

Как обеспечить  
информационную  
безопасность детей в  
школе и детском саду?

# Правительство утвердило Концепцию информационной безопасности детей.

Правительство указывает, что дети крайне уязвимы с точки зрения информационной безопасности. С одной стороны, они обладают нестабильной эмоциональной сферой и низким уровнем критичности восприятия. С другой – интернет-среда наполнена деструктивной информацией, в том числе противоправного характера. Такая ситуация способствует формированию у детей и подростков неправильного восприятия традиционных российских духовно-нравственных ценностей и провоцирует «психологический слом», следствием которого могут стать депрессивное состояние или проявление девиантного поведения, повышенной агрессии к окружающим (раздел I Концепции, утв. распоряжением Правительства от 28.04.2023 № 1105-р).

Школы и детские сады обязаны обеспечить информационную безопасность детей.

Под ней Правительство РФ понимает состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и физическому, психическому, духовному, нравственному развитию.

## Кого назначить ответственным?

Информационная безопасность – комплексная сфера, поэтому в ее обеспечении должны принимать участие все работники школы и детского сада в пределах своей компетенции. Дополнительно образовательная организация обязана создать безопасные условия обучения (п. 2 ч. 6 ст. 28 Федерального закона от 29.12.2012 № 273-ФЗ). Получается, что за информационную безопасность отвечает и **руководитель** как единоличный исполнительный орган.

## ПРИМЕР

Распределение  
полномочий по  
информационной  
безопасности

между  
сотрудниками

Должность и

Функции

### *Учитель и воспитатель*

Контролирует, чтобы содержание частей ООП и их реализация обеспечивали комфортную атмосферу для детей, позволяли обучить детей вопросам информационной безопасности.

Подбирает средства обучения и воспитания, которые соответствуют законодательству, в том числе с позиции информационной безопасности.

Распределение  
полномочий по  
информационн  
ой  
безопасности  
между  
сотрудниками

Должность и  
Функции

*Классный руководитель*

Реализует воспитательные мероприятия, в том числе по вопросам информационной безопасности.

Взаимодействует с родителями, чтобы углубить их знания в сфере инфобезопасности, объясняет, как обучить этому детей

*Педагог-психолог*

Проводит просветительскую и профилактическую работу по вопросам психологической уязвимости в цифровой среде.

Проводит индивидуальную работу с детьми и родителями, если они пострадали от действий в интернете — мошенничества, буллинга и т. д.

Распределение  
полномочий по  
информационн  
ой  
безопасности  
между  
сотрудниками

Должность

Функции

### *Администратор сайта*

Мониторит наполнение сайта школы и детского сада, в том числе на соответствие законодательства о защите прав детей.

Контролирует, чтобы наполнение госпабликов соответствовало правилам инфобезопасности, в том числе создает просветительский контент по этим вопросам

### *Педагог-библиотекарь*

Контролирует безопасность использования цифровых ресурсов библиотеки.

Мониторит состав библиотечного фонда, чтобы в нем отсутствовала литература экстремистского характера и другая, способная причинить вред психике детей.

Распределение  
полномочий по  
информационн  
ой  
безопасности  
между  
сотрудниками

Должность и  
Функции

### *Заместитель руководителя*

Организует мониторинг соблюдения работниками законодательства в сфере инфобезопасности и защиты прав детей.

Предлагает проекты локальных актов, планов мероприятий и других документов в сфере обеспечения инфобезопасности в школе или детском саду.

Удобно поручить основные вопросы информационной безопасности заместителю руководителя или коллегиальному органу – например, совету. В него можно включить педагогов, родителей и представителей органов власти. Пригласите членов общественных организаций, например кибердружин. Поручите членам совета проводить регулярный мониторинг качества системы контентной фильтрации и принимать участие в мероприятиях по информационной безопасности (Методические рекомендации Минкомсвязи от 16.05.2019).

Назначение ответственных оформите приказом. Если решили создать совет, регламент его работы изложите в отдельном локальном акте, например положении.

Распределение  
полномочий по  
информационн  
ой  
безопасности  
между  
сотрудниками

Должность и  
Функции

***Руководитель***

Ведет общий контроль исполнения поручений в сфере инфобезопасности.

Утверждает локальные акты по вопросам инфобезопасности.

Организует взаимодействие с социальными партнерами, госорганами, общественными организациями по вопросам инфобезопасности.

## Раздел сайта «Информационная безопасность»

***Школы*** могут оформить раздел сайта на основании Методических рекомендаций, направленных письмом Минобрнауки от 14.05.2018 № 08-1184. Раздел понадобится, чтобы информировать учеников, родителей и педагогов о безопасном поведении в интернете.

**Детские сады** вправе не оформлять раздел «Информационная безопасность», так как Методические рекомендации адресованы только школам. Однако сады должны также соблюдать законодательство об информационной безопасности детей, вести работу с родителями (п. 29.3.5.1 ФОП ДО). Поэтому рекомендуем оформить этот раздел и опубликовать там документы.

***Что включить в раздел «Информационная безопасность»?***

### ***Локальные акты***

Приказ об организации информационной безопасности детей и назначении ответственного.

Положение об ограничении доступа обучающихся к информации в интернете.

Политика обработки персональных данных.

Положения об обработке персональных данных обучающихся и работников.

Копии документов в формате PDF или в виде электронного документа, подписанного электронной подписью.

## Раздел сайта «Информационная безопасность»

### *Нормативное регулирование*

Нормативные правовые акты разных уровней. Например, сделайте ссылки на федеральные акты:

- ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- ФЗ «О персональных данных»;
- ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;
- распоряжение Правительства от 28.04.2023 № 1105-р.

Добавьте региональные и муниципальные акты, которые регулируют вопросы информационной безопасности несовершеннолетних.

Можете разместить письма Минпросвещения от 29.03.2019 № 03-393, от 07.06.2019 № 04-474 и Минобрнауки от 14.05.2018 № 08-1184

### *Педагогам*

Укажите информацию о ближайших мероприятиях, проектах и программах по вопросам информационной безопасности несовершеннолетних и информационной грамотности педагогических работников.

Разместите методички и другие материалы для работы педагогов

Текст на странице сайта.

Копии документов в формате PDF

## Раздел сайта «Информационная безопасность»

### *Обучающимся*

Разместите памятки от Минобрнауки. Например, про социальные сети, кибербуллинг, цифровую репутацию и т.д.

Перечислите детские конкурсы и проекты, которые посвящены цифровому обучению.

### *Родителям*

Разместите памятки от Минобрнауки – про информационную безопасность дома, контроль общения ребенка в интернете и др.

Детские безопасные сайты

Перечислите рекомендуемые к использованию в учебном процессе безопасные сайты. Разместите их баннеры.

Используйте перечень рекомендуемых интернет-ресурсов для детей и родителей, который направило Минпросвещения письмом от 29.12.2021

# Информационная инфраструктура

Информационная инфраструктура школы и детского сада в основном включает две составляющие: *организация доступа к интернету и библиотечный фонд*. Также образовательные организации пользуются платформой ФГИС «Моя школа», но безопасность ее контента изначально контролирует Минпросвещения.

## **Интернет**

С 2022 года все государственные и муниципальные школы и детские сады подключают к интернету через единую сеть передачи данных (ЕСПД). Это снимает задачу организации контентной фильтрации и детального мониторинга ресурсов (распоряжение Правительства от 29.12.2021 № 3963-р).

ЕСПД – виртуальная сеть для доступа социально значимых объектов к государственным информационным системам и интернету. Ядро сети – сервис контентной фильтрации для безопасного доступа ко всем необходимым для обучения образовательным сайтам и сервисам. При этом блокируются запрещенные Роскомнадзором сайты и ресурсы, содержащие экстремистские и порнографические материалы, информацию о наркотиках, призывы к суициду, кибербуллинг и другие темы, опасные для психики детей. Для борьбы с вредоносным ПО в систему контентной фильтрации встроен антивирус, который проверяет входящий трафик и блокирует зараженные файлы и сайты.

ЕСПД также блокирует доступ к популярным социальным сетям. Школы и детские сады могут предоставлять или блокировать доступ к информационным ресурсам через личные кабинеты (письмо Минпросвещения от 09.07.2024 № 04-ПГ-МП-35844).

Подключение к ЕСПД проводит только «Ростелеком». Он же проверяет помещения и оборудование образовательной организации на безопасность и соответствие требованиям для размещения криптографических средств защиты информации.

Чтобы управлять работой ЕСПД, зарегистрируйтесь в личном кабинете на сайте «Ростелекома». Это можно сделать через «Госуслуги».

В разделе «Сведения об организации» автоматически отображаются сведения о школе или детском саде. В «Обратной связи» можно заполнить электронную форму – написать по любому вопросу, кроме технической проблемы. Есть также раздел «Создание заявки». Через него регулируют включение и отключение контентной фильтрации, блокируют или разрешают доступ к конкретным ресурсам.

Поручите ответственному ознакомиться с гайдом по личному кабинету от «Ростелекома». В нем подробно изложены варианты действий при разных ситуациях – поломки интернета, блокировки ПО и т. д. При необходимости используйте регламент технической поддержки. В нем указаны телефон и почта для круглосуточной связи, а также что входит в компетенцию техподдержки.

# Библиотечный фонд

**Библиотечный фонд** нужно проверять на отсутствие экстремистских материалов и наличие возрастной маркировки. Последняя должна стоять на документах, которые изготовили с 1 сентября 2012 года: печатных изданиях, кино-, видео- и фотопродукции, компьютерных программах и базах данных. Исключение составляют:

- **учебники и учебные пособия**, которые Минобрнауки и Минпросвещения 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).

Поручите заведующему библиотекой также мониторить библиотечный фонд, чтобы в нем не было экстремистской литературы. Это можно проводить одновременно с проверкой маркировки или отдельно, например при плановой или внеплановой инвентаризации. Подробнее – в рекомендациях «Как проводить проверку библиотечного фонда», «Как проверить библиотечный фонд на экстремистские материалы».

# Просветительские мероприятия

Правительство распорядилось интегрировать в образовательный процесс уроки информационной безопасности и цифровой грамотности детей, а также постоянно проводить просветительские мероприятия, направленные на информирование детей, родителей, работников (раздел IV Концепции, утв. распоряжением Правительства от 28.04.2023 № 1105-р).

Основная просветительская работа среди детей проводится в школе, так как дошколята еще не способны осознать риски цифрового пространства. В детском саду больше внимания уделяйте работе с родителями.

Для обучения инфобезопасности можно отвести урочное и внеурочное время, занятия дополнительного образования.

В зависимости от возраста учеников подойдут разные приемы и формы работы.

**На уровне начального образования** педагоги формируют у школьников базовые умения работы с информацией. Например, приучают детей мыслить критически, анализировать новую информацию, сопоставлять ее с уже известной, сравнивать и делать выводы, находить источник информации в конкретных ситуациях.

В работе с младшими школьниками лучше использовать игровые методы, чтобы в непринужденной и доступной форме имитировать жизненные ситуации, учиться с ними справляться.

## **На уровне ООО и СОО**

В основной школе подростки уже достаточно активно используют интернет, в том числе для выполнения домашних заданий и школьных проектов. Они совершают покупки через маркетплейсы, играют в онлайн-игры, вступают в онлайн-сообщества. Это показывает, насколько дети нуждаются в информационной безопасности. Попросите педагогов соблюдать баланс между негативом и позитивом в подаче материала детям.

**Основная задача в средней школе** – сформировать представление об основных опасностях интернета. Важно убедить детей не выдавать личную информацию в соцсетях, сообщениях в чатах или электронной почте, при регистрации на сомнительных ресурсах.

Пусть педагоги объяснят подросткам также опасность личных встреч с людьми, с которыми познакомились через интернет, особенно если те упорно настаивают на встрече и на том, что о ней не нужно говорить родителям, учителям.

Необходимо объяснить детям, что в интернете, так же как и в реальной жизни, нужно вести себя вежливо и корректно, чтобы не становиться причиной киберагрессии. Нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

С подростками удобно организовать кейс-поединки на тему информационной безопасности. Учебные кейсы – проблемные ситуации, для которых нет очевидного и единственно верного решения. Задача учеников – найти выход из ситуации. Такой подход позволяет расширить кругозор детей, проявить смекалку и усвоить навыки безопасности на практике.

# Полезные ресурсы

Предложите педагогам использовать федеральные и региональные ресурсы при реализации занятий по инфобезопасности.

## **Платформа «Урок цифры»**

Возможность получить знания от ведущих технологических компаний: «Яндекса», «Лаборатории Касперского», Фирмы «1С», госкорпорации «Росатом», VK, Благотворительного фонда «Вклад в будущее», «Авито» и Группы «Астра».

На платформе представлена коллекция уроков по работе в цифровой среде. Каждый урок имеет разбивку материалов по классам – для 1–4-х, 5–9-х и 10–11-х. Контент разнообразный – содержит видеолекции, сценарии, тренажеры и другие форматы, которые сгруппированы по разделам «ученику», «учителю», «родителю».

## ***Портал «Лига безопасного Интернета»***

Можно найти разноформатный материал по вопросам безопасного использования интернета детьми – статьи, курсы лекций и семинаров, наглядные пособия, памятки и др.

Проводят Всероссийский ежегодный урок безопасного интернета и конкурс школьных сочинений «Безопасный интернет»

## ***Памятки по инфобезопасности***

Разместите памятки и другую полезную информацию для детей и родителей в специальном подразделе сайта школы

Направляйте педагогов на повышение квалификации в области обеспечения безопасности и развития детей в информационном пространстве (раздел V Концепции, утв. распоряжением Правительства от 28.04.2023 № 1105-р). Особенно это понадобится ответственному за информационную безопасность, учителям, которые обучают с помощью интернета, классным руководителям и воспитателям.

# Воспитательные мероприятия

Помимо просветительских мероприятий по темам инфобезопасности важно проводить разнонаправленную *воспитательную работу* с детьми:

- воспитывать детей в духе уважения к традиционным ценностям через усвоение системы семейных ценностей и представлений о семье;
- обеспечивать ценностное, моральное и нравственно-этическое развитие детей;
- возвращать у детей ответственность за свою жизнь, здоровье и судьбу, изживать социальное потребительство и инфантилизм;
- развивать систему социальных и межличностных отношений и общения детей;
- формировать познавательные потребности и интересы, детскую любознательность и исследовательскую активность, творческие способности;
- воспитывать у детей толерантность;
- поддерживать проекты, направленные на продвижение традиционных ценностей в информационной среде.

Проверьте, чтобы в рабочие программы воспитания школы и детского сада включали эти цели. В общем они уже содержатся в примерных программах из ФОП ДО, НОО, ООО и СОО. Используйте любые форматы в качестве воспитательных мероприятий – упомянутые разработчиками ФОП и придуманные вашими коллегами.

# Какие документы оформить?

Установленного законом перечня документов нет.

Решите это самостоятельно.

Предлагаем примерный набор актов, чтобы организовать работу: *приказ об ответственном, план мероприятий, положения об информационной безопасности и работе совета* – если создали его.

Ознакомьте работников с локальными актами по инфобезопасности и разместите их в общедоступном для всех месте – например, на информационном стенде в фойе или на сайте школы.