**Информационная безопасность детей в образовательной организации**

Введение гаджетов в жизнь человека начинается с самых ранних лет, при этом свободный доступ детей и подростков к информации не всегда способствуют развитию здорового мышления, напротив, может негативным образом повлиять на психику, вовлечь в неправомерные действия. Ребенок может стать жертвой киберпреступников, оружием массового поражения в руках идеологов, политологов и рекламщиков, втянут в киберэкстремизм. Дети все чаще подвергаются кибербуллингу и становятся зависимыми от интернета, поэтому вопрос информационной безопасности сейчас наиболее актуален.

Законодательство в области защиты ребенка от информации, пропаганды и агитации, наносящей вред его здоровью, нравственному и духовному развитию:

* Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
* Федеральный закон от 25 июля 2002 г. №114-ФЗ "О противодействии экстремистской деятельности" (ред. 14.04.2021);
* Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 09.03.2021) "Об информации, информационных технологиях и о защите информации";
* Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. 05.04.2021).

Первое определение информационной безопасности детей было прописано в федеральном законе №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». В нем определено, что «информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию»[1].

Тем самым можно определить следующие задачи, стоящие перед образовательной организацией для обеспечения информационной безопасности обучающихся:

1. Защита учащихся от неправомерной информации;
2. Обеспечение безопасности информации, имеющейся в ОО;
3. Формирование и развитие навыков цифровой компетенции;
4. Лицензирование программного обеспечения;
5. Публикация на сайте образовательной организации.

Согласно ч.3 ст.6 ФЗ №436 «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 (ред. 05.04.2021 г.) «Классификация информационной продукции осуществляется по следующим категориям информационной продукции:

* информационная продукция для детей, не достигших возраста шести лет;
* информационная продукция для детей, достигших возраста шести лет;
* информационная продукция для детей, достигших возраста двенадцати лет;
* информационная продукция для детей, достигших возраста шестнадцати лет;
* информационная продукция, запрещенная для детей (информационная продукция, содержащая информацию, предусмотренную [частью 2 статьи 5](http://www.consultant.ru/document/cons_doc_LAW_381448/9083b03e61777d3fe172fb3ef707a10e10688262/#dst100044) настоящего Федерального закона)»[1].

Меры по защите детей от недопустимой информации можно разделить на административные и организационные, технические и аппаратно-программные.

Административные и организационные меры включают в себя: приказы, локальные акты, журналы (приказ о назначении ответственного за организацию работы с Интернетом и ограничение доступа, правила использования сети Интернет в ОО, внесение изменений в должностные инструкции отдельных работников ОО, план мероприятий по обеспечению информационной безопасности и др.); контроль библиотечного фонда на наличие запрещенных материалов; обучение сотрудников ОО в области информационной безопасности.

Технические, аппаратно-программные меры включают в себя системы контентной фильтрации (СКФ). Способы организации СКФ:

* Фильтрующий сервер в интернете;
* Услуга фильтрации от провайдера;
* СКФ уровня ОО.

Технологии организации системы контент-фильтрации:

* Ограничение доступа к ресурсам. Интернет – черный список (запрещенные сайты).
* Предоставление доступа к ресурсам. Интернет – белый список (разрешенные сайты).

В дополнении к вышеперечисленному в ч. 5 ст. 46 Федерального закона от 07.07.2003г. №126-ФЗ «О связи» операторы связи, оказывающие услуги по предоставлению доступа к информационно-телекоммуникационной сети Интернет, также обязаны осуществлять ограничение доступа к информации, распространение которой на территории России запрещено.

С возникновением потребности в фильтрации контента в Интернете, государства столкнулись с трудностями применения традиционных методов контроля над средствами массовой информации в сети. Одну из основных проблем для цензоров представляет динамичность социальной составляющей интернета – огромное количество материала вновь и вновь создается множеством пользователей. Другим препятствием является международный характер сети, когда серверы с информацией зачастую находятся вне юрисдикции и досягаемости правоохранительных органов отдельных стран[4]. Также необходимо не забывать, что интернет меняется в техническом плане в области борьбы за приватность данных, что делает задачу по его контролю все более сложной.

Самый надёжный способ фильтрации – «белый список» сайтов с нормативно указанным в локальных актах ОО способом его расширения.

Одной из мер по защите детей от неправомерной информации является контроль библиотечного фонда на наличие запрещенных материалов. В соответствии с федеральным законом «О противодействии экстремистской деятельности» № 114-ФЗ от 25.07.2002 в библиотеке ОУ запрещено распространение, производство, хранение и использование литературы экстремисткой направленности. Библиотекарь ежеквартально обязан проводить сверку имеющихся в фондах библиотеки документов с Федеральным списком экстремистских материалов, изымать их из оборота библиотеки, вести журнал сверок фонда библиотеки с Федеральным списком экстремистских материалов (Сайт Министерства юстиции РФ) [http://minjust.ru/extremistmaterials» [3](http://minjust.ru/extremistmaterials)].

В последние годы в школах участились попытки несанкционированного получения информации, в том числе персональных данных педагогов и учащихся. Информационным системам и сетям могут угрожать такие опасности, как: компьютерное мошенничество, компьютерные вирусы, хакеры, вандализм, хищение, разглашение конфиденциальной информации и другие виды угроз. Противодействовать такой тенденции можно, создав в образовательном учреждении систему информационной безопасности, при этом необходимо учитывать, что при комплексном использовании всего арсенала имеющихся средств защиты и подготовке пользователей с соблюдением ими установленных правил процесс построения информационной безопасности не является разовым мероприятием. Он должен постоянно совершенствоваться, быть управляемым.

Для обеспечения компьютерной безопасности образовательной организации рекомендуется:

1. Обеспечить защиту компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.). Решение данной проблемы возможно только при условии, исключающем вывод локальных сетей ОУ на Интернет, либо размещение своего сайта у удаленного провайдера;
2. Необходимо иметь как минимум два сервера. Наличие хороших серверов позволит протоколировать любые действия работников ОУ в вашей локальной сети;
3. Установить контроль за электронной почтой, обеспечив постоянный контроль за входящей и исходящей корреспонденцией;
4. Установка соответствующих паролей на персональные компьютеры администрации и педагогов, а также определение работы с информацией на съемных носителях;
5. Использование лицензионного программного обеспечения;

Немало важную роль в информационной безопасности играет и цифровая компетенция учащихся и педагогов, которая включает в себя:

* Информационную безопасность (защита от клипового мышления, умение проверять достоверность информации, умение избегать лишней информации);
* Коммуникативную безопасность (культура сетевого этикета, цифровой имидж, цифровой след);
* Техническую безопасность (навык по работе с компьютером, гаджетами, сетью, программами и другими устройствами, от которого зависит сохранность личных данных);
* Потребительскую безопасность (умение быть грамотным покупателем и ответственным потребителем контента в сети).

Формировать цифровую компетенцию можно с помощью проведения Единых уроков безопасности в сети интернет, декады безопасности в сети интернет, проведения тематических классных часов, разработка и реализация программ внеурочной деятельности.

Согласно постановлению Правительства РФ от 10 июля 2013 года №582 (с изменениями на 11 июля 2020г.) "Об утверждении [правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации](https://docs.cntd.ru/document/499032487#6560IO)" определяется перечень информации обязательный к размещению на сайте ОО, при этом размещение персональных данных обучающихся должны быть обеспечены согласиями от законных представителей.

Кроме того, статьёй 13.21 КоАП РФ предусмотрены более высокие штрафные санкции (до 200 тысяч рублей) для средств массовой информации в случаях, если они нарушают установленный порядок распространения информационной продукции среди детей.

Процесс информатизации стал неотъемлемой частью нашего общества, тем самым объединив мир в единую общую систему. Информация обладает определенной силой воздействия на каждого из нас. Человек стал зависим от глобального информационного пространства, поэтому в настоящее время обеспечение информационной безопасности является одной из приоритетных задач мирового уровня.

**Список используемой литературы:**

## Федеральный закон №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 (ред. 05.04.2021 г.) Режим доступа: <https://docs.cntd.ru/document/902254151>

## ГОСТ Р 50922-2006 Национальный стандарт Российской Федерации Защита информации. Режим доступа: <https://docs.cntd.ru/document/1200058320/>

## Письмо Комитета по образованию Санкт-Петербурга «О направлении методических рекомендаций по организации деятельности библиотек в образовательных учреждениях». Режим доступа: <http://k-obr.spb.ru/media/uploads/userfiles/2019/07/01/03-28-4945_19-0-0_My2IzZm.PDF>

## Статья «Новые методы блокировки нежелательной информации» автор Станислав Лапшин. Режим доступа: <https://sites.google.com/site/metodyblokirovkinezelanojinfor/sredstva-i-metody-filtracii-kontenta-v-internete>

## Постановление Правительства РФ от 10 июля 2013 года №582 (с изменениями на 11 июля 2020г.) "Об утверждении [правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации](https://docs.cntd.ru/document/499032487#6560IO)". Режим доступа: https://base.garant.ru/70413268/