

Как обеспечить информационную безопасность детей в школе и детском саду

Елена Болотова, профессор кафедры права ИСГО МПГУ, автор более 190 научных работ по вопросам правовой подготовки педагогов и проблемам образовательного права, доцент, д. п. н.

Виктория Ярцева, юрист-редактор Системы Образование, эксперт по образовательному праву, разработчик положений об обработке персональных данных, официальном сайте и других популярных шаблонов, лектор региональных и федеральных вебинаров

- Кого назначить ответственным
- Какие документы оформить
- Какие мероприятия провести
- Как установить СКФ
- Как проверить библиотечный фонд
- Какие обучающие мероприятия провести
- Кого отправлять на повышение квалификации
- Как проводить мониторинг
- Кто проконтролирует

Кого назначить ответственным

Ответственным за информационную безопасность назначьте работника, который обладает властными полномочиями и имеет доступ к информационным структурам образовательной организации. Например, заместителя руководителя.

Пример

Пример должностных обязанностей ответственного за информационную безопасность

Работник, ответственный за информационную безопасность:

- планирует использование ресурсов сети Интернет в образовательной организации на основании заявок преподавателей и других работников образовательной организации;
- разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете образовательной организации локальные нормативные акты образовательной организации в сфере обеспечения информационной безопасности детей;
- организует получение сотрудниками образовательной организации электронных адресов и паролей для работы в сети Интернет и информационной среде образовательной организации;

- организует контроль использования сети Интернет в образовательной организации;
- организует контроль работы оборудования и программных средств, обеспечивающих использование Реестра безопасных образовательных сайтов в образовательной организации;
- организует контроль реализации в образовательной организации методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- систематически повышает свою профессиональную квалификацию по направлению «Организация защиты детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях»;
- обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;
- соблюдает правила и нормы охраны труда, техники безопасности и противопожарной защиты, правила использования сети Интернет.

Минкомсвязи рекомендует образовательным организациям создать совет по обеспечению информационной безопасности обучающихся. В него можно включить педагогов, родителей и представителей органов власти. Пригласите членов общественных организаций, например, из Общероссийского детского общественного движения «Страна молодых», кибердружин и других.

Члены совета могут проводить регулярный мониторинг качества системы контентной фильтрации и принимать участие в мероприятиях по информационной безопасности ([Методические рекомендации Минкомсвязи от 16.05.2019](#)).

Образцы

[Приказ о совете по информационной безопасности учащихся](#)

[Положение о совете по информационной безопасности учащихся](#)

Какие документы оформить

Минкомсвязи рекомендует разработать семь локальных актов, которые регулируют вопросы информационной безопасности в образовательной организации ([Методические рекомендации Минкомсвязи от 16.05.2019](#)). Подробности смотрите в таблице.

Перечень документов по информационной безопасности

Название документа	Что включить	Где разместить
--------------------	--------------	----------------

<u>Положение об ограничении доступа обучающихся к информации в интернете</u>	Опишите правила использования интернета в образовательной организации и основные аспекты работы системы контентной фильтрации (СКФ)	На сайте в разделе «Информационная безопасность», подраздел «Локальные акты»
<u>Приказ о назначении ответственного лица за информационную безопасность</u>	Определите работника, который будет отвечать за обеспечение безопасного доступа в интернет. Укажите полномочия ответственного	Храните по правилам делопроизводства
<u>Порядок проведения проверки эффективности использования СКФ</u>	Опишите, кто и как проверяет работу СКФ в образовательной организации. Приложите образец акта проверки СКФ	
<u>Журнал работы СКФ</u>	Отразите в журнале сведения: дату проверки, Ф. И. О. и должность проверяющего, номер компьютера, результаты проверки, принятые меры	
<u>План мероприятий по обеспечению информационной безопасности</u>	Составьте план на учебный год, включите совместные мероприятия с органами власти и общественными организациями	На сайте в разделе «Информационная безопасность», подраздел «Локальные акты»
<u>Приказ о порядке использования персональных устройств с выходом в интернет</u>	Определите, как вы будете ограничивать доступ в интернет с персональных устройств детей. Возьмите с родителей согласие о том, что руководитель образовательной организации не несет ответственность за негативное воздействие на ребенка от интернета, доступ к которому он получил со своего устройства. В противном случае родители могут предоставить право образовательной организации забирать устройство на время учебного процесса	На сайте в разделе «Сведения об образовательной организации», подраздел «Документы». Продублируйте акт в разделе «Информационная безопасность», подраздел «Локальные акты»
Инструкции для обучающихся по информационной безопасности при использовании интернета	Включите в инструкции информацию из памяток, направленных <u>письмом Минобрнауки от 14.05.2018 № 08-1184</u>	В учебных кабинетах, в которых есть доступ в интернет

Разработайте локальные акты, которые требует [пункт 3.1](#) Требований, утвержденных [приказом Минкомсвязи от 16.06.2014 № 161](#). Отрадите в документах:

- условия и порядок размещения знака информационной продукции на материалах образовательной организации, например порядок классификации и маркировки документов библиотечного фонда, маркировки видеоматериалов;
- условия допуска детей на зрелищные мероприятия;
- меры по методической поддержке работников образовательной организации, в том числе направление их на повышение квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию;
- меры по предотвращению, выявлению и устранению нарушений законодательства о защите детей от информации, причиняющей вред их здоровью и развитию.

Рассмотрите локальные акты на заседании управляющего совета, утвердите их и ознакомьте с ними работников и учащихся ([п. 3.2](#) Требований, утв. [приказом Минкомсвязи от 16.06.2014 № 161](#)). Разместите локальные акты на [информационном стенде](#) в местах, где дети могут почитать. Опубликуйте документы на [сайте](#) образовательной организации, например в специальном разделе об информационной безопасности.

Какие мероприятия провести

Чтобы обеспечить информационную безопасность детей, установите СКФ, проверяйте библиотечный фонд, проводите просветительскую работу среди детей и родителей, отправляйте педагогов на повышение квалификации и проводите мониторинг.

Как установить СКФ

Решите, каким способом будете контролировать контент, к которому получают доступ дети. Главное, чтобы они не могли получить информацию из «черного списка» и пользовались только ресурсами «белого списка». Понятия «черный» и «белый» список ввели эксперты в [Методических рекомендациях Минкомсвязи от 16.05.2019](#). В «черный список» входит запрещенная для детей информация, а в «белый» – ресурсы из реестра безопасных образовательных сайтов (РБОС).

Ситуация

Какую информацию относят к запрещенной и ограниченной в распространении среди детей

К **запрещенной** относят информацию, которая:

- побуждает детей к совершению действий, представляющих угрозу их жизни и здоровью, в том числе к причинению вреда своему или чужому здоровью, самоубийству, убийству;

- может вызвать у детей желание употребить наркотические средства, психотропные и одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- оправдывает допустимость насилия и жестокости либо побуждает проявлять насилие по отношению к людям или животным;
- содержит изображение или описание сексуального насилия;
- отрицает семейные ценности, пропагандирует нетрадиционные сексуальные отношения и формирует неуважение к родителям и другим членам семьи;
- оправдывает противоправное поведение;
- содержит нецензурную брань;
- содержит информацию порнографического характера;
- содержит сведения о несовершеннолетнем, пострадавшем в результате противоправных действий, в том числе фамилии, имени, 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 и иную информацию, которая позволяет прямо или косвенно установить личность такого несовершеннолетнего.

К ограниченной в распространении относят информацию, которая:

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

Такой перечень устанавливает [статья 5](#) Федерального закона от 29.12.2010 № 436-ФЗ.

СКФ можно организовать разными способами:

- установить систему фильтрации на персональных компьютерах, сервере для локальной сети и устройстве для создания Wi-Fi;
- использовать внешний фильтрующий сервер, в том числе DNS-сервер или прокси-сервер;

- получить услугу фильтрации через оператора связи или специализированную организацию, которая предоставляет доступ в интернет образовательной организации.

Региональные и местные органы управления образованием могут устанавливать единые технические решения для всех подведомственных образовательных организаций. При этом школа и детский сад вправе отказаться от единого решения и разработать собственную схему СКФ ([ч. 1 ст. 28 Федерального закона от 29.12.2012 № 273-ФЗ](#)).

Когда заключаете договор на услуги контентной фильтрации, укажите, что СКФ должна соответствовать требованиям, которые изложены в [Методических рекомендациях Минкомсвязи от 16.05.2019](#).

Внимание

В договоре с организацией, которая предоставляет услуги СКФ, укажите, что она несет ответственность за ненадлежащее оказание услуг и должна возместить причиненный ущерб

Поручите ответственному за информационную безопасность вести [журнал работы СКФ](#). В него вносят сведения о том, когда включали и отключали СКФ.

Предупредите педагогов, что они не имеют права самостоятельно отключать СКФ. Если хотят отключить фильтрацию на своих персональных компьютерах, то могут это сделать, только когда нет детей на территории образовательной организации. Для этого педагог должен написать докладную записку ответственному за информационную безопасность или руководителю образовательной организации и указать причину, сроки отключения СКФ. Отключить фильтрацию можно с письменного согласия ответственного или руководителя образовательной организации.

Проверьте, есть ли на компьютерах образовательной организации антивирусные программы. Они помогут исключить доступ детей к негативной информации.

Как проверить библиотечный фонд

Поручите заведующему библиотекой провести [инвентаризацию библиотечного фонда](#) и проверить, на всей ли продукции стоит знак возрастного ограничения. Он должен стоять на документах, которые изготовили с 1 сентября 2012 года. Маркировка должна быть на печатных изданиях, кино-, видео- и фотопродукции, компьютерных программах и базах данных. Исключение составляют:

- учебники и учебные пособия, которые Минобрнауки рекомендовало или допустило к использованию в образовательном процессе ([п. 1 ч. 4 ст. 11 Федерального закона от 29.12.2010 № 436-ФЗ](#));
- издания, которые содержат научную, научно-техническую, статистическую информацию ([п. 1 ч. 2 ст. 1 Федерального закона от 29.12.2010 № 436-ФЗ](#));

- периодические печатные издания, которые специализируются на распространении информации общественно-политического или производственно-практического характера ([п. 5 ч. 4 ст. 11 Федерального закона от 29.12.2010 № 436-ФЗ](#));
- издания, которые содержат нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина ([п. 1 ч. 4 ст. 8 Федерального закона от 27.07.2006 № 149-ФЗ](#));
- издания, которые содержат информацию о состоянии окружающей среды ([п. 2 ч. 4 ст. 8 Федерального закона от 27.07.2006 № 149-ФЗ](#));
- издания, которые содержат информацию о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств ([п. 3 ч. 4 ст. 8 Федерального закона от 27.07.2006 № 149-ФЗ](#)).

Пример

Примеры знака возрастного ограничения

Знак информационной продукции определяет ее категорию и зависит от возраста детей, которым можно показывать эту продукцию. Вместо знака можно поставить текстовое предупреждение или указать и знак, и текст одновременно.

Возраст ребенка	Какой знак ставить	Какое текстовое предупреждение указать
До 6 лет	0+	—
От 6 до 12 лет	6+	«для детей старше шести лет»
От 12 до 16 лет	12+	«для детей старше 12 лет»
От 16 до 18 лет	16+	«для детей старше 16 лет»
Любой – если информация запрещена для детей	18+	«запрещено для детей»

Законодатель не определяет размер, цвет знака и место, где его размещать. Исключение – когда информация запрещена для детей. Но таких документов в школе и детском саду быть не должно.

Чтобы быстро промаркировать информационную продукцию, распечатайте знаки возрастных ограничений на самоклеющихся листах формата А4.



Если на продукции, которая не входит в [исключения](#), не обнаружили знака ограничения, поручите работникам библиотеки промаркировать ее. Иначе проверяющие могут

оштрафовать образовательную организацию и ее работников до 200 тыс. руб. и конфисковать немаркированную продукцию ([ч. 2 ст. 13.21 КоАП](#)).

Чтобы промаркировать продукцию, ее надо классифицировать. Для этого закупите услуги у экспертов или экспертных организаций, которые имеют аккредитацию Роскомнадзора. Можно классифицировать продукцию своими силами. В таком случае создайте комиссию по возрастной классификации продукции библиотечного фонда.

В состав комиссии включите специалистов в сфере возрастной психологии, культуры, педагогики, филологии и библиотечного дела, например заведующего библиотекой, педагога-психолога, учителя русского языка и литературы и учителя начальных классов.

Комиссия должна оценить немаркированную продукцию и определить, какой знак на что поставить. Для этого члены комиссии руководствуются положениями [главы 2](#) Федерального закона от 29.12.2010 № 436-ФЗ.

Работу комиссии организуйте на основании положения, которое образовательная организация разрабатывает самостоятельно. Укажите в положении термины и определения, которыми будет пользоваться комиссия. Пропишите порядок классификации каждого вида продукции.

Чтобы обезопасить себя при закупке книг и другой информационной продукции, включите в договоры с поставщиками пункт об ответственности поставщика, если он поставит продукцию без знаков возрастного ограничения. В таком случае образовательная организация вправе требовать возмещения убытков, которые понесет в результате того, что поставщик нарушил [Закон от 29.12.2010 № 436-ФЗ](#). Такой совет дает Минкомсвязи в [Рекомендациях](#), утвержденных 22.01.2013 № АВ-П17-531.

Какие обучающие мероприятия провести

Обучайте учеников и воспитанников цифровой безопасности в рамках занятий по информатике и ИКТ, курсов по выбору, внеурочной деятельности, дополнительного образования. Проводите тематические мероприятия – собственные или совместно с общественными организациями и органами власти. Например, присоединяйтесь к единому уроку по безопасности в интернете, всероссийскому «Уроку цифры».

Предложите детям поучаствовать в квесте по цифровой грамотности «Сетевичок». В конкурсе могут принять участие ученики с 1-го по 4-й класс, с 5-го по 8-й и с 9-го по 11-й. Чтобы участвовать, каждый ребенок должен пройти [регистрацию на сайте](#).

Проводите с учениками классные часы по информационной безопасности. Раздайте детям [памятки](#), которые направило Минобрнауки [письмом от 14.05.2018 № 08-1184](#). Расскажите ученикам, что организовали [специальный подраздел сайта](#), в котором собрали полезную и интересную информацию для детей. Разместите в подразделе памятки для детей, информацию про конкурсы и проекты, которые посвящены цифровому обучению.

На родительских собраниях обсудите, что важно следить за информационной безопасностью детей дома, контролировать интернет-контент, которым пользуется ребенок. Раздайте родителям памятки, которые направило Минобрнауки [письмом от 14.05.2018 № 08-1184](#).

Кого отправлять на повышение квалификации

Отправляйте на повышение квалификации: ответственного за информационную безопасность, учителей-предметников, которые обучают с помощью интернета, классных руководителей, воспитателей.

Эксперты Временной комиссии по развитию информационного общества рекомендуют ответственным проходить курс по теме «Организация защиты детей от видов информации, распространяемой посредством интернета, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования». Педагоги должны пройти курс «Безопасное использование сайтов в интернете в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации». Курсы можно пройти бесплатно на [сайте «Единый урок»](#).

Как проводить мониторинг

Поручите ответственному за информационную безопасность следить ежеквартально за изменением законодательства в сфере информационной безопасности детей. Обо всех изменениях ответственный должен сообщать руководителю образовательной организации и педагогам. Если из-за новшеств в законодательстве надо поправить локальные акты, то поручите ответственному подготовить проекты новых документов.

Попросите ответственного готовить ежегодно до 30 августа три отчета – о качестве работы СКФ и соблюдении мер по защите детей от негативной информации, а также о сайтах, которые организация использовала в обучении и воспитании ([Методические рекомендации Минкомсвязи от 16.05.2019](#)).

Если ответственный получит жалобу о нарушении законодательства в сфере информационной безопасности детей, то должен в течение 10 дней ее рассмотреть и принять меры. Заявителю надо отправить мотивированный ответ о предпринятых действиях ([подп. 3.4–3.4.2](#) Требований, утв. [приказом Минкомсвязи от 16.06.2014 № 161](#)).

Кто проконтролирует

То, как школа и детский сад соблюдают законодательство в сфере информационной безопасности детей, могут проверить: учредитель, региональные органы управления образованием, прокуратура, общественные объединения. Кроме того, Временная комиссия Совета Федерации по развитию информационного общества проводит ежегодный мониторинг качества работы СКФ и соблюдения мер по защите детей от негативной информации. Результаты мониторинга направляют в Минпросвещения и Минцифры.

Эксперты Временной комиссии по развитию информационного общества рекомендуют проверять школы и сады по трем направлениям. Подробности смотрите в таблице.

Что проверяют в сфере информационной безопасности детей

Направление проверки	Что проверяют	Как подготовиться
Соблюдение Методических рекомендаций Минкомсвязи от 16.05.2019	Проконтролируют, есть ли СКФ и как она работает, все ли локальные акты приняли, назначен ли ответственный	Назначьте приказом ответственного за информационную безопасность детей. Утвердите локальные акты , которые перечислены в Методических рекомендациях Минкомсвязи от 16.05.2019 и пункте 3.1 Требований, утвержденных приказом Минкомсвязи от 16.06.2014 № 161
Организационно-административные мероприятия	Проверяют, как образовательная организация соблюдает Требования, утвержденные приказом Минкомсвязи от 16.06.2014 № 161	Установите СКФ. Проверяйте библиотечный фонд. Проводите просветительскую работу среди детей и родителей. Отправляйте педагогов на повышение квалификации и проводите мониторинг
Доступ к информации в интернете	Проверяют, можно ли в образовательной организации через интернет получить доступ к негативной информации, в том числе запрещенной для детей, – в форме сайтов, графических изображений, аудиовизуальных произведений	Ежегодно контролируйте, как работает СКФ. Дети должны получать доступ только к информации из «белого списка» и той, которая соответствует их возрасту

Внимание

Если не примете меры по защите детей от информации, которая причиняет вред их здоровью и развитию, то организации и ее работникам грозит административная ответственность по части 2 статьи 13.21 и статье 6.17 КоАП

Проверяющие оштрафуют:

- должностных лиц на сумму до 20 тыс. руб.;
- образовательную организацию – до 200 тыс. руб.

Кроме того, проверяющие могут приостановить деятельность образовательной организации на срок до 90 суток и конфисковать предмет административного правонарушения, то есть продукцию, которая содержит вредную и запрещенную информацию.

Чтобы не получить наказание, проверьте контрольные точки, на которые обращают внимание проверяющие:

- есть ли локальные акты, которые регулируют доступ к вредной и запрещенной информации, и назначен ли за это ответственный;
- есть ли контроль доступа в сеть Интернет и фильтрация контента;
- обучаете ли детей правилам безопасного поведения в интернет-пространстве, что предотвратит риск их вовлечения в противоправную деятельность;
- принимаете ли меры по защите детей от негативной информации.

© Материал из Справочной системы «Образование»

<https://plus.1obraz.ru>

Дата копирования: 16.08.2023