**Понятие медиабезопасности**

**Медиа**- первая составная часть сложных слов, обозначающих объекты и понятия, относящиеся к сфере средств массовой информации.

**Безопасность -**состояние, при котором не угрожает опасность, есть защита от опасности.

**Медиабезопасность**- обеспечение государством информационной безопасности граждан, защита физического, умственного и нравственного развития, а так же человеческого достоинства во всех аудиовизуальных медиа услугах и электронных СМИ.

Обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

**Виды информации, причиняющей вред здоровью и развитию несовершеннолетних**

К информации, причиняющей вред здоровью и развитию несовершеннолетних, относится информация:

* ​Побуждающая к совершению действий, представляющих угрозу жизни и (или) здоровью;
* Способная вызвать желание употребить наркотические средства, табачные изделия, алкогольную продукцию, пиво и напитки, изготавливаемые на его основе, 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;
* Отрицающая семейные ценности;
* Оправдывающая противоправное поведение;
* Содержащая нецензурную брань;
* Содержащая информацию порнографического характера.

​**Риски, которые встречаются в интернете**

Выделяют следующие виды рисков:

* **Контентные риски** - материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, нецензурную лексику и т.д.;
* **Коммуникационные риски** (связаны с межличностными отношениями интернет-пользователей) - незаконный контакт, домогательство, киберпреследование;
* **Электронные риски** - возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.;
* **Потребительские риски** - злоупотребление в Интернете правами потребителя.

**Правила безопасности в Интернете**

* **​​**Пользоваться антивирусом (современный, регулярно обновляемый антивирус обеспечит надежной защитой от разнообразных интернет-угроз);
* Регулярно загружать обновления (обновления программ закрывают уязвимости, которыми могут воспользоваться злоумышленники);
* ​Не загружать ничего со случайных сайтов (высока вероятность того, что вместе с загруженной программой/книгой/фильмом вы получите и вредоносную программу);​
* Не проходить по ссылкам в спамовых письмах (такие ссылки зачастую ведут на мошеннические, либо зараженные вредоносными программами сайты);
* Не открывать приложения в письмах, если есть хоть какие-то сомнения в надежности адресанта (высока вероятность того, что в приложении содержится вредоносная программа (даже если это документ Word);
* Не пытаться «отписаться» от спама (особенно в том случае, когда в спамерскомписьме есть соответствующая ссылка);
* Не откликаться на заманчивые предложения, особенно если они связаны с получением быстрых денег;​

**Правила безопасности в социальных сетях**

* **​**Не передавайте информацию людям, которых вы лично не знаете. Не доверяйте людям, с которыми вы познакомились в социальной сети, ведь они могут быть кем угодно!
* Публикуйте только ту информацию о себе, которая не содержит ваших адресов, телефонов, планов на выходные. Как можно меньше реальной информации о себе!
* Помните, то, что когда-либо было опубликовано, «стереть» уже невозможно. Оставляя комментарии, сообщения, публикуя фотографию, вы помещаете ее в сеть навсегда. Поэтому совершая любое действие в социальной сети, нужно думать о последствиях!
* Цените и уважайте друг друга в социальных сетях. Оскорбляя даже неизвестного вам человека, помните, что вы сделали это и в реальной жизни! Будьте осторожны, высказывая свое мнение в социальной сети, оно может обидеть других людей в реальном мире.
* Социальные сети помогают улучшить наше общество: они позволяют объединиться людям, чтобы бороться с различными проблемами, а также осуществлять проекты, чтобы претворить свои идеи в жизнь. Поэтому, если каждый человек задумается о серьезности своих действий в социальной сети, то он сделает нашу жизнь более безопасной и комфортной.

**Основные советы родителям**

Для лучшего взаимопонимания и устранения возможных недоразумений, лучше сразу расставить все точки над «и», установить некоторые ограничения для самостоятельного выхода в Интернет. Обсудите это с детьми, чтобы они понимали необходимость подобных запретов, тогда вместе вы обязательно сможете сделать прогулки ребенка в Сети наиболее безопасными.

**Как сделать прогулки ребенка в Интернете более безопасными:**

* Составьте список правил работы детей в Интернете и помните, что лучше твердое «нет», чем неуверенное «да». Пусть ограничения будут минимальны, но зато действовать всегда   и без ограничений.
* Расскажите детям о необходимости сохранения   конфиденциальных данных в тайне и о том, как лучше это сделать. Вот несколько простых правил, которых следует   придерживаться:
	+ ​при общении использовать только имя или псевдоним;
	+ номер телефона, свой адрес, место учебы нельзя никому   сообщать;
	+ не пересылать свои фотографии;
	+ без контроля взрослых не встречаться с людьми,   знакомство с которыми завязалось в Сети.​
* Поясните, что в сети, несмотря на кажущуюся безнаказанность за   какие-то проступки, там действуют те же правила, что и в   реальной жизни: хорошо - плохо, правильно - не правильно.​
* Научите детей развивать и доверять интуиции. При малейших   признаках беспокойства, путь рассказывают об этом вам.
* Если детям по каким-либо причинам нужно вводить   регистрационное имя, помогите его придумать так, чтобы   оно не несло в себе никакой личной информации.
* Объясните, что люди в Сети часто выдают себя совсем за   других. Поэтому встречаться с ними не стоит.
* Научите детей следовать нормам морали, быть воспитанными   даже в виртуальном общении.
* Обязательно расскажите о правах собственности, о том, что   любой материал, выставленный в Сети, может быть   авторским.
* Неправомерное использование такого материала может быть   уголовно наказуемым.
* Объясните, что далеко не все, что можно увидеть в Интернете   – правда. При сомнениях, пусть лучше уточнит у вас.
* Используйте современные программы, которые предоставляют   возможность фильтрации содержимого сайтов,   контролировать места посещения и деятельность там.​

**Что такое антивирус?**

​

**Антивирусная программа (антивирус)** - программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления  зараженных (модифицированных) такими программами файлов, а также для профилактики предотвращения заражения файлов или операционной системы вредоносным кодом.

**​Методы обнаружения вирусов:**

* ​сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах;
* обнаружение подозрительного поведения любой из программ, похожего на поведение зараженной программы

**Продукты для домашних пользователей:**

* собственно антивирусы
* комбинированные продукты (например, к классическому антивирусу добавлен антиспам, файрвол, антируткит и т.д.)

**Нормативно-правовая база защиты детей от вредоносной информации регулируется:**​

* **​**Нормами международного права (ст. 13, 17, 34 Конвенции ООН о правах ребенка 1989 г., Европейской декларацией о свободе обмена информацией в Интернете 2003 г., Европейской конвенцией о совместном кинопроизводстве 1992 г. и пр.);
* Федеральным законодательством (ст. 14, 14.1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», Федеральным законом от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" и пр.);
* Приказом Генерального прокурора Российской Федерации от 26.11.2007 № 188 «Об организации прокурорского надзора за исполнением законов о несовершеннолетних и молодежи» (п. 3.2);
* Нормативными правовыми актами субъектов Российской Федерации.

**Полезные ссылки:​**

* [​Как защититься от интернет-угроз](https://ciur.ru/glr/glr_skoj/SiteAssets/pamyatka.pdf)
* [Руководство по информационной грамотности​](https://ciur.ru/glr/glr_skoj/SiteAssets/book101.pdf)
* [Обеспечение безопасности детей при работе в Интернет](https://ciur.ru/glr/glr_skoj/SiteAssets/book331.pdf)
* [Медиаобразование для родителей: освоение семейной медиаграмотности​​](https://ciur.ru/glr/glr_skoj/SiteAssets/book336.pdf)
* ​[Психологическая помощь в сети Интернет​](https://ciur.ru/glr/glr_skoj/SiteAssets/psyhelp_in_internet.pdf)
* [Этика в сети](http://www.etika.ru/)
* [Небезопасный Интернет](https://www.securelist.com/ru/analysis/208050652/Nebezopasnyy_internet)
* [Центр безопасного Интернета в России](http://www.saferunet.ru/)
* [Обзор программных продуктов для безопасного Интернета​](http://www.rgdb.ru/innocuous-internet-software)