровью, особенно детей и подростков. Например, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства).

Последствия

Столкновение с контентными рисками может иметь негативные последствия для эмоциональной сферы, психологического развития, социализации, а также физического здоровья. Например:

- **Психологическое давление** – информация, содержащая шокирующий контент, может оказывать психологическое давление на пользователей, которые не способны до конца осознать смысл происходящего.
- **Вред здоровью** – под впечатлением от сайтов с подобным содержимым пользователи могут пострадать не только в эмоциональном плане, но и нанести прямой урон здоровью.

Меры защиты

Для предупреждения контентных рисков рекомендуется:

- **Использовать специальные технические средства** – программы родительского контроля и контентной фильтрации, настройки безопасного поиска. Они позволяют установить запрет на посещения сайтов негативного содержания, ограничить время доступа к интернету, мониторить переписку в социальных сетях и онлайн-мессенджерах.
- **Выработать «семейные правила» использования интернета** — ориентироваться на них, чтобы знать, как поступать при столкновении с негативным контентом.

Некоторые методические рекомендации для обучающихся по теме «Контентные риски, настройка и безопасное использование смартфона или планшета, семейный доступ»:

- **Объяснить, что поиск информации в интернете может быть связан с рисками.** Важно рассказать о подозрительных ресурсах и фишинговых сайтах, о том, как злоумышленники распространяют негативные материалы.
- **Объяснить, как сделать работу со смартфоном безопасной.** Например, объяснить, что в начале работы со смартфоном нужно установить пин-код или функцию TouchID (или FaceID), чтобы сохранить данные на устройстве в случае его потери. Также важно рассказать о выборе паролей для аккаунтов от различных сервисов и о том, что нужно отключить функционал, доступный по отпечатку пальца, кроме разблокировки телефона.
- **Объяснить, как выбирать подходящий контент.** Можно рассказать о категории для детей в AppStore или GooglePlay, где приложения уже отобраны согласно интересам ребёнка и возрастным ограничениям.
- **Объяснить, как устанавливать приложения.** Нужно использовать официальные магазины, чтобы избежать установки вирусов и другого вредного ПО.
- **Объяснить, как устанавливать запрет на дополнительные покупки.** Это поможет избежать незапланированных расходов, а ребёнку – научиться планировать бюджет.
- **Объяснить, что такое семейный доступ.** Можно рассказать о том, что семейный доступ позволяет всем членам семьи совместно пользоваться приложениями, совершать покупки, создавать общие медиатеки.
- **Использовать специальные приложения.** Например, Kaspersky Safe Kids, которое позволяет удалённо контролировать использование устройства ребёнком, контролировать время работы устройства и установленных приложений, смотреть, какие ресурсы часто посещает ребёнок.

Урок 8. Публичные аккаунты, настройки приватности публичных страниц, правила ведения публичных страниц, овершеринг.

Некоторые методические рекомендации для обучающихся по теме «Публичные аккаунты, настройки приватности публичных страниц, правила ведения публичных страниц, овершеринг»:

О настройках приватности публичных страниц:

- Объяснить, что настройки приватности позволяют контролировать, кто может видеть контент. Например, можно скрыть номер телефона, школы, класса, убрать адрес дома.
- Показать, как с помощью настроек можно выстраивать цифровое пространство: делать так, чтобы заявки в друзья присылали все пользователи, а основную информацию видели только друзья.
- Рассказать о правилах уважения чужой приватности: перед тем, как отметить кого-то, лучше спросить у него разрешения на это.

О правилах ведения публичных страниц:

- Показать, что в публичных постах не стоит публиковать личную информацию, которая может быть использована против пользователя (например, жалобы на работу, семейные конфликты, интимные подробности).
- Объяснить, что даже если пост удалён, он может быть сохранён или переслан другими пользователями.

- Показать, что не стоит искать признания и сочувствия у подписчиков, откровенно рассказывая о своих мыслях или изливая душу незнакомцам.
- Объяснить, что в интернете люди могут быть несдержанными и жестокими, и если они начнут писать неприятные комментарии или ругательства, то не стоит вестись на провокации и принимать это близко к сердцу.

Об овершеринге:

- Объяснить, что овершеринг (от англ. overshare — чрезмерно много делиться) — это стремление человека излишне делиться личной информацией, причём не только о себе.
- Показать, что чрезмерная откровенность в сети может быть опасной: рассказы о дорогих подарках, новом гаджете, фотографии квартиры и любая демонстрация объектов, которые свидетельствуют о достатке, могут привести к мошенничеству и грабежу.
- Показать, что эмоциональные комментарии в соцсетях или блогах могут спровоцировать психологические атаки — буллинг, груминг, шантаж, абьюз, преследование, или привести к уголовной или административной ответственности.

Урок 9. Фишинг, анализ проблемных ситуаций, разработка кейсов с примерами, как защититься от фишеров в социальных сетях и мессенджерах.

Фишинг (англ. phishing) – вид интернет-мошенничества, при котором злоумышленники пытаются выманить у жертвы личную информацию под видом официального запроса. Это делается обычно в форме письма, сообщения или даже звонка от доверенного сервиса: банка, магазина, «Госуслуг» и так далее.

Фишинг (англ. phishing. Образовано от двух слов: fishing — «рыбная ловля» и password – «пароль») — это способ мошенничества в интернете, при котором злоумышленники пытаются украсть личные данные: пароли, номера банковских карт, логины.

Не зря слово созвучно с английским «выуживанием»: злоумышленники «ловят» доверчивых пользователей на поддельные сайты, письма или сообщения.

Чаще всего на обман попадают люди, которые не очень хорошо разбираются в современных технологиях или не знают о мошеннических атаках. Как объяснить им, что такое фишинг, простыми словами?

Классический пример: на электронную почту приходит письмо якобы от банка с просьбой срочно обновить пароль, но на самом деле ссылка ведёт на фишинговый сайт – это копия настоящего ресурса, созданная для кражи данных.

Некоторые методические рекомендации для обучающихся по теме «Фишинг»:

- **Не открывать ссылки от неизвестных отправителей.** Нужно проверять название ссылки: не перепутаны ли буквы, нет ли лишних символов.
- **Проверять, безопасно ли соединение.** Название сайта должно начинаться с HTTPS и иметь значок закрытого замка. Это означает, что соединение защищено, и данные автоматически шифруются.
- **Никому не сообщать свои пароли, логины, пин-коды и другие личные данные.** Даже по телефону.
- **Не вводить пароли и логины на сторонних сайтах.**
- **Установить антивирусную программу и регулярно её обновлять.**
- **Получив письмо от друга с вложением, уточнить, было ли оно отправлено им или его взломали.**
- **Везде, где есть возможность, подключить двухфакторную аутентификацию.**
- **Не осуществлять оплату, используя общественный Wi-Fi.**
- **Обращать внимание на дизайн сайта.** Орфографические ошибки, небрежная верстка, неработающие кнопки и ссылки — всё это указывает, что сайт не настоящий.
- **Быть осторожным при переходе по ссылкам, нажимать рекламу или взаимодействовать с публикациями в социальных сетях.**
- **Скачивать ПО только из надёжных источников и внимательно изучать исполняемые файлы.**

8. Заключение

Актуальность представляемой темы определена вызовами цифровизации образования и поисками ресурсов повышения цифровой гигиены и безопасности воспитания детей и подростков.

Понятие «цифровая гигиена» стремительно набирает популярность, но в контексте воспитания оно не рассматривалось, в связи с этим нет четкого его сущностно-смыслового содержания.

Проведённый нами анализ научной литературы показал, что в науке сложилось четыре подхода к пониманию понятия «цифровая гигиена», но ни один из них не раскрывает сути феномена «цифровая гигиена в воспитании».

В современное воспитание термин «цифровая гигиена» вошёл недавно и приобрёл огромную популярность в связи с развитием контента дистанционного образования. В научной литературе мы встречаем описание ключевых особенностей мира, в котором сейчас живём: хрупкость, тревожность, нелинейность, непостижимость. Для успешной жизни в таком мире необходимы новые навыки, качества и компетенции, в том числе и личные гибкие качества организатора с критическим мышлением, компетенцией работать в команде, мотивацией к непрерывному самообразованию и самовоспитанию.

Катализатором перемен, в том числе и в образовании, выступила пандемия. Цифровая гигиена сегодня как феномен, является актуальным и в воспитании, в целом трактуется как знания и правила потребления информации

в современном мире ТВ и Интернета, позволяющие сохранить ментальное здоровье, финансы и собственную идентичность.

Социальные сети, блог-платформы и телевидение создают возможности для безопасного пользования, но в результате отсутствия элементарных навыков и компетентности многие из нас оказываются в цифровой ловушке.

Актуальность раскрываемой нами научной проблемы определена следующими вызовами:

1. Усиление рисков жизнедеятельности человека в цифровом пространстве.

2. Дискурс здоровья и благополучия современного человека как ценность и принципы жизни всё больше стимулирует интерес к качеству воспитательной среды с точки зрения её безопасности.

3. Безопасность воспитательной деятельности неизбежно мотивирует поиск инструментов её оценивания.

4. В условиях устойчивой неопределённости и угроз гигиенической безопасности необходима система под подготовки и определения роли педагога в решении задач воспитательной деятельности.

5. Научная тенденция поиска основ гигиенической оценки в теории и практике воспитания.

Исследование темы цифровой гигиены в воспитании детей и подростков даст возможность на методолого-теоретическом уровне раскрыть содержание понятия, а на практическом уровне – использовать рекомендации по организации цифровой гигиены в воспитательной деятельности образовательной организации. Чтобы сохранить способность здраво мыслить и рассуждать и действовать, необходимы знания о цифровой гигиене.

Большая часть информации разрушительна и направлена на продвижение моделей поведения, характерных для общества потребителей, понижение интеллектуального и нравственно-духовного уровня личности пользователей, борьбу с традиционными семейными и нравственными ценностями, распространение фейков и социального неблагополучия.

Психолого-педагогический анализ источников обоснования актуальности данной проблематики показал, что поднимаемая нами тема исследования является нераскрытой в аспекте воспитательной деятельности. Обоснование категорий, которые востребованы современным состоянием практической деятельности в сфере воспитания, позволит определить условия, в которых действие цифровых внешних и личностных внутренних факторов не повлечёт отрицательного последствия на психическое здоровье подрастающего поколения.

Изучение теоретико-методологических оснований научных публикаций по данной проблематике позволяет сделать нам вывод, о том, что в науке сложилось общее представление о цифровой гигиене как о своде правил, соблюдение которых позволит личности относительно безопасно использовать информационные технологии и минимизировать риски, связанные с их применением для решения различных задач.

Тема цифровой гигиены в цифровом мире раскрывается в работе D. Thomson, особенности адаптации z-поколения к цифровой среде и

информационная гигиена поднимались в отечественных исследованиях Е.А.Максимовой, И.А. Молодцовой, М.В. Бердника. Автор Д.В. Руденкин анализирует уровень развития навыков цифровой гигиены современной российской молодежи в рамках социологического исследования. В работах Н.В. Шишариной поднимается проблема гигиенической оценки воспитательной деятельности и её безопасности.

В целом изучение литературы показало, что наметилось четыре основных подхода в понимании феномена цифровой гигиены, ядром которой является безопасное поведение личности.

1. Цифровая гигиена рассматривается как инструмент защиты психики человека от деструктивного воздействия цифровых потоков. Этот подход актуален как для отечественных, так и для зарубежных исследователей.

2. Цифровая гигиена понимается как свод правил, соблюдение которых позволяет человеку научиться избегать или минимизировать влияние информационного контента на своё сознание и поведение.

3. Цифровая гигиена представлена как система мер безопасности.

4. Цифровая гигиена как перечень рекомендаций, позволяющих избежать правовых и морально-этических последствий от необдуманных действий в цифровом пространстве. Он представлен в трудах отечественных исследователей, зарубежных работах.

5. Цифровая гигиена рассматривается как комплексная система правил использования цифровых технологий, направленных на минимизирование рисков цифрового общества.

Психолого-педагогический анализ источников обоснования актуальности данной проблематики показал, что поднимаемая нами тема исследования является нераскрытой в аспекте воспитательной деятельности.

Обоснование категорий, которые востребованы современным состоянием практической деятельности в сфере воспитания, позволит определить условия, в которых действие цифровых внешних и личностных внутренних факторов не повлечёт отрицательного последствия на психическое здоровье подрастающего поколения.

Важно в контексте нашего исследования выделить характеристики-основания «цифровой гигиены в воспитании»:

- меры по защите психики детей и подростков (время, анализ, источники);
- свод этических правил для детей и подростков (ограничения, критика, публикации);
- предосторожность от противоправных действий (пароли, отказ от сомнительных контентов).

В основу исследования цифровой гигиены в воспитании детей и подростков взята методология конвергентного подхода (сближения, слияния, интеграция, объединения, схождения смыслов, взаимообогащения).

Конвергентный подход позволил нам провести анализ литературы и теоретическое исследование, разработать и методологически обосновать модель цифровой гигиены в воспитании детей и подростков. В основе модели лежат её три компонента: факторы (фактчекинг и критическое мышление);

качества личности (ответственность: доверие, свобода и безопасность); характеристики-основания (меры по защите психики, свод этических правил, предосторожность от противоправных действий).

8. Рекомендуемый список использованных источников и литературы:

Нормативные документы:

1. Доктрина информационной безопасности Российской Федерации» // Официальный сетевой ресурс Президента России (электронный ресурс). Режим доступа: <http://kremlin.ru/acts/news/53418> (дата обращения: 29.08.2025);
2. Концепция Государственной национальной политики РФ на период до 2025» // Официальный сетевой ресурс Президента России (электронный ресурс). Режим доступа: <http://kremlin.ru/acts/bank/36512> (дата обращения: 29.08.2025)
3. Конституция Российской Федерации (электронный ресурс). Режим доступа: <http://www.constitution.ru> (дата обращения: 29.08.2025).
4. Основы государственной культурной политики» // Официальный сетевой ресурс Президента России (электронный ресурс). Режим доступа: <http://www.kremlin.ru/acts/bank/39208> (дата обращения: 29.08.2025)
5. Стратегия национальной безопасности Российской Федерации // Официальный сетевой ресурс Президента России (электронный ресурс). Режим доступа: <http://www.kremlin.ru/acts/bank/47046> (дата обращения: 29.08.2025)
6. Стратегия развития воспитания в Российской Федерации на период до 2025 года». Официальная публикация // Российская газета 08.06.2015 (электронный ресурс). Режим доступа: <https://rg.ru/2015/06/08/vospitanie-dok.html> (дата обращения: 29.08.2025)
7. Указ Президента Российской Федерации от 09.11.2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» <http://www.kremlin.ru/acts/bank/48502> (дата обращения: 18.09.2025)
8. Указ Президента РФ от 21.07.2020 N 474 "О национальных целях развития Российской Федерации на период до 2030 года" 23 Стратегия цифровой трансформации отрасли науки и высшего образования (утв. в 2021 Минобрнауки России) 24 Oxford Dictionaries. 2022 https://en.oxforddictionaries.com/definition/digital_detox (дата обращения: 18.09.2025)

Рекомендуемая литература

1. Алиева А.А., Иванова П.Ф. Цифровая гигиена для старшего поколения // Сборник научных трудов по итогам конкурсов научных работ. материалы конкурсов научных работ, проведенных Кузбасским институтом ФСИИ России в 2020-2021 учебном году. Новокузнецк, 2021. С. 6-7.

2. Артюхова Ю.В. Ценности и воспитание // Педагогика. 1999. №4. С. 128.
3. Ашманов И. С., Касперская Н. Цифровая гигиена. СПб.: Питер, 2024.-400с.
4. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с.
5. Баюров, А.Е. Виртуальная реальность в образовании / А.Е. Баюров, О.А. Петрова // Актуальные проблемы авиации и космонавтики. – 2019. – Т. 3. – С. 633-635
6. Богданова Д.А. Обучение навыкам для цифровой эры: современный ландшафт // Педагогика информатики. 2020. № 2. С. 1–17. Данильченко П.А., Седина М.С. Цифровая гигиена в социальных сетях как элемент защиты информации // Colloquium-journal. 2018. № 13-8 (24). С. 45–46.
7. Брызгалина Е.В., Станченко С.В. Воспитание как образовательный результат: ценностно-ориентированный подход к оцениванию в системе общего образования // Вестник Российского университета дружбы народов. Серия: Философия. 2021. Т. 25. № 4. С. 574—588. DOI: 10.22363/2313-2302-2021-25-4-574-588).
8. Буракова, И.С. Технологии виртуальной реальности в образовании / И.С. Буракова, О.В. Донева, Ю.А. Баратилова // Университетская наука. – 2021. – №. 1. – С. 135-137
9. Бухтияров И.В. и др. Основы информационной гигиены: концепции и проблемы инноваций. Гигиена и санитария. 2014. 93 (4): 5-9. 2.
10. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014. – 182 с.
11. Волков Б.С. Психология юности и молодости: учеб. для вузов. М.: Трикста, 2006. С. 122.
12. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.
13. Горбунова, Н.В. Применение технологий виртуальной реальности в контексте профессионального образования / Н.В. Горбунова // Проблемы современного педагогического образования. – 2023. – №. 79-1. – С. 131-134
14. Гудинова Ж. В. и др. К вопросу разработки основ информационной гигиены. Современные проблемы науки и образования. 2014. (3): 541-541.
15. Денисова, Т.С. Обзор VR/AR технологий и эффекты от их развития в РФ / Т.С. Денисова, А.А. Осипов // Молодежная школа-семинар по проблемам управления в технических системах имени А.А. Вавилова. – 2020. – Т. 1. – С. 8.
16. Джабраилов, З.А. VR/AR-технологии и их применение / З.А. Джабраилов, И.А. Магомедов, А.М. Багов // Педагогический журнал. – 2021. – Т. 11. – №. 2-1. – С. 166-171

17. Ефремова, С.Г. Исследование влияния VR, AR, MR технологий на качество образования в современном мире и их дальнейшие пути развития / С.Г. Ефремова, Н. А. Морошкин // Моя профессиональная карьера. – 2020. – Т. 2. – №. 11. – С. 187-192
18. Дети в информационном обществе // <http://detionline.com/journal/about> (дата обращения: 18.09.2025).
19. Еремин А.Л. Информационная и цифровая гигиена: Учеб. пособие – С-Пб.: Издательство ЛАНЬ, 2023. – 92 с.
20. Еремин А.Л. Информационная гигиена: современные подходы к гигиенической оценке контента и физических сигналов носителей информации. Гигиена и санитария. 2020. 99 (4): 351-355.
21. Еремин А. Л. К биофизике эволюции интеллектуальных систем //Биофизика РАН – 2022. – Т. 67. – №. 2. – С. 409-416.
22. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.:ЮНИТИ-ДАНА, 2016. – 239 с.
23. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с.
24. Иванов, И.И. Иммерсивные технологии в образовании: перспективы и вызовы / И.И. Иванов // Педагогика. – 2021. – № 1. – С. 10-15
25. Карташева М. И. Роль системы Я в структуре ментальной регуляции психических состояний в процессе учебной деятельности // Ярославский педагогический вестник. 2022. № 1 (124). С. 162-174. <http://dx.doi.org/10.20323/1813-145X-2022-1-124-162-174>.
26. Касперская Н., Ашманов И. Методическое пособие по выявлению признаков риска поведения в социальных медиа. Цифровая гигиена. М.: АО «Крибрум», 2019. 38 с.
27. Кравцов, Б.С. Применение VR-Ar технологий в образовании / Б.С. Кравцов // "Технологическое образование в системе" Школа-Колледж-Вуз": традиции и инновации. – Воронеж: ВГПУ, 2021. – С. 192-196
28. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.
29. Лемэр Л. Г., канд. техн. наук Ашманов И. С., канд. психол. наук Ковалева Ю. В., канд. психол. наук Самосват О. И., Брежнева Т. С., Смагина А. А., Теделури М.М., Курицын А.Н., Шулаева О.В. Цифровая гигиена и работа с большими данными: Сборник материалов предназначен для подготовки преподавателей к проведению занятий вводного модуля программы «Цифровая гигиена и работа с большими данными», реализуемой в рамках проекта Министерства просвещения Российской Федерации «Центры цифрового образования детей “IT-куб”». М., 2021. 30с.<https://kribrum.ru/upload/gigiena-2021.pdf> (дата обращения: 18.09.2025).

30. Максимова Е.А., Молодцова И.А., Бердник М.В. Информационная гигиена как фактор предотвращения последствий Z-цифровизации // Вестник УрФО. Безопасность в информационной сфере. 2018. № 3(29). С. 67–73.
31. Молодцова И.А., Сливина Л.П. Особенности адаптации Z-поколения к цифровой среде: информационная гигиена // Вопросы школьной и университетской медицины и здоровья. 2019. № 4. С. 20–21.
32. Мухамадиева, К.Б. Дополненная и виртуальная реальность в образовании / К.Б. Мухамадиева // Образование и проблемы развития общества. – 2021. – №. 1 (14). – С. 68-75
33. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение, 2019. – 80 с.
34. Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa> (дата обращения: 18.09.2025)
35. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.
36. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности // Студенческий: электрон. научн. журн. 2019. № 22(66) Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.
37. Руденкин Д.В. Уровень развития навыков цифровой гигиены современной российской молодежи: итоги социологического исследования // Социодинамика. 2022. № 1. С. 36-55. DOI: 10.25136/2409-7144.2022.1.37487 URL: https://nbpublish.com/library_read_article.php?id=3748 (дата обращения: 18.09.2025).
38. Шишарина Н.В. Гигиеническая оценка воспитательной деятельности и критерии её безопасности // Народное образование. 2022. № 6. С. 171–179.
39. Шишарина Н.В., Ромм Т.А. Гигиеническая оценка в теории и практике воспитания. Образование и саморазвитие. 2021, 16 (3) С. 261–277. DOI: 10.26907/esd.16.3.23.
40. Федорова С.Н., Голикова Н.Д. Цифровая компетентность субъектов образовательного процесса // Вектор науки Тольяттинского государственного университета. Серия: Педагогика, психология. 2022. №3. С.36-42
41. Хозе, Е.Г. Виртуальная реальность и образование / Е.Г. Хозе // Современная зарубежная психология. – 2021. – Т. 10. – №. 3. – С. 68

9. Глоссарий основных понятий и терминов по цифровой гигиене

Информационная гигиена. Раздел системы знаний, изучающий влияние информации на здоровье, работоспособность человека и продолжительность его жизни.

Big Data. Обозначение структурированных и неструктурированных данных огромных объёмов и многообразия, обрабатываемых программными инструментами.

Хаб данных. Особый класс онлайн-информационных систем, представляющих собой совокупность данных из нескольких источников, организованных для распространения и совместного использования.

Цифровая детоксикация (Digital detox). Период времени, когда человек добровольно воздерживается от использования цифровых устройств, таких как смартфоны, компьютеры и платформы социальных сетей.

Цифровая гигиена на рабочем месте. Правила, которые должен соблюдать каждый сотрудник во время работы с электронными устройствами и интернетом.

Конфиденциальность. Не нужно вводить рабочие пароли на сторонних сайтах, сообщать учётные данные посторонним и публиковать корпоративную информацию в открытом доступе.

Менеджер паролей. Приложение для компьютера или смартфона, которое помогает создавать, сортировать и хранить данные для доступа.

Не переходить по подозрительным ссылкам. Это могут быть фишинговые ресурсы, их цель – получить персональные данные, которые могут использовать для подделки документов и других незаконных действий от имени компании.

Не пользоваться незащищёнными сетями. Если сотрудник работает удалённо, он не должен подключаться к бесплатному Wi-Fi в кафе и других общественных местах, потому что у публичных сетей обычно нет защиты от перехвата данных.

Регулярно обновлять ПО и антивирус. Установить софт, который предупреждает об угрозах, и объяснить удалённым работникам, как следить за актуальностью сервисов.

Спам-фильтр. Инструмент, который распознаёт и блокирует подозрительные письма.

Информационная гигиена – раздел системы знаний, изучающий закономерности влияния информации на индивидуальное и общественное здоровье, работоспособность человека, продолжительность его жизни и разрабатывающий практические мероприятия по оздоровлению информационной среды и оптимизации интеллектуальной деятельности.

Информация – это: 1. сведения (сообщения, данные) независимо от формы их представления; 2. это данные, определены в контексте и поэтому являются интерпретируемыми; данные создаются путем моделирования или измерений объектов реального мира.

Гигиена (греч. «здоровый») – раздел медицины, изучающий влияние жизни и труда на здоровье человека и разрабатывающий меры (санитарные нормы и правила), направленные на предупреждение заболеваний, обеспечение оптимальных условий существования, укрепление здоровья и продление жизни, изучающая влияние факторов окружающей среды на здоровье человека, его работоспособность и продолжительность жизни, разрабатывающий нормативы,

требования и санитарные мероприятия, направленные на оздоровление населённых мест, условий жизни и деятельности людей.

Информационное общество – общество, в котором информация и уровень её применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан.

Здоровье – состояние полного физического, психического и социального благополучия, а не только отсутствие болезней и физических дефектов.

Знания (knowledge): информация об объектах, событиях, понятиях и правилах, их отношениях и свойствах, систематизированная для целевого регулярного использования.

Информационная система – система обработки информации вместе с соответствующими организационными ресурсами, такими как человеческие, технические и финансовые ресурсы, которая предоставляет и распределяет информацию.

Природа сигналов-носителей информации – физическая (визуальная, аудиальная, тактильная, вестибулярная), химическая (обонятельная, вкусовая), физическая и химическая (интероцептивная - от внутренних органов). Некоторые параметры и характеристики физических сигналов-носителей информации определены в нормативных документах.

Право на доступ к информации – граждане и организации вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных федеральными законами.

Запрещенная к распространению информация (в России) - материалы с порнографическими изображениями несовершеннолетних, информация о способах разработки наркотических средств, совершения самоубийства, самодельного изготовления взрывчатых веществ и пр.

Умственные функции – общие умственные функции: сознания, ориентированности, интеллектуальные, психосоциальные, темперамент и личностные функции, волевые и побудительные, сна (МКФ, код b110-b139); специфические умственные функции: внимания, памяти, психомоторные, эмоций, восприятия, мышления, познавательные высокого уровня, речи, вычисления, последовательных сложных движений, самоощущения и ощущения времени (МКФ, код b140-189).

Интеллект – разум, рассудок, умственные способности: учиться из опыта, приспосабливаться, адаптироваться к новым ситуациям, применять знание, чтобы управлять окружающей средой или мыслить абстрактно. 8 Интеллектуальные функции – общие умственные функции, требующиеся, чтобы понимать и конструктивно объединять различные умственные функции, включая все познавательные функции и их развитие на протяжении жизни (МКФ, код b117).

Интеллектуальная система (ИС) – совокупность взаимодействующих между собой относительно элементарных структур и процессов, объединенных в целое выполнением функции интеллекта, несводимой к функции ее компонентов. Признаки И.С.: взаимодействует со средой и другими системами

как единое целое; состоит из иерархии подсистем более низкого уровня; способность логически и творчески активно отражать объективную реальность, целенаправленно, опосредованно и обобщенно познавать существенные связи и отношения вещей.

Ноогенез – процесс появления, развёртки в пространстве и развития во времени интеллектуальных систем. Ноогенез представляет собой совокупность закономерных, взаимосвязанных, характеризующихся определенной временной последовательностью структурных и функциональных преобразований всей иерархии и совокупности взаимодействующих между собой относительно элементарных структур и процессов.

Скорочтение (speed reading), быстрое чтение, глоссерное чтение – способность быстрого восприятия текстовой информации при использовании особых способов чтения.

Мнемоника, мнемотехника – совокупность специальных приёмов и способов, облегчающих запоминание нужной информации и увеличивающих объём памяти путём образования ассоциаций (связей): замена абстрактных объектов и фактов на понятия и представления, имеющие визуальное, аудиальное или кинестетическое представление, связывание объектов с уже имеющейся в памяти информацией, различные модификации для упрощения запоминания.

Ноотропные средства – фармакологические препараты (ноотропы), оказывающие активирующее влияние на обучение, улучшающие память и умственную деятельность, объединенные в группу с психостимуляторами (АТХ, код N06BX).

Прикладная психология — это использование психологических методов для решения практических проблем в образовании, управлении, эргономике, здравоохранении, с областями: школьная, спортивная, общественная психология, промышленная, организационная, инженерная психология, психология гигиены труда, психоанализ, нейропсихология и психиатрия, психическое здоровье, медицинская и клиническая психология и др.

Психофизика – количественно исследует взаимосвязь между физическими стимулами и появляющимися в результате их воздействия ощущениями и восприятиями.

Информационная экология – это наука, изучающая закономерности влияния информации на формирование и функционирование интеллектуальных биосистем и их здоровье включая человека, человеческие сообщества и человечество в целом, ставящая своей задачей развитие методов совершенствования информационной среды.

Информационная этика – рассматривает влияние информационных и коммуникационных технологий (ИКТ) на общество и окружающую среду, этические вопросы, связанные с интернетом и средствами связи, вопросы конфиденциальности, информационных перегрузок, интернетзависимость, цифрового разрыва, видеонаблюдения, навигации и робототехники, которые являются предметом обсуждения и требуют межкультурного контроля.

Поиск знаний – извлечение знаний стремится возвращать информацию в структурированной форме, соответствующей когнитивным процессам человека, в отличие от простых списков элементов данных. Он опирается на ряд областей, включая эпистемологию (теорию познания), когнитивную психологию, когнитивную нейронауку, логику и логический вывод, машинное обучение и обнаружение знаний, лингвистику и информационные технологии.

Количество информации – наименование величины; единицы количества информации – бит и байт (Б) (соотношение $1 \text{ Б} = 8 \text{ бит}$); единица информации в двоичной системе счисления; термин используют в устройствах цифровой обработки и передачи информации, например в цифровой вычислительной технике (компьютерах), для записи объема запоминающих устройств, количества памяти, используемой компьютерной программой.

Скорость передачи информации – внесистемная единица величин. Единицы – бит/с и байт/с. Область применения – информационные технологии и связь.

Интерфейс – общая граница (пространство) между двумя функциональными единицами, определяемая различными характеристиками, относящимися к функциям, физическим обменам сигналами с целью передачи информации. Обмен может происходить между компьютерным оборудованием и людьми, а также программным обеспечением, периферийными устройствами и их комбинациями. Человеко-машинный интерфейс: дисплейный (текстовый, графический), звуковой (речевой, неречевой).

Качество данных – связано с измерениями: доступность, полнота, переносимость, безопасность, своевременность, точность, интерпретируемость, достоверность, происхождение, актуальность, соответствие, согласованность и ремонтпригодность, объединяемых в три категории: доступность, информативность и удобство использования.

Качество информации (InfoQ) – это потенциал набора данных для достижения конкретной (научной или практической) цели с использованием данного метода эмпирического анализа.

Клипковая культура (clip culture) – термин, для описания культуры развитых стран, определяемой господством свойственным средствам массовых коммуникаций способа представления и восприятия информации.

Интернет-мем, мем - идея, поведение, стиль или изображение, которые распространяются через Интернет, часто через платформы социальных сетей.

Информационно-зависимые заболевания – «цифровые», заболевания, связанные с информационно-компьютерными технологиями (ИКТ), информационными перегрузками, нервно-эмоциональным перенапряжением – факторами риска болезней: психических, сердечно-сосудистой системы (инфаркты, инсульты, ишемическая болезнь сердца), пищеварительной системы (язвенная болезнь); повышению уровня травматизма и суицидов, состояниям тревоги и депрессии, биполярных аффективных расстройств, панических расстройств, синдрома дефицита внимания и гиперактивности (СДВГ), игровых расстройств – зависимости (аддикции) от компьютерных игр; а также: компьютерного синдрома, аддикций – патологических зависимостей от телевидения, от социальных сетей, фобий – номофобия; маний – сенсорных,

связанных с интернетом; депрессий, формируемых социальными сетями; интернет-зависимых суицидов и пр.

Цифровая трансформация – цель развития Российской Федерации на период до 2030 года; комплексное преобразование деятельности участников отрасли и органов исполнительной власти, связанное с переходом к новым бизнес-моделям, каналам коммуникаций, а также процессам и культуре, которые базируются на новых подходах к управлению данными с использованием цифровых технологий.

Цифровое образование – проект, направленный на повышение уровня цифровых компетенций обучающихся, научно-педагогических работников, а также формирования компетентной команды управления процессом цифровой трансформацией.

Цифровой университет – проект, направленный на создание и развитие цифровых сервисов в сфере науки и высшего образования, охватывающих все виды бизнес-процессов образовательных организаций высшего образования, направленных на удовлетворение потребностей всех участников образовательного процесса.

Big Data – обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия, обрабатываемых горизонтально масштабируемыми программными инструментами.

Хаб данных – особый класс онлайн информационных систем, представляющих собой совокупность данных из нескольких источников, организованных для распространения и совместного использования.

Цифровая детоксикация (Digital detox) – это период времени, когда человек добровольно воздерживается от использования цифровых устройств, таких как смартфоны, компьютеры и платформы социальных сетей. Развиваются тренды цифровая диета (digital dieting), цифровой аскетизм (digital asceticism) и др.

Цифровое здоровье (здравоохранение) (Digital health) – область знаний и практики, связанная с разработкой и использованием цифровых технологий для улучшения здоровья; расширяет концепцию здоровья, включая в нее цифровых потребителей с более широким спектром интеллектуальных устройств и подключенного оборудования; охватывает другие виды использования цифровых технологий в здравоохранении, такие как Интернет вещей, искусственный интеллект, большие данные и робототехника.

Искусственный интеллект (ИИ) (artificial intelligence, AI): способность приобретать, обрабатывать, создавать и применять знания, определенные в форме модели, для выполнения одной или нескольких поставленных задач. Комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека. Искусственный интеллект – это область компьютерных наук, в которой особое внимание уделяется моделированию процессов человеческого интеллекта машинами, которые работают и реагируют как люди.

Кибербезопасность – область, занимающаяся защитой информации, систем и сетей от несанкционированного доступа, утечек данных, вредоносных программ и других киберугроз.

Информационная безопасность – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Информационная безопасность – правильная защита «цифровых следов».

Социальная инженерия – набор методов и практик, которые заставляют человека выполнить какие-либо действия – необязательно в его интересах.

Фишинг – основной вид интернет-мошенничества и основной способ для злоумышленников проникнуть в локальные сети компании. Используется для кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Массовые атаки – злоумышленники берут за основу несколько самых популярных интернет-сервисов, формируют легенду и рассылают тысячи писем через различные адреса.

Таргетированные атаки – персонифицированные и целенаправленные атаки; сбор и систематизация данных о жертве.

Генеративный искусственный интеллект — это тип ИИ, который может создавать новый контент и идеи, включая диалоги, истории, изображения, видео и музыку. Как и любой ИИ, он основан на моделях машинного обучения, предварительно обученных на огромных объёмах данных.

Цифровая личность – это совокупность информации, которую человек оставляет в виртуальной среде. Она включает данные о прошлом, настоящем, увлечениях, интересах, а также социальные взаимодействия и действия в сети.

Некоторые уровни цифровой личности:

- **Идентификационный.** Включает базовую информацию о личности, такую как имя, возраст, пол, образование. Этот уровень формируется пользователем при регистрации на сайтах, в социальных сетях и других сервисах.

- **Коммуникативный.** Отражает способность индивида к общению в интернете, стиль общения, предпочтения в выборе коммуникационных платформ.

- **Информационно-контентный.** Включает информацию, которую пользователь генерирует и распространяет в сети, например, посты в социальных сетях, блоги, комментарии.

- **Поведенческий.** Включает в себя паттерны поведения пользователя в интернете, его активность, предпочтения, привычки и интересы.

Цифровая среда – это пространство, созданное с помощью компьютерных технологий, интернета и электронных устройств, в котором происходит обмен информацией, общение, обучение, работа и развлечения. В такой среде информация представлена в цифровой форме, а коммуникация происходит через электронные средства.

Цифровая среда имеет виртуальную и материальную составляющие: виртуальная – это пространство, где происходит взаимодействие, материальная – технические устройства, обеспечивающие взаимодействие.

Компоненты

Некоторые элементы цифровой среды:

- **Интернет** – глобальная сеть, обеспечивающая доступ к информации, общению и онлайн-сервисам.
- **Социальные сети** – платформы, где люди общаются, обмениваются мнениями и контентом.
- **Образовательные ресурсы** – онлайн-курсы, видеоуроки, библиотеки.
- **Электронная коммерция** – интернет-магазины, платформы для продаж и покупок.
- **Цифровые сервисы** – банковские приложения, госуслуги, облачные хранилища.
- **Виртуальная и дополненная реальность** – технологии, позволяющие создать искусственные диджитал-миры.

Виды

Цифровая среда затрагивает различные сферы жизни, например:

- **Образование** – дистанционное обучение, онлайн-курсы, электронные учебники и тестирования.
- **Работа и бизнес** – удалённая работа, онлайн-конференции, документооборот.
- **Общение** – социальные сети, мессенджеры, видеозвонки позволяют оставаться на связи с родными и друзьями.
- **Развлечения** – онлайн-игры, стриминговые сервисы, виртуальные туры.

Влияние

Цифровая среда создаёт новые возможности для общения, обучения, работы и развлечений, но также поднимает вопросы, связанные с приватностью и безопасностью в цифровой среде, этичным и экологичным использованием цифровых технологий. Например:

Цифровизация образования – интерактивные методы обучения, технологии адаптивного обучения, которые настраиваются под индивидуальные особенности учеников.

Цифровая трансформация бизнеса – компании активно внедряют цифровые технологии в свои бизнес-процессы, стремясь повысить эффективность, гибкость и конкурентоспособность в быстро меняющейся среде.

Регулирование

Развитие цифровой среды требует комплексного подхода, включающего совершенствование нормативно-правовой базы, развитие инфраструктуры, повышение цифровой грамотности населения и активное сотрудничество всех заинтересованных сторон. Однако этот процесс сопряжён с рядом вызовов, требующих комплексного подхода к их решению.

Например:

- обеспечение кибербезопасности, защита конфиденциальности данных;
- преодоление цифрового неравенства;
- решение этических вопросов.

Цифровая культура – это новая форма взаимодействия человека с миром, сформированная под влиянием цифровых технологий. Она включает в себя знания, нормы, ценности и модели поведения, связанные с использованием цифровых инструментов в различных сферах жизни.

Некоторые составляющие цифровой культуры:

- **Цифровая грамотность.** Способность эффективно использовать цифровые устройства, интернет и программное обеспечение, навыки поиска, анализа и критической оценки информации.
- **Этика и цифровая безопасность.** Соблюдение норм поведения в онлайн-среде (сетевой этикет), ответственное отношение к персональным данным и конфиденциальности.
- **Креативность и самовыражение.** Использование технологий для творчества: графический дизайн, музыка, анимация, виртуальная реальность. Развитие цифровых форм искусства и контента (NFT, цифровая мода, 3D-моделирование).
- **Коллективная работа и коммуникация.** Онлайн-обучение, дистанционная работа, коллаборация в облачных сервисах, развитие виртуальных сообществ и платформ для обмена опытом.
- **Технологическая адаптивность.** Готовность к освоению новых технологий, таких как искусственный интеллект, метавселенные, блокчейн. Способность критически оценивать влияние технологий на общество.

Цифровая культура помогает людям адаптироваться, работать и учиться эффективнее, а также безопасно и этично взаимодействовать с цифровой средой.

Блокчейн (от англ. block – «блок, модуль» и chain – «цепочка») – технология хранения и передачи данных в виде цепочки блоков. Каждый блок содержит информацию о транзакциях, связан с предыдущим и защищён с помощью криптографии.

Особенности:

- Нет единого центра управления или сервера, на котором хранятся все данные.
- Информация распределена на множестве узлов по всему миру, каждый узел (компьютер) содержит полную копию всех блоков.
- Изменить информацию в одном блоке без изменения всех последующих невозможно, что делает систему устойчивой к подделкам.

Бот (сокращение от «робот») – компьютерная программа, которая может выполнять различные задачи автоматически. Боты могут имитировать действия пользователя или полностью заменять его.

Некоторые виды ботов:

- **Чат-боты.** Общаются с пользователями в режиме реального времени, предоставляют информацию, решают типовые вопросы,

поддерживают клиентов. Примеры: боты в мессенджерах (Telegram, WhatsApp), на сайтах компаний, в мобильных приложениях.

- **Боты-помощники.** Автоматизируют рутинные задачи, такие как бронирование билетов, заказ еды, управление умным домом. Примеры: Google Assistant, Siri, Alexa.

- **Боты-виртуальные ассистенты.** Оказывают персонализированную помощь пользователям, напоминают, планируют задачи. Примеры: корпоративные боты для сотрудников, персональные ассистенты для отдельных пользователей.

- **Боты-пауки (краулеры).** Индексируют веб-страницы для поисковых систем, собирают данные для анализа рынка. Примеры: Googlebot, Bingbot.

- **Боты для считывания веб-страниц.** Извлекают структурированные данные с веб-сайтов (цены, характеристики товаров, новости).

- **Боты для мониторинга.** Отслеживают состояние веб-сайтов, серверов, социальных сетей.

- **Социальные боты.** Имитируют поведение реальных пользователей в социальных сетях, распространяют информацию, манипулируют общественным мнением.

- **Боты для совершения покупок.** Автоматически покупают товары онлайн, мониторят цены, участвуют в аукционах.

Боты могут быть и **вредоносными программами**, которые используют для получения полного контроля над компьютером.

Чак бот – продвинутый вариант чат-бота с расширенными возможностями анализа данных и автоматизации процессов.

Некоторые особенности чак ботов:

- способны обрабатывать до 500 различных параметров одновременно, включая историю взаимодействия, временные метки и эмоциональный окрас сообщений;

- могут не только отвечать на стандартные вопросы, но и анализировать поведение пользователя, предлагать персонализированные решения и даже прогнозировать будущие запросы;

- используют сложные нейросетевые модели для анализа контекста разговора, что позволяет создавать более естественные и продуктивные диалоги;

- отличаются высокой степенью интеграции с существующими CRM-системами и другими корпоративными приложениями.

Нейросеть – это программа, которая работает по аналогии с человеческим мозгом: обучается и «принимает решения». Она анализирует полученные данные, находит в них закономерности и делает выводы.

В основе нейросети лежат алгоритмы, которые заточены на обработку информации (например, текстов, изображений или музыки).

Некоторые типы нейросетей и их задачи:

- **Полносвязные (feedforward).** Самый простой тип, где каждый нейрон соединён со всеми следующими. Такие нейросети используют для классификации данных и прогнозирования.
- **Свёрточные (CNN).** Специализируются на изображениях: «разбивают» картинку на слои, анализируют её и распознают объекты.
- **Рекуррентные (RNN).** Анализируют последовательности и помогают, например, в составлении прогнозов погоды или переводе текста.
- **Генеративные (GAN).** Генерируют – создают тексты (ChatGPT), музыку (Suno), изображения (Midjourney) и другие данные.

Нейросети применяются во многих сферах жизни – от маркетинга до медицины. С помощью нейросетей можно автоматизировать рутинные процессы и значительно сэкономить время на выполнение задач. Однако стоит помнить, что иногда нейросети могут ошибаться, и информацию нужно перепроверять

Chat GPT – умный чат-бот на русском языке, который помогает с анализом данных, генерацией текстов, программированием, обучением, переводами и решением повседневных задач.

Мессенджер (от англ. messenger – посыльный, курьер) – это программа для мгновенного обмена текстовыми сообщениями и мультимедиа между зарегистрированными пользователями через интернет.

Основная цель мессенджеров – обеспечить удобный и быстрый способ общения в реальном времени. В современных мессенджерах часто есть функции звонков, видеосвязи, групповых чатов и интеграции с другими сервисами.

Некоторые виды мессенджеров:

- **Текстовые** – предоставляют возможность общения через текстовые сообщения.
- **Голосовые** – позволяют пользователям общаться голосом, не звоня друг другу.
- **Видеомессенджеры** – предлагают возможность видеозвонков и видеоконференций.
- **Многофункциональные** – сочетают в себе ряд вышеперечисленных функций.

Примеры популярных мессенджеров: WhatsApp, Telegram, Facebook Messenger, Viber, WeChat, Signal, Slack, Microsoft Teams.

Использовать мессенджер можно на компьютере, смартфоне или планшете – в приложении либо веб-версии для браузера.

Браузер – это программа для просмотра веб-страниц, которая преобразует получаемый из сети код в понятные для человеческого восприятия элементы и позволяет управлять ими. Название происходит от английского слова browse – просматривать.

Некоторые функции браузеров:

- позволяют скачивать на устройство пользователя файлы любого типа;
- хранят ссылки, пароли, историю посещений, платёжную информацию;

- позволяют общаться в социальных сетях, по email, через чаты и форумы;
- позволяют получать онлайн-образование;
- защищают от вирусов и блокируют рекламу;
- переводят страницы с иностранного языка;
- дают возможность для кастомизации интерфейса;
- поддерживают расширения и виджеты.

Браузеры делятся на десктопные и мобильные. Десктопные предназначены для работы на компьютерах и ноутбуках, мобильные – для смартфонов и планшетов.

Некоторые популярные браузеры в 2025 году:

- **Google Chrome.** Известен самой большой в мире библиотекой расширений, которая позволяет гибко настраивать его под свои нужды. В 2025 году в Chrome появились ИИ-функции (поиск и анализ контента) и новый режим энергосбережения.

- **Brave.** Защищённый браузер на базе Chromium, построенный на принципах приватности пользователей и высокой скорости работы. Блокирует раздражающую рекламу и предотвращает мониторинг активности в Интернете, ускоряя загрузку веб-страниц.

- **Opera One.** Новая версия браузера Opera с полностью обновлённым интерфейсом и полезными функциями, включая модульный дизайн, острова вкладок, встроенную блокировку рекламы (adblock) и чат-бот Agia на базе ИИ.

Информационно-коммуникационные технологии (ИКТ) – это совокупность способов, механизмов и средств, используемых для сбора, обработки, хранения и передачи информации.

Некоторые виды ИКТ:

- **Компьютеры и ноутбуки** – позволяют проводить различные вычисления и работать с разнообразными программами и приложениями.

- **Интернет** – предоставляет доступ к огромному объёму информации и ресурсам.

- **Мобильные устройства** – расширяют возможности доступа к информации и общению с помощью приложений, электронной почты, мессенджеров и других сервисов.

- **Электронные учебники и материалы** – обогащают обучение различными элементами, такими как видео, аудио и интерактивные задания.

- **Вебинары и видеоконференции** – позволяют проводить образовательные мероприятия и лекции в режиме реального времени без привязки к месту.

- **Интерактивные доски** – предоставляют возможность ученикам взаимодействовать с учебным материалом.

- **Образовательные платформы и онлайн-курсы** – открывают доступ к различным курсам и обучающим программам, которые можно изучать в удобное время.

- **Электронные тесты и оценка** – позволяют оценивать знания учеников.

- **Облачные технологии** – предоставляют возможность хранения и обмена информацией и ресурсами в облаке, что облегчает совместную работу и доступ к данным из разных мест.

Сетевая личность – личность, использующая возможности сети для решения личностных и общественных проблем.

Некоторые особенности сетевой личности:

- **Сетевая мобильность.** Способность действовать в ситуации неопределённости в сети, использовать опыт коллективного субъекта для решения конкретных проблем, быть готовым помочь другим нуждающимся.

- **Рефлексивная позиция.** Способность выявлять стереотипы своего поведения, смотреть на себя глазами других людей, помогать другим людям отрефлексировать свои действия и т. д..

- **Устойчивость к неопределённости.** Способность к познанию, созданию знаний.

- **Критическое мышление.** Системное, диалектическое мышление.

- **Принадлежность к профессиональному сообществу.** Например, к науке.

Сетевая идентичность» (также виртуальная идентичность, интернет-идентичность, онлайн-идентичность, интернет-личность). Это совокупность гипертекстовых компонентов сетевого облика индивида, формируемого им в рамках онлайн-среды с целью самопрезентации и отражающего реальные аспекты его личности. Главным отличием сетевой идентичности от реальной является возможность индивида полностью контролировать первую, корректировать её по своему усмотрению, чтобы представлять перед другими пользователями в нужном ему свете.

Виртуальная реальность (VR, англ. virtual reality) – технология, которая погружает пользователя в искусственно созданный трёхмерный цифровой мир так, что он кажется реальным. Для этого используется специальное оборудование: VR-очки или шлем, сенсоры движения, контроллеры.

Дополненная реальность (AR, Augmented Reality) – технология, которая позволяет накладывать цифровые объекты на реальное окружение пользователя в режиме реального времени. В отличие от виртуальной реальности (VR), AR дополняет существующую реальность виртуальными элементами: 3D-моделями, текстом, изображениями или анимацией. Дополненная реальность – результат введения в зрительное поле любых сенсорных данных с целью дополнения сведений об окружении и изменения восприятия окружающей среды. Пример: во время видеоконференции пользователь меняет фон позади себя на космическое пространство или офисный интерьер – использует базовый принцип AR-технологии.

Иммерсивная среда в образовании (от англ. immersion – «погружение») – это смоделированная с помощью цифровых технологий среда, которая позволяет учащимся полностью погрузиться в учебный процесс. Вместо пассивного восприятия информации учащиеся взаимодействуют с контентом, отбатывают навыки в реальных ситуациях и учатся через практику.

Цель иммерсивного обучения – сделать учебный процесс более интерактивным, увлекательным и эффективным, помочь развивать ключевые навыки, такие как критическое мышление, решение проблем и сотрудничество.

Для создания иммерсивных сред в образовании используют **виртуальную реальность (VR)** и **дополненную реальность (AR)**.

- **VR** создаёт полностью искусственную среду, где ученики взаимодействуют с 3D-моделями, симуляциями и виртуальными объектами.

- **AR** не погружает пользователя в виртуальное окружение, а дополняет реальный мир виртуальными объектами и информацией. Например, на окружающий мир с помощью камеры смартфона накладываются цифровые элементы: картинки, 3D-объекты, анимацию.

Технологии

Для VR и AR используют **специальные устройства** (шлемы, очки, сенсорные экраны) и **программное обеспечение**. Например:

- **VR-очки** или **шлемы** создают ощущение присутствия в виртуальном мире.

- **Платформы для разработки AR-приложений** (Vuforia, ARKit и ARCore) обеспечивают распознавание объектов, анализ освещения и точное размещение виртуальных элементов в окружающей среде.

Примеры

- **Виртуальные экскурсии** по историческим местам или научным явлениям в 3D-формате. Например, проект Google Expeditions позволяет учителям проводить виртуальные экскурсии по всему миру.

- **Интерактивные уроки** с виртуальными симуляциями, где ученики могут экспериментировать и изучать различные явления и процессы. Например, они могут исследовать атомную структуру вещества или изучать законы физики, взаимодействуя с виртуальными моделями и симуляциями.

- **Виртуальные лаборатории**, где ученики могут выполнять эксперименты и исследования в безопасной и контролируемой среде. Например, они могут изучать химические реакции, физические законы или биологические процессы, имитируя их в виртуальной среде.

Исследования подтверждают преимущества иммерсивных технологий для обучения.

Например:

- Иммерсивный опыт улучшает запоминание сложных или абстрактных тем, основанных на неосознаваемых концепциях.

- Технологии помогают развивать процедурные навыки в различных областях, например, студенты-инженеры и медики, использовавшие технологии виртуальной реальности, продемонстрировали лучшие результаты в работе с оборудованием и хирургических навыках по сравнению с традиционными методами обучения.

Однако внедрение иммерсивных технологий в образовательный процесс также сопряжено с вызовами. Например, необходимы значительные

инвестиции в оборудование и программное обеспечение, что может стать барьером для многих образовательных учреждений.

Психодиагностика цифровых образовательных сред (ЦОС) – это направление педагогической психологии, изучающее психологические аспекты взаимодействия человека с цифровыми технологиями в обучении. Оно включает исследования, связанные с:

- влиянием цифровых сред на когнитивные процессы, мотивацию, эмоциональное состояние и социальные взаимодействия обучающихся;
- эффективностью и доступностью цифровых образовательных ресурсов;
- методами оценки и диагностики, нацеленными на совершенствование процесса обучения в цифровой среде.

Предмет

Психодиагностика ЦОС изучает:

- Психологические особенности управления учебно-воспитательным процессом в условиях цифровизации образовательной среды.
- Психолого-педагогические аспекты технологизации и информатизации образовательной среды.
- Психологические закономерности развития учебных групп и их влияние на продуктивность учебной деятельности обучающихся.

Методы

Для психодиагностики в ЦОС используются, следующие методы:

- Компьютерные системы психодиагностики – автоматизируют подсчет и интерпретацию результатов тестирования, что снижает ошибки при их обработке вручную.
- Компьютерное адаптивное тестирование способностей обучающихся – обеспечивает более высокую точность измерений в отличие от классических тестов.
- Наблюдение за мимикой, эмоциями, жестами субъекта диагностики, обработка визуальной и аудиальной информации – позволяет собрать диагностический материал для нейронного анализа.

При этом психодиагностика в ЦОС может сочетать методы, необходимые для полной психологической диагностики участников образовательного процесса.

Задачи психодиагностики ЦОС:

- Выявление психологических особенностей участников образовательного процесса в условиях цифровизации.
- Разработка психолого-педагогических рекомендаций на основе психодиагностики, которые можно использовать в учебном процессе.
- Оценка эффективности психодиагностических практик в ЦОС – например, выявление, насколько они способствуют совершенствованию процесса обучения.

Вредоносное ПО (malware) – это программа или файл, специально разработанные для нанесения вреда компьютеру, сети, серверу или пользователю. Оно действует путём: кражи, шифрования или удаления конфиденциальных данных; изменения или захвата основных вычислительных

функций; отслеживания действий пользователя на компьютере без его разрешения.

Некоторые типы вредоносного ПО:

- **Вирусы** – прикрепляются к файлам или документам, активируются только после того, как пользователь откроет заражённый файл.
- **Сетевые черви** – распространяются по сети самостоятельно, не требуют прикрепления к файлам или приложениям.
- **Троянские программы (трояны)** – маскируются под легитимное программное обеспечение, чтобы обманом заставить пользователя установить их. После установки троян может выполнять скрытые действия: похищать конфиденциальные данные, открывать доступ к устройству или изменять системные настройки.
- **Шпионское ПО** – действует незаметно для пользователя, собирает персональную информацию: пароли, данные банковских карт, историю браузера и даже записи нажатий клавиш (кейлоггинг).
- **Программы-вымогатели (ransomware)** — шифруют файлы на устройстве и требуют выкуп за их разблокировку.

Способы распространения

Вредоносное ПО может распространяться через:

- **Фишинговые атаки** – электронные письма с вредоносными вложениями или ссылками, которые обманом заставляют пользователей установить вредоносное ПО.
- **Физические носители** – например, USB-накопители, которые могут переносить вредоносное ПО непосредственно в систему.
- **Скрытые загрузки** – веб-сайты, которые автоматически загружают вредоносное ПО без согласия пользователя.

Методы обнаружения

Для обнаружения вредоносного ПО используют, например:

- **Сигнатурный анализ** – обнаруживает вредоносные программы по уникальным последовательностям байтов в файлах.
- **Анализ поведения (анализ в реальном времени)** – отслеживает, как программа ведёт себя после запуска. Если она начинает выполнять подозрительные действия, антивирус может её остановить.
- **Облачный анализ** – когда антивирус обнаруживает подозрительный файл, он отправляет его хэш (уникальный идентификатор) или сам файл на сервер антивирусной компании. На сервере файл проверяется с использованием алгоритмов, больших баз данных и машинного обучения.

Киберсоциализация (от англ. cyber – префикс, связанный с информационно-коммуникационными технологиями и англ. socialization – социализация) – **процесс социализации личности в киберпространстве**. Термин «киберсоциализация» был предложен и обоснован в 2005 году российским учёным, кандидатом педагогических наук Владимиром Плешаковым. Это процесс качественных изменений структуры самосознания и мотивационно-потребностной сферы личности, который происходит под влиянием и в результате использования человеком информационно-коммуникационных, компьютерных, электронных, цифровых, мультимедиа,

сотовой связи и интернет-технологий. **В отличие от традиционной социализации**, которая происходит в реальном мире через взаимодействие с семьёй, близкими, друзьями, школой, социальными институтами, **киберсоциализация осуществляется преимущественно через интернет и социальные сети**. Это включает в себя создание онлайн-профилей, участие в дискуссиях на форумах, ведение блогов и другие формы цифрового взаимодействия.

Учёные выделяют два типа киберсоциализации:

Позитивная – безопасное освоение пользователем киберпространства с перенесением положительного опыта в жизнь.

Негативная – высокая степень вовлечённости пользователя в виртуальные коммуникации в сочетании с девиантными формами общения в интернет-среде.

Кибернасилие (также называют «цифровое насилие», «онлайн-насилие», «насилие в онлайн-среде») – **нанесение вреда с помощью электронных форм общения и контакта**. Оно может включать в себя различные способы угнетения и подавления человека с целью манипуляции его действиями.

Некоторые проявления кибернасилия:

- электронные письма и сообщения с целью запугивания и шантажа;
- распространение неправдивой информации, слухов, сплетен;
- создание блогов, вебстраниц для публикации историй, фотографий, карикатурных картинок, видео, шуток о других людях без их разрешения на публикацию;
- вскрытие электронной почты и страниц в социальных сетях и распространение полученной таким путём информации;
- использование чужих паролей для изменения профиля людей и использования информации, которая может затронуть чувства других людей;
- создание опросников, когда посетителям страницы предлагается оценить какого-то человека и его качества с унижением его достоинства;
- размещение и рассылка фотографий другим людям с целью насмешек и обсуждения;
- вымогательство через электронное общение личной информации и распространение этой информации другим людям;
- обсуждение людей в публичных чатах и форумах с целью их дискредитации, унижения, оскорбления.

Кибернасилие может проводиться анонимно, что затрудняет поиск его источника и людей, вовлечённых в этот процесс.

Ценность – это то, что имеет для человека значимость, важность, значение. Это может быть материальный объект, идея, принцип, норма или идеал, который человек считает важным и стремится к нему.

Примеры ценностей:

- индивидуальные – честность, любовь, здоровье, самореализация;
- социальные – справедливость, равенство, свобода, уважение к правам других людей;
- культурные – традиции, искусство, наука, религия.

В философии

Ценности – это основные идеи и убеждения, которые определяют, что считается хорошим, правильным или ценным в жизни. Их изучает отдельный философский раздел – аксиология (буквально, наука о ценностях).

Особенности:

- Ценности могут быть объективными (существуют независимо от человека) или субъективными (зависят от личных убеждений и культуры).
- Философы разных эпох и культур обсуждали, откуда берутся ценности и как они связаны с существованием человека.

В психологии

Ценности – это фундаментальные убеждения и принципы, которые определяют поведение и мотивацию человека. Они служат внутренними ориентирами, влияющими на принятие решений и формирование жизненных приоритетов. Ценности существуют как многоуровневая система, в которой есть высшие ценности (ценности-цели) и второстепенные (ценности-средства). Ценности личности образуют систему её ценностных ориентаций, т.е. систему важнейших качеств личности.

Особенности:

- Ценности могут быть осознанными, когда человек ясно понимает, что для него важно, и неосознанными, когда они проявляются через поведение и реакции на события.
- Ценности могут быть внутренними (личные убеждения) или внешними (социальные нормы, ожидания общества).

Ценности цифрового мира:

- **Открытость и доступность информации.** Информация считается ключевым фактором накопления человеческого капитала.
- **Свобода.** Цифровой мир предлагает открытое информационное пространство, доступность ресурсов, потенциал самовыражения и самореализации.
- **Персонализация и индивидуализация.** Например, в сфере здравоохранения создаются электронные персональные медицинские карты, в образовании – индивидуальные учебные задания.
- **Цифровая этика, вежливость и взаимоуважение в сети.**
- **Автоматизация и оптимизация деятельности, социальная мобильность.**
- **Конфиденциальность и анонимность в сети.**
- **Навыки работы с информацией,** способность к быстрой адаптации, гибкость мышления.
- **Творчество** и его проявление в условиях алгоритмичных решений, принятых на основе результатов функционирования искусственного интеллекта.
- **Возможность влиять на изменения социального поведенческого протокола.**

В зависимости от направленности цифровые ценности можно разделить на шесть подгрупп: социальные, политические, моральные, экономические, материальные, личностные.

Ценностные ориентации личности – это совокупность убеждений и принципов, которые определяют, что человек считает важным и значимым в жизни. Они отражают мировоззрение, жизненные установки и направленность интересов.

Ценностные ориентации считаются одним из наиболее значимых компонентов структуры личности человека. Ценностные ориентации, являясь одним из центральных личностных новообразований, выражают сознательное отношение человека к социальной действительности и в этом своём качестве определяют широкую мотивацию его поведения и оказывают существенное влияние на все стороны его действительности. Особое значение приобретает связь ценностных ориентаций с направленностью личности.

Система ценностных ориентаций определяет содержательную сторону направленности личности и составляет основу её взглядов на окружающий мир, отношения к другим людям, к себе самой, основу мировоззрения, ядро мотивации и «философию жизни». Ценностные ориентации – это способ дифференциации объектов действительности по их положительной или отрицательной значимости. Понятийно ценностные ориентации – это избирательное отношение человека к материальным и духовным ценностям, система его установок, убеждений, предпочтений, выраженная в сознании и поведении, способ дифференциации человеком объектов по их значимости. Ценностные ориентации отграничивают существенное и важное для данного человека от несущественного. В силу этого ценностные ориентации выступают важным фактором, обуславливающим мотивы действий и поступков личности. Ценностные ориентации являются важнейшим решающим фактором развития личности.

Ценностные ориентации могут включать как материальные, так и нематериальные аспекты: здоровье, семья, карьера, свобода, творчество и духовность.

Система ценностных ориентаций – иерархическая структура, в которой одни ценности занимают более высокое положение по сравнению с другими. На вершине иерархии находятся наиболее значимые ценности, которые определяют основные цели и направления деятельности человека. Ниже, расположены менее значимые ценности, которые могут меняться в зависимости от ситуации и обстоятельств. Система может варьироваться в зависимости от культурных и социальных контекстов, а также индивидуальных особенностей личности. Например, в коллективистских культурах ценности, связанные с семьёй и обществом, могут занимать более высокое место, чем в индивидуалистических культурах, где акцент делается на личные достижения и независимость.

Ценностные ориентации определяют мотивы и цели деятельности человека, его отношение к различным аспектам жизни.

Некоторые функции системы ценностных ориентаций:

- Ориентирующая – помогает человеку определить свои цели и приоритеты.
- Регулятивная – влияет на выбор средств и способов достижения целей.

- Оценочная – позволяет человеку оценивать свои действия и поступки с точки зрения их соответствия ценностям.

Важно отметить, что система ценностных ориентаций не является статичной и может меняться в течение жизни под влиянием различных факторов. Ценностные ориентации играют мотивационную роль и определяют выбор деятельности. Ценности реализуются в ценностные ориентации и представляют собой элемент диспозиционной структуры личности.

Диспозиционная структура личности – концепция, которая предполагает, что личность состоит из диспозиций –предрасположенностей, которые определяют поведение в различных ситуациях. Эта идея лежит в основе диспозиционной теории личности, разработанной в психологии и социологии. Основатели диспозиционного подхода: в психологии — американский психолог Гордон Олпорт (1897–1967).; в отечественной социологии – Владимир Александрович Ядов.

Основная идея: сущность личности определяется разными склонностями и предрасположениями, которые люди проносят через всю жизнь. Диспозиции не хаотичны, а образуют систему, которая иерархически организована.

Особенности:

- Диспозиции формируются на стыке между потребностями и ситуациями, в которых эти потребности могут быть удовлетворены.

- В каждой конкретной ситуации ведущая роль принадлежит определённому уровню диспозиций.

По В.А. Ядову, диспозиции образуют иерархию:

- Низший уровень – элементарные фиксированные установки, формируются на основе потребностей физического существования и в простейших ситуациях.

- Средний уровень – система социальных установок (аттитюдов), содержит эмоциональный (оценочный), когнитивный (рассудочный) и поведенческий аспекты.

- Высший уровень – общая (доминирующая) направленность интересов личности в определённые сферы социальной деятельности, система ценностных ориентаций на цели жизнедеятельности и средства их достижения.

По Г.Олпорту, диспозиции делятся на три типа:

Тенденции – устойчивые предрасположенности к определённым видам поведения или мышления. Например, если человек имеет тенденцию к творчеству, он будет стремиться создавать новые идеи и проекты.

Черты – более устойчивые диспозиции, отражают основные характеристики. Например, честность – черта, которая характеризует человека как честного и правдивого.

Способности – диспозиции, связанные со способностями к определённой деятельности. Например, способность к математике может быть связана с умением решать сложные математические задачи.

Традиционные российские духовно-нравственные ценности.

Согласно Указу Президента РФ от 9 ноября 2022 года №809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных

российских духовно-нравственных ценностей» к традиционным ценностям России относятся:

- жизнь и достоинство человека;
- права и свободы человека;
- патриотизм и гражданственность;
- служение Отечеству и ответственность за его судьбу;
- высокие нравственные идеалы;
- крепкая семья;
- созидательный труд;
- приоритет духовного над материальным;
- гуманизм и милосердие;
- справедливость;
- коллективизм;
- взаимопомощь и взаимоуважение;
- историческая память и преемственность поколений;
- единство народов России.

Указ рассматривает традиционные ценности как основу российского общества, которая позволяет защищать и укреплять суверенитет страны, обеспечивать её единство и развивать человеческий потенциал.