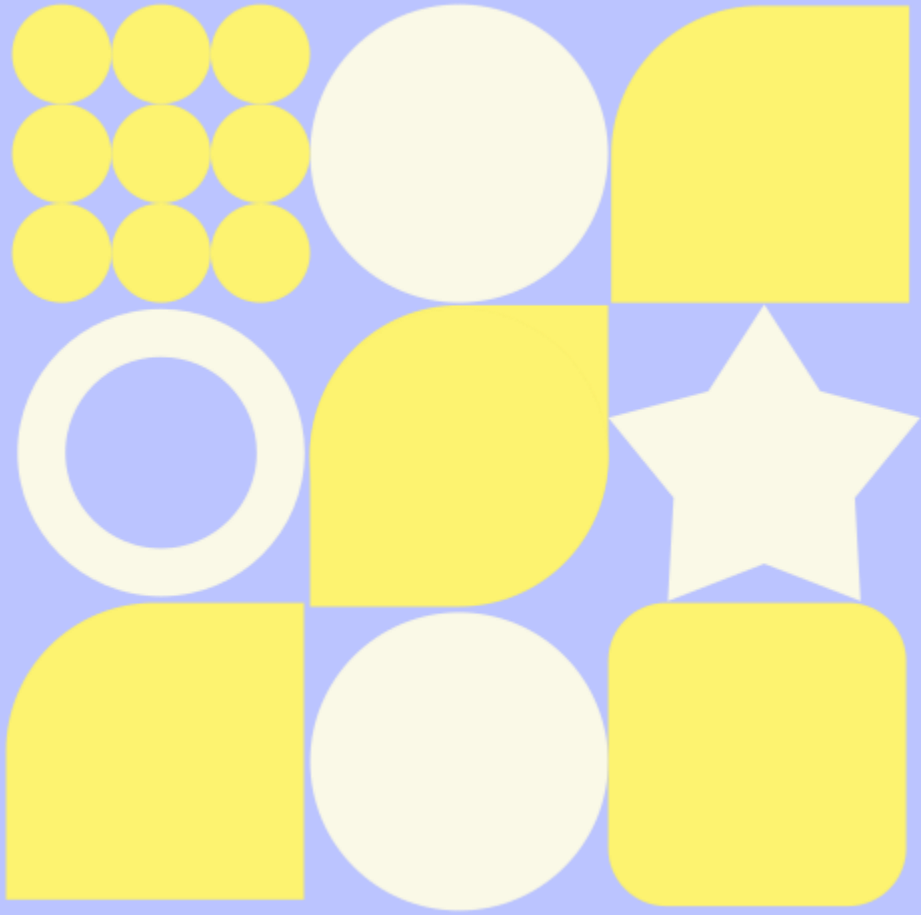
Кибербезопасность и профилактика киберпреступности: обзор и ключевые задачи

Значимость защиты в сети для детей, педагогов и родителей в современном обществе.

Иванова Наталья Михайловна, учитель математики и информатики МКОУ «Новодугинская СШ», региональный методист



Современный контекст интернет-безопасности

Интернет всесторонне влияет на жизнь детей, создавая риски деструктивных воздействий. Государственные концепции, нормативы и слаженная работа школы с родителями обеспечивают устойчивую защиту несовершеннолетних.

Национальные приоритеты: защита детства и интернет-безопасность

Конституция Российской Федерации закрепляет приоритет защиты прав и интересов детей как основу государственной политики в сфере воспитания и образования.

Создаются условия для всестороннего развития личности, формируются патриотизм и гражданственность, опираясь на духовно-нравственные ценности российского общества.

Интернет-безопасность является ключевой задачей в условиях цифровизации, требующей внимания к новым угрозам и обеспечения психологического благополучия детей.

Законодательная база по профилактике правонарушений

Конституция РФ и Федеральный закон «Об образовании» предусматривают основы защиты и воспитания несовершеннолетних в безопасной среде.

Федеральный закон «Об основных гарантиях прав ребенка» закрепляет права ребенка на защиту от вредных воздействий в информационной среде.

Стратегия национальной безопасности РФ включает задачи по профилактике правонарушений среди несовершеннолетних, учитывая угрозы цифровизации.

Конвенция ООН о правах ребенка и международные нормы служат фундаментом для формирования комплексных профилактических мер и защиты детей.

Современные интернет-риски для несовершеннолетних

1. **Распространение деструктивных идеологий**

Интернет активно используется для массового распространения разрушительных идеологий, которые формируют искажённые представления у подростков, способствуя их вовлечению в противоправные сообщества.

2. **Криминализация подростковой среды**

Сеть облегчает доступ детей и подростков к криминализации подростковой среды через социальные платформы, что вовлекает молодёжь в асоциальное поведение и опасные группы.

3. **Опасность буллинга и кибербуллинга**

Травля в сети становится все более актуальной проблемой. Кибербуллинг, беспрерывный и всепроникающий, наносит серьёзный ущерб психологическому здоровью несовершеннолетних.

Опасности для детей и подростков в сети «интернет»:

- ✓ Вовлечение в опасные группы и движения
- ✓ Буллинг (травля) в интернете
- ✓ Домогательство, педофилия
- ✓ Завладение личной информацией или материалами с целью шантажа
- ✓ Кража паролей/аккаунтов в социальных сетях или играх
- ✓ Зависимость от социальных сетей
- ✓ Зависимость от сетевых игр, «серфингом», онлайн-казино;
- ✓ Доступность материалов, предназначенных для старшей аудитории;
- ✓ Фишинг(создание сайтов-двойников с целью наживы во время покупки товаров или услуг)
- ✓ Нежелательные покупки и многое другое

Статистика интернет-активности среди детей и родителей

Большинство детей проводят много времени в интернете, что требует усиления контроля со стороны взрослых.

Высокий уровень активности несовершеннолетних в сети подчеркивает важность родительского контроля и профилактики рисков.

Основные ошибки несовершеннолетних в сети Интернет

Тип ошибки	Процент (%)
Указание реального возраста	58
Номер школы	39
Фото с видом домашней обстановки	29
Информация о родственниках	23
Геолокация	10
Адрес и телефон	7

Частые ошибки подростков при размещении личной информации онлайн создают угрозы безопасности.

Распространение личных данных увеличивает риск вовлечения в опасные ситуации в интернете.

ФГБУ «Центр защиты прав и интересов детей», 2021

Основные типы интернет-угроз для детей и подростков

Вовлечение в деструктивные группы

Подростков привлекают в опасные онлайн-сообщества через игры и манипуляции, что оказывает разрушительное воздействие на их поведение и мировоззрение.

Буллинг и домогательства

Интернет обеспечивает круглосуточное пространство для травли и неподобающего обращения, что наносит ущерб психологическому здоровью детей.

Фишинг и кража аккаунтов

Мошенники используют фишинг-атаки для кражи личных данных и доступа к аккаунтам детей, что приводит к финансовым и личностным потерям.

Интернет-зависимость и нежелательный контент

Чрезмерное использование сети приводит к зависимости, открывая доступ к материалов старшей аудитории, онлайн-казино и азартным играм.

Особенности интернет-коммуникации: иллюзия анонимности

Социальные сети создают у школьников ложное чувство защищённости, что стимулирует рискованное поведение и доверие незнакомцам.

Половина подростков заводят новые знакомства онлайн, при этом треть получают поддерживающие контакты от взрослых, что увеличивает риск негативных последствий.

Более трети школьников встречались с онлайн-знакомыми в реальной жизни, что подчеркивает опасность анонимности и необходимость контроля.

Вовлечение в деструктивные группы: механизмы и примеры

1. Вовлечение происходит через онлайн-игры, где кураторы манипулируют подростками, навязывая правила и угрозы за невыполнение заданий.

2. В играх используются психологические методы внушения исключительности участников и изоляции от окружающих, что затрудняет выход из группы.

3. Примеры таких деструктивных движений включают ультра-движения, анархизм, девиантное поведение, скулшутинг и сатанизм.

4. Наркомания, нацизм и скулшутинг также присутствуют в онлайн-пространстве, вовлекая тысячи несовершеннолетних в противоправную деятельность.

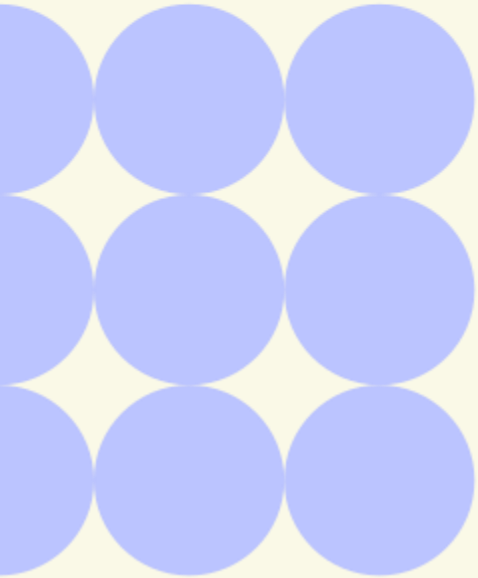
Численность участников деструктивных групп в интернете

Данные демонстрируют масштаб распространения различных деструктивных сообществ среди пользователей, включая подростковую аудиторию.

Наибольшее вовлечение наблюдается в ультра-движениях, что требует особого внимания к профилактике в образовательной среде.

ЦНТИ МФТИ и «Крибрум», 2019

Кибербуллинг: масштабы и последствия



Около 33% детей сталкиваются с кибербуллингом — систематической травлей в сети, которая ведет к эмоциональному стрессу и социальной изоляции.

Круглосуточный характер травли и постоянный доступ к интернет-платформам усугубляют воздействие и не дают жертвам возможности уйти от агрессии.

Особенно подвержены риску дети, активно пользующиеся социальными сетями, для которых прекращение использования платформ оказывается затруднительным.

Основные поводы для кибербуллинга учащихся

Частыми причинами травли являются особенности внешнего вида и физические характеристики, вызывающие у агрессоров чувство превосходства или неодобрения.

Социальный статус и уровень интеллекта также провоцируют негативное поведение, формируя предвзятость и дискриминацию среди сверстников.

Индивидуальные качества и поведение ребёнка, не соответствующие нормам группы, становятся основаниями для возникновения агрессии.

Ответственность за буллинг лежит на агрессоре и поддерживающей его группе, при этом жертва не несет вины за травлю.

Защита от домогательств и шантажа в сети

Рекомендуется не публиковать данные о местоположении, использовать настройки приватности для закрытия страницы, а также избегать встреч с незнакомцами из интернета.

Обязательны сложные пароли с регулярной заменой и настройкой двухэтапной аутентификации для аккаунтов с целью предотвращения краж и шантажа.

Признаки вовлечения подростка в опасные онлайн-группы

Резкие изменения в поведении и настроении, замкнутость, необъяснимая раздражительность или возбуждение могут сигнализировать о вовлечении.

Падение успеваемости и подозрительные телесные повреждения, а также тайное использование нескольких аккаунтов — типичные признаки.

Появление странных записей, символики и загадочных хэштегов на страницах в соцсетях свидетельствует о вовлечении в деструктивное сообщество.

Стратегия поведения родителей для профилактики риска

1. Внимательно наблюдайте за эмоциональным состоянием и поведением ребёнка, проявляйте искренний интерес к его жизни без критических оценок.

2. Совместно с ребенком устанавливайте временные лимиты на пользование интернетом и обсуждайте правила использования сети.

3. Уважайте интересы подростка к цифровым активностям, поддерживайте доверие и открытый диалог о возможных опасностях.

4. Предлагайте офлайн-активности как дополнение, а не замену онлайн-среде, способствуя гармоничному развитию.

Модель конструктивного диалога родителя с ребенком

Эффективное взаимодействие для предотвращения интернет-рисков

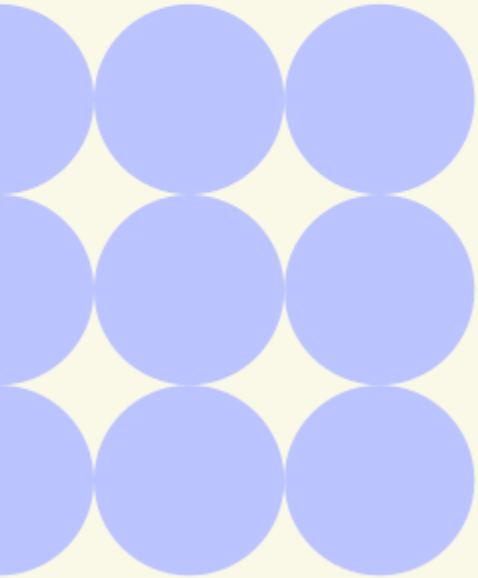
Вовлечение родителей в цифровую жизнь подростка

Совместно просматривайте сайты и обсуждайте игры, чтобы понять интересы и повысить доверие среди детей и родителей.

Устанавливайте договорённости о времени использования интернета без крайних ограничений, избегая использования сети как награды или наказания.

Развивайте у подростков навыки самоконтроля и самостоятельного управления временем онлайн для формирования ответственного поведения.

Профилактика интернет-зависимости и развитие самоконтроля



Обучайте ребёнка соблюдать баланс между онлайн-активностью и офлайн-жизнью для предотвращения вредных последствий зависимости.

Корректируйте чрезмерную активность подростка, помогая ему осознанно распределять время и энергию.

Формируйте умения самостоятельного контроля времени пребывания в интернете, особенно для подростков старше 12 лет и при отсутствии родительского контроля.

Основные принципы онлайн-безопасности для детей

Понимайте, что интернет, как и реальный мир, содержит разные типы людей и информацию, требующую осознанного отношения.

Применяйте в сети такие же правила безопасного поведения, какими руководствуетесь в офлайн-жизни.

Не стесняйтесь обращаться за помощью к взрослым при возникновении подозрений или неприятных ситуаций в интернете.

Всегда критически оценивайте получаемую информацию и будьте осторожны с контактами и контентом, чтобы сохранить свою безопасность.

Программы и сервисы родительского контроля

Сравнительная таблица основных функций популярных программ родительского контроля для защиты детей в интернете.

Каждая программа имеет уникальный набор функций, при этом большинство обеспечивает фильтрацию сайтов и мониторинг активности, а KasperskySafeKids дополнительно предлагает отслеживание геолокации.

Программа	Фильтрация сайтов	Ограничение времени	Мониторинг активности	Геолокация
iProtectYouPro	+	+	+	—
KidsControl	+	+	+	—
MipkoTimeSheriff	—	+	+	—
NetPoliceLite	+	—	—	—
Интернет-Цензор	+	—	—	—
KasperskySafeKids	+	+	+	+

Действия родителей при выявлении проблемы

Первым шагом должно стать установление доверительного диалога с подростком для выявления причин его вовлечения в деструктивную деятельность без осуждения и упрёков.

Важно совместно с ребёнком искать безопасные альтернативы, которые удовлетворят его потребности, и поддерживать контакт с образовательным учреждением и специалистами для комплексной помощи.

Если ситуация угрожает безопасности, родителям следует незамедлительно обратиться за помощью к психологам, педагогам и, при необходимости, правоохранительным органам.

Рекомендации детям: определение интернет-рисков

Интернет — удобное и полезное пространство, но необходимо помнить, что не вся информация там надежна, и надо критически оценивать получаемые данные.

Опасность исходят от вредного контента, попыток вовлечения в негативные сообщества и рисков раскрытия личной информации злоумышленникам.

Для защиты важно использовать разрешённые сайты, избегать общения с незнакомцами и обращаться к взрослым, если возникают подозрения или неприятные ситуации.

Памятка для младших школьников по интернет-безопасности

1 Спрашивай совета у родителей

Если что-то в интернете вызывает у тебя беспокойство или вопросы, обязательно расскажи об этом родителям. Они помогут разобраться и скажут, насколько это безопасно.

2 Добавляй в друзья только знакомых

Не принимай в друзья в социальных сетях тех, кого не знаешь лично. Это поможет избежать опасных ситуаций и сохранить личную безопасность.

3 Не отправляй свои фотографии незнакомым

Не пересылай фото людям, которых ты не знаешь. Это защитит тебя от возможного шантажа и неприятных ситуаций.

ДЛЯ ШКОЛЬНИКОВ МЛАДШИХ КЛАССОВ:

Всегда спрашивай родителей о том, что тебя встревожило в интернете. Они помогут тебе понять, **безопасно это или нет**!

Добавляй в друзья **только знакомых** людей

Если тебя кто-то расстроил или обидел, обязательно **расскажи** взрослому

Не отправляй фотографии людям, которых ты **не знаешь**

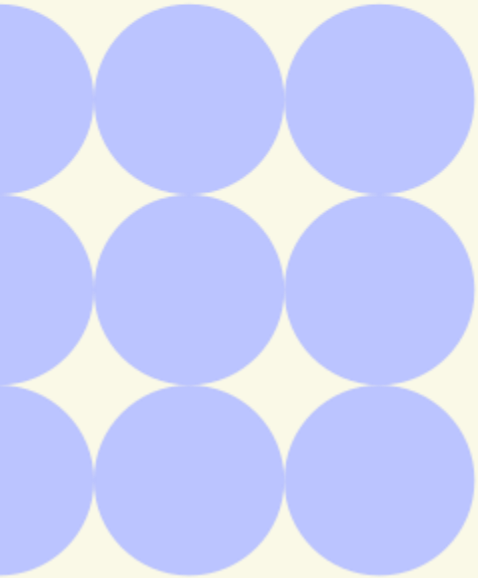
Не рассказывай о себе **незнакомым** людям: где ты живешь, в какой школе учишься, не давай номер телефона

Не встречайся вживую без взрослых с людьми из интернета. В интернете многие люди рассказывают о себе **неправду**

Но в то же время, общаясь в интернете, будь дружелюбен с другими. Не лиши грубых слов, потому что ты можешь нечаянно **обидеть** человека

Не нажимай на **подозрительные** ссылки

Памятка для средних школьников: цифровая гигиена



Не указывай личные данные при регистрации на сайтах, чтобы защитить себя от доступа незнакомцев к вашей информации и избежать возможных мошенничеств.

Используй веб-камеру только во время общения с друзьями, избегай подозрительных ссылок и не переходи на неизвестные ресурсы.

Если сталкиваешься с тревожными ситуациями онлайн, обязательно делись ими с родителями или педагогами, чтобы получить поддержку и защиту.

ПРОСТЫЕ ПРАВИЛА РАБОТЫ В ИНТЕРНЕТ-СРЕДЕ ДЛЯ ШКОЛЬНИКОВ СРЕДНИХ КЛАССОВ:

Не указывай **личную** информацию при регистрации на сайте (свое настоящее имя, возраст, город проживания и т. п.), т. к. она может быть доступна незнакомым людям

Используй веб-камеру **только при общении с друзьями**

Всегда **сообщай взрослым** обо всех случаях в интернете, которые вызвали у тебя смущение или тревогу

Если тебе пришло сообщение с незнакомого адреса, не открывай его, это может быть письмо **с вирусом**

Нежелательные письма от незнакомых людей называются «спам». Если ты получил такое письмо, **не отвечай** на него

Если тебе приходят письма с неприятным и оскорбляющим содержанием, если кто-то ведет себя по отношению к тебе неподобающим образом, **сообщи** об этом родителям или педагогу

Не нажимай на **неизвестные** ссылки

Памятка для старших школьников: расширенные рекомендации

1. Не размещай персональные данные в интернете: адрес, телефон, фотографии, чтобы обезопасить себя от злоумышленников и кражи личной информации.

2. Остерегайся сомнительных предложений работы или игр с крупными выигрышами, так как в интернете часто встречается мошенничество.

3. Не скачивай файлы из неизвестных источников, чтобы избежать вирусов и вредоносного ПО, способного нанести ущерб устройствам и безопасности.

4. При возникновении сомнительных ситуаций консультируйся с педагогами или родителями, не оставляй проблему без внимания.

ПРОСТЫЕ ПРАВИЛА РАБОТЫ В ИНТЕРНЕТ-СРЕДЕ ДЛЯ ШКОЛЬНИКОВ СТАРШИХ КЛАССОВ:

Интернет. Территория безопасности

ЗНАНИО

Мы хотим, чтоб Интернет был вам другом много лет!
Правила эти обеспечат безопасность вам в Интернете.

Не выкладывай в свободный доступ номера телефонов, домашний адрес, электронную почту и другую личную информацию.

Не сообщай личный пароль друзьям и знакомым, а тем более посторонним людям.

Не реагируй на сомнительные сообщения в сети и не переходи по незнакомым ссылкам.

Ограничь доступ к личным фотографиям.

Не нажимай на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными они не были.

Знакомясь с новыми людьми в интернете, помни: не все люди являются теми, за кого себя выдают.

Если незнакомый человек приглашает на встречу, посоветуйся с родителями. Назначай встречу в общественном месте и в присутствии взрослых.

Помни, что информация не всегда бывает полезной и достоверной. Всегда сообщай взрослым, если что-то вызывает неприязнь и дискомфорт.

Если при общении в интернете тебе угрожают или пишут что-то неприятное, ничего не отвечай и расскажи об этом родителям.

Постарайся общаться только с теми, кого знаешь.

Куда обратиться за помощью ребенку и семье

1. В случае необходимости обратись на горячие линии психологической и консультативной помощи по телефонам 8 (800) 555-89-81 и 8 (800) 2000-122. Там специалисты готовы оказать поддержку бесплатно и анонимно.

2. В экстренной ситуации:
- экстренная медико-психологическая помощь: 8 (499) 791-20-50;
- телефон горячей линии психологической помощи МЧС России: 8 (495) 989-50-50;
- Горячая линия «Ребенок в опасности» Следственного комитета РФ: 8-800-200-19-10;

Также доступны онлайн-сервисы поддержки, такие как мырядом.онлайн и ПомощьРядом.рф, а для комплексной помощи можно найти ближайшие психолого-педагогические центры по адресу https://ovzrf.ru/navigator/.

Интернет-ресурсы по кибербезопасности для всех участников

Информационные памятки

Полезные памятки для детей и родителей на сайте fcprc.ru помогут разобраться с основами интернет-безопасности и методами защиты.

Вебинары и онлайн-лекции

На fcprc.ru доступны вебинары для педагогов и родителей по вопросам психологической безопасности и профилактики интернет-рисков.

Блог лаборатории Касперского

Актуальные статьи и советы по цифровой гигиене и распознаванию опасного контента для различных возрастных групп.

Родительские сценарии

Методические материалы и сценарии родительских собраний на УРОКБЕЗОПАСНОСТИ.РФ помогают организовать профилактические беседы с детьми.

Информационно-методические материалы

Твоя психологическая безопасность (Памятка): https://fcprc.ru/wp-content/uploads/2019/05/6.-Tvoya-psihologicheskaya-bezopasnostpamyatk-dlya-detej.pdf

Как защитить ребенка от интернет-рисков (Памятка): https://fcprc.ru/wp-content/uploads/2019/05/5.-Kak-zashhitit-detei-ot-internet-riskovpamyatka-roditelyam.pdf

Родителям о психологической безопасности детей и подростков (Памятка): https://fcprc.ru/wp-content/uploads/2019/05/4.Roditelyam-o-psihologicheskojbezopasnosti-detej-i-podrostkov-pamyatka.pdf

Применение медиативных и восстановительных технологий в сфере предупреждения деструктивных проявлений среди несовершеннолетних: https://fcprc.ru/wp-content/uploads/2021/05/Primenenie-mediativnyh-i-vosstanovitelnyhtehnologij-v-sfere-preduprezhdeniya-destruktivnyh-proyavlenij-sredinesovershennoletni_compressed.pdf

Работа с родителями обучающихся образовательных организаций по проведению профилактической деятельности с несовершеннолетними, склонными к суицидальному поведению. Методические рекомендации для педагогов-психологов и социальных педагогов образовательных организаций: https://fcprc.ru/wpcontent/uploads/2021/04/Rabota-s-roditelyami-obuchayushhihsya-obrazovatelnyhorganizatsij-po-provedeniyu-profilakticheskoj-deyatelnosti-s-nesovershennoletnimisklonnymi-k-suitsidalnomu-povedeniyu.pdf

Интерактивные материалы, статьи и полезные ресурсы для родителей:

Наглядно-методическое пособие для родителей «Формула семьи»: https://fcprc.ru/materials-category/informatsionno-metodicheskie-materialy-dlya-roditelej/

Статья об осознанном родительстве: https://растимдетей.рф/articles/uchimsya-osoznannomu-roditelstvu

Видео про безопасность в интернете в рамках акции УРОКБЕЗОПАСНОСТИ.РФ: https://www.youtube.com/watch?v=W_XwekfKdnY ()

Блог «Лаборатории Касперского»: https://www.kaspersky.ru/blog/digital-literacyfor-everyone/9004/
Онлайн-родительское собрание «Пространство социальных сетей без риска для детей» (Сценарий и презентация): https://fcprc.ru/spec-value-oflife/metodicheskie-materialy-dlya-spetsialistov/

Критерии распознавания фейков и поддельных аккаунтов

Критерий	Описание
Профиль не заполнен	Отсутствие персонализированных данных и личных фото
Вымышленные персонажи	Использование вымышленных имён и образов
Много нерелевантных репостов	Контент несвязанный тематически, являющийся спамом
Новость без источника	Информация без подтверждённых источников и ссылок
Анонимность	Отсутствие конкретного автора и подтверждения фактов
Проверка даты	Несправедливое использование устаревших или фальсифицированных данных

Таблица с основными признаками, по которым можно определить недостоверную информацию и фальшивые аккаунты в социальных сетях.

Фейки легко распознать по несоответствию контента, отсутствию достоверных данных и анонимности авторов. Это важно для своевременной защиты от дезинформации.

ПАМЯТКА ПЕДАГОГАМ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ

1. Объясните учащимся правила поведения в Интернете. Расскажите о мерах, принимаемых к нарушителям, ответственности за нарушение правил поведения в сети.
2. Совместно с учащимися сформулируйте правила поведения в случае нарушения их прав в Интернете.
3. Приучайте несовершеннолетних уважать права других людей в Интернете. Объясните им смысл понятия «авторское право», расскажите об ответственности за нарушение авторских прав.
4. Проявляйте интерес к "виртуальной" жизни своих учеников, и при необходимости сообщайте родителям о проблемах их детей.
5. Научите учеников внимательно относиться к информации, получаемой из Интернета. Формируйте представление о достоверной и недостоверной информации. Настаивайте на посещении проверенных сайтов.

ПАМЯТКА ПЕДАГОГАМ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ

6. Обеспечьте профилактику интернет-зависимости учащихся через вовлечение детей в различные внеклассные мероприятия в реальной жизни (посещение театров, музеев, участие в играх, соревнованиях), чтобы показать, что реальная жизнь намного интереснее виртуальной.

7. Периодически совместно с учащимися анализируйте их занятость и организацию досуга, целесообразность и необходимость использования ими ресурсов сети для учебы и отдыха с целью профилактики интернет-зависимости и обсуждайте с родителями результаты своих наблюдений.

8. В случае возникновения проблем, связанных с Интернет-зависимостью, своевременно доводите информацию до сведения родителей, привлекайте к работе с учащимися и их родителями психолога, социального педагога.

ПАМЯТКА ПЕДАГОГАМ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ

9. Проводите мероприятия, на которых рассказывайте о явлении Интернет-зависимости, ее признаках, способах преодоления.

10. Систематически повышайте свою квалификацию в области информационнокоммуникационных технологий, а также по вопросам здоровьесбережения.

11. Станьте примером для своих учеников. Соблюдайте законодательство в области защиты персональных данных и информационной безопасности. Рационально относитесь к своему здоровью.

12. Разумно используйте в своей жизни возможности интернета и мобильных сетей.

Итоги: совместная ответственность за кибербезопасность

Эффективное обеспечение кибербезопасности детей возможно только через тесное сотрудничество педагогов и родителей, основанное на информированности, доверии и своевременном обращении за помощью.