Безопасность детей в Интернете

Проблема информационной безопасности

В Интернете содержится огромный массив информации, некоторая часть которой может нанести вред здоровью, а также физическому, психическому, духовному и нравственному развитию. Интернет является зоной «трудовой» деятельности мошенников, здесь действуют педофилы, кибербуллеры, сектанты и иные злоумышленники, которые находят детей в сети, а затем под различными предлогами вступают с ними в переписку и личный контакт.

Дети также становятся источниками угроз и правонарушений. Не редки случаи осуществления ими атак на интернет-ресурсы, мошенничество и распространение запрещенного контента.

Проблема закрытости детей

Главной проблемой в обеспечении безопасности детей в Интернете являются порой не угрозы, исходящие из сети. **Узловой проблемой является закрытость детей при возникновении опасности из интернета!**

По данным опросов, **более половины детей** сталкивались с интернет-угрозами, **не ставя в известность своих родителей.**

Практика показывает, что большинство родителей не уделяет должного внимания интернет-безопасности и интернет-воспитанию своих детей.

Проблема доверия детей о проблемах в Интернете связана с их низкой культурой кибербезопасности и страхом осуждения со стороны взрослых.

Поэтому основной вывод, который нам, педагогам надо понять, и соответственно донести до законных представителей является недопустимость осуждения ребенка, столкнувшегося с интернет-опасностью!

Нормативно-правовые основы информационной безопасности

Приведенные законы являются основными нормативно-правовыми актами в области информационной безопасности несовершеннолетних. Существует также ряд подзаконных актов. Для работы в образовательной организации опираться следует на указанные законы.

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

Рассмотрим основные понятия информационной безопасности детей.

Понятие информационной безопасности детей подразумевает состояние защищенности детей, при котором отсутствует риск, связанный с **причинением информацией вреда** их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Информация, причиняющая вред здоровью и (или) развитию детей имеет деление на две группы. *(см. след. слайд)*

Информация, причиняющая вред здоровью и (или) развитию детей двух видов

Информация, **запрещенная** для распространения среди детей

Информация, распространение которой среди детей определенных возрастных категорий **ограничено**

К информации, **запрещенной** для распространения среди детей, относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных законом;
- содержащая изображение или описание сексуального насилия;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- пропагандирующая либо демонстрирующая нетрадиционные сексуальные отношения и (или) предпочтения;
- пропагандирующая педофилию;
- способная вызвать у детей желание сменить пол;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера;
- о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего;
- содержащаяся в информационной продукции, произведенной иностранным агентом.

К информации, распространение которой среди детей определенных возрастных категорий **ограничено**, относится информация:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия (за исключением сексуального насилия), преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Осуществление классификации информационной продукции

Классификация информационной продукции осуществляется ее производителями или распространителями самостоятельно до начала ее оборота на территории Российской Федерации.

Классификация информационной продукции осуществляется по следующим категориям информационной продукции:

1) информационная продукция для детей, не достигших возраста шести лет;

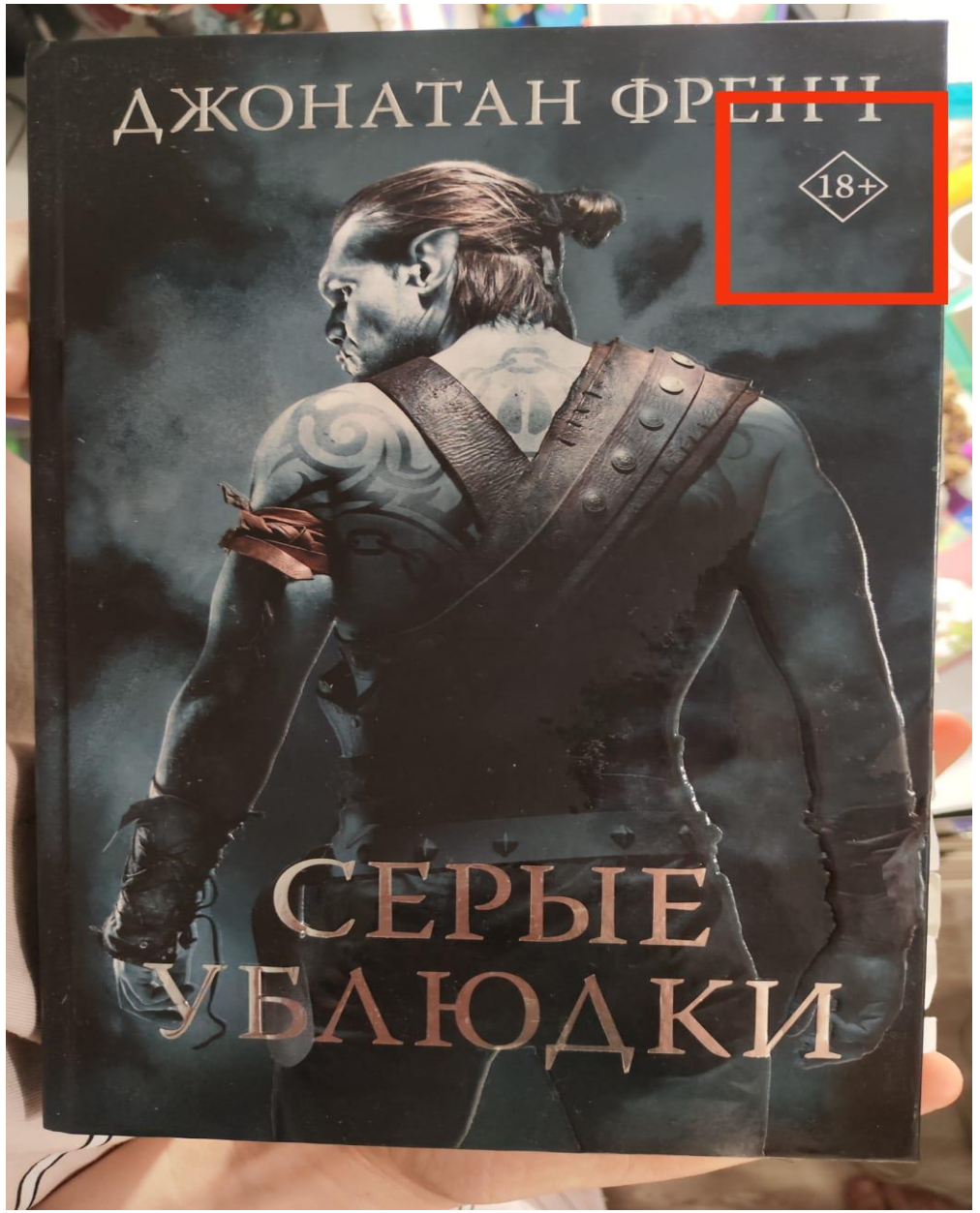
2) информационная продукция для детей, достигших возраста шести лет;

3) информационная продукция для детей, достигших возраста двенадцати лет;

4) информационная продукция для детей, достигших возраста шестнадцати лет;

5) информационная продукция, запрещенная для детей

Данная классификация должна на продукции.



Классификация информационной продукции, предназначенной и (или) используемой для обучения и воспитания детей в организациях, осуществляющих образовательную деятельность по реализации основных общеобразовательных программ, образовательных программ среднего профессионального образования, дополнительных общеобразовательных программ, осуществляется в соответствии с Федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ и законодательством об образовании.

Систематизация видов опасности

Специалисты по интернет-безопасности группируют виды опасности на крупные блоки. *(см. след. слайд)*

Основные опасности Интернета

Негативная информация, содержащаяся в интернет-пространстве	Противоправные и социально-опасные действия самого ребенка	Целенаправленные действия третьих лиц в отношении ребенка

Систематизация видов опасности

Эксперты по кибербезопасности рекомендуют обратить внимание на следующие отдельные варианты интернет-опасности:

- небезопасный гейминг;
- доксинг;
- кибербуллинг;
- опасный и не подходящий для детей контент;
- опасные незнакомцы.

Основная задача педагогов познакомить законных родителей с интернет-угрозами и мерами по их профилактике! Это общая обязанность педагогов по обеспечению безопасности детей. Самая важная информация представлена ниже.

НЕБЕЗОПАСНЫЙ ГЕЙМИНГ

Под видом фальшивых приложений и на ненастоящих игровых сайтах поджидают киберугрозы в виде вредоносных программ и онлайн-мошенничества.

В частности, популярные игры Brawl Stars и Roblox были использованы как оболочка для вредоносных программ.

Ребенок должен понимать, что, скачивая различные подозрительные файлы с просторов сети, он может столкнуться с вредоносными программами. Может быть нанесен вред устройству таким файлом. Существует риск похищения персональных данных и платежных систем.

Решение.

Советы родителям и педагогам. Объяснить ребенку, что игры нужно скачивать только из официальных источников и что не стоит кликать на все подряд. Переход по заманчивым предложениям на игровых сайтах могут привести не получению бесплатных приложений, а к проникновению вредоносных программ.

ДОКСИНГ

Доксинг - явление при котором недоброжелатели намеренно ищут и публикуют личную информацию о человеке со злым умыслом. Данная информация может использоваться для шантажа или дискредитации человека в социальном пространстве. Для этого доксеры собирают личные данные, в том числе и те, что люди сами размещают на страницах соцсетей.

Треть школьников выкладывают фотографии, на которых видно обстановку детей публикуют номер телефона.

Решение.

Советы родителям и педагогам. Научите ребенка в настройках профиля устанавливать максимальные настройки приватности. Помогите определить ребенку какую информацию и фотографии не стоит размещать в соцсетях. Чрезмерная открытость в сети чревата последствиями для безопасности.

КИБЕРБУЛЛИНГ

Обидные сообщения, угрозы, распространение ложной информации о человеке являются примерами онлайн-травли (кибербуллинг). Дети могут столкнуться с ней в социальных сетях, мессенджерах и даже на игровых онлайн-платформах. Последствия кибербуллинга могут привести к депрессии, а порой к суициду. Опасно и то, что в некоторых случаях кибербуллинг может переходить в личное общение между подростками. Ситуация осложняется тем, что дети зачастую не хотят делиться с родителями аспектами своей цифровой жизни и скрывают, что происходит с ними в Сети. Закрытость детей уже была отмечена как основная проблема в обеспечении их информационной безопасности.

В цифровой среде специалисты выделяют несколько видов проявления онлайн-агрессии.

Хейтинг (hating) - необоснованная критика в виде комментариев и сообщений в адрес конкретного человека.

Троллинг (trolling) - агрессивные комментарии с целью высмеять.

Грифинг (griefing) - в онлайн-играх термин обозначает провокационное поведение человека, который портит другим игровой процесс.

Секстинг (sexting) - публикация фото- и видеоматериалов с обнаженными людьми с целью шантажа или мести.

Кибersталкинг (cyberstalking) – навязчивое преследование в интернете со стороны одного человека или группы.

Решение.

Советы родителям и педагогам. Важно договориться с ребенком, чтобы он обязательно делился, если в Сети кто-то стал ему угрожать, шантажировать его, что-то вымогать или вести себя оскорбительно. Для этого необходимо выстраивать доверительные отношения в семье и интересоваться онлайн-жизнью ребенка. Его важно предупредить о том, что с интернет-травлей может столкнуться любой, вне зависимости от возраста, интересов или внешности, – в этом случае следует сразу прекратить всякое общение с обидчиками. Также ребенку нужно знать, что часто злоумышленники в интернете могут выдавать себя за тех людей, которыми они не являются. Признаком того, что ребенок подвергается кибербуллингу, может стать внезапное удаление своей страницы в соцсетях и явные изменения в поведении, эмоциональном и физическом состоянии, ухудшение успеваемости в школе.

ОПАСНЫЙ И НЕ ПОДХОДЯЩИЙ КОНТЕНТ

Сцены жестокого насилия, употребления запрещенных веществ, нецензурная лексика являются недопустимыми для детей. Интернет изобилует и подобным видом контента. Не зря на фильмах, роликах и компьютерных играх ставится отметка «18+». Родителям стоит обращать внимание на данную маркировку, о которой мы уже говорили. Но самым эффективной профилактикой интернет-угроз является нахождение в курсе, того во что играют и что смотрят дети.

Решение:

Советы родителям и педагогам. Запрет будет самым неправильным решением. Запреты, ограничения приведут к возрастанию недоверия между законными представителями и детьми. Поговорите с ребенком, проведите аналогии с реальной жизнью. Например, многие знают, что нельзя никуда уходить с посторонними или переходить дорогу на красный свет. Такие же правила действуют и в цифровом мире. Не отвечать незнакомцам, не переходить по подозрительным ссылкам, критически относиться к крайне щедрым или пугающим сообщениям.

ОПАСНЫЕ НЕЗНАКОМЦЫ

Социальные сети - важный элемент социализации детей. Однако там встречаются разные люди, и не всегда у них благие намерения. Сегодня актуальна угроза онлайн-груминга – когда взрослый человек пытается установить доверительные отношения с ребенком и встретиться в реальной жизни или получить приватные фотографии или видео, в том числе для дальнейшего шантажа.

Около 80% детей получают заявки в друзья от незнакомых людей. В 20% случаев это заявки от взрослых. В группе риска дети 7–10 лет.

Решение:

Советы родителям и педагогам. Проверьте, что на странице ребенка в социальных сетях нет номера школы, где он учится, номера телефона, информации о родителях, а сам профиль закрыт для посторонних. Интересуйтесь у ребенка, с кем и о чем он общается онлайн, при этом важно соблюдать баланс и не запугивать его или излишне контролировать.

РЕКОМЕНДАЦИИ СПЕЦИАЛИСТОВ ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ

- когда ребенок только начинает осваивать цифровое пространство, стоит воспользоваться программами родительского контроля, но прежде рассказать юному пользователю об этом – для чего родители ставят такую программу;
- используйте надежные защитные решения на всех устройствах (в том числе на смартфонах);
- обратите внимание на настройки приватности в социальных сетях: не публикуйте слишком много личной информации – и детей научите тому же;
- проверьте, что на странице вашего ребенка в социальных сетях нет номера школы, где он учится, номера телефона, информации о родителях, а сам профиль закрыт для посторонних;
- используйте надежные пароли: минимум 12 символов с буквами в разном регистре, цифрами и спецсимволами;
- настройте двухфакторную аутентификацию в тех сервисах, которые это позволяют;
- не открывайте вложения из подозрительных писем или сообщений в мессенджерах и соцсетях и не переходите по ссылкам из них;
- скачивайте приложения только из официальных ресурсов;
- проверяйте адрес сайта перед тем, как вводить на нем личные или платежные данные;
- если столкнулись с кибербуллингом, не вступайте в диалог с обидчиком, заблокируйте его, сообщите о травле администраторам площадки.
- время нахождения ребенка в телефоне во время отсутствия родителей (на работе, ночью) считается наиболее опасным. Телефон ставить на зарядку рядом с кроватью ребенка нельзя.

РЕКОМЕНДАЦИИ СПЕЦИАЛИСТОВ ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ

Особое внимание следует уделить смартфонам. Специалисты дают рекомендации как защитить смартфон ребёнка от киберугроз.

1.Установите ПИН-код на сим-карту устройства, чтобы предотвратить её использование на других устройствах.

2. Воспользуйтесь возможностью биометрической аутентификации, такой как распознавание отпечатка пальца или лица, чтобы надёжно защитить смартфон и его содержимое.

РЕКОМЕНДАЦИИ СПЕЦИАЛИСТОВ ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ И ВЗРОСЛЫХ

3. Активируйте службы геолокации, чтобы иметь возможность контролировать местонахождение устройства ребёнка.

4. Настройте функции родительского контроля с помощью операционной системы или отдельных приложений.

Ссылка на мероприятие

https://edu-skills.ru/?id=33