

Положение  
об организации и обеспечении информационной безопасности  
обучающихся при работе в сети «Интернет»  
в общеобразовательном учреждении

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании следующих документов:

- «Конвенция о правах ребенка» (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990);
- Федеральный закон от 24.07.1998 № 124 «Об основных гарантиях прав ребенка в Российской Федерации»;
- Федеральный закон от 25.07.2002 № 114 «О противодействии экстремистской деятельности»;
- Федеральный закон от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 29.12.2010 № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» и все его изменения;
- Федеральный закон от 28.07.2012 № 139 «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 02.12.2015 № 2471-р;
- методические рекомендации Совета Федерации Федерального собрания Российской Федерации 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;
- приказ Департамента образования и молодежной политики ХМАО – Югры от 19.08.2013 № 798 «О контроле за Интернет-ресурсами, используемыми в деятельности образовательными учреждениями».

1.2. Настоящее положение разработано с целью ограничения доступа общеобразовательной организации к информации, причиняющей вред здоровью (или) развитию обучающихся, а также не соответствующей целям и задачам образования.

1.3. Контроль организации контентной фильтрации (далее – КФ) ресурсов сети «Интернет» в образовательной организации осуществляется департаментом образования и муниципальным автономным учреждением «Информационно-методический центр» (далее – МАУ «ИМЦ»).

1.4. Все обязанности по обеспечению эффективного функционирования средств контентной фильтрации (далее – СКФ) регулируются локальными нормативными актами образовательной организации (приказами, положением и должностными инструкциями, утвержденными директором образовательной организации).

1.5. Ознакомление с положением и его соблюдение обязательно для всех сотрудников образовательной организации.

1.6. Срок действия данного Положения не ограничен. Положение действует до принятия нового.

2. ОБЯЗАННОСТИ ДИРЕКТОРА И СОТРУДНИКОВ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ ПРИ РАБОТЕ В СЕТИ «ИНТЕРНЕТ»

## 2.1. ДИРЕКТОР образовательной организации:

- осуществляет общее управление по организации КФ в образовательной организации;
- устанавливает правила по ограничению физического доступа обучающихся к автоматизированным рабочим местам (далее – АРМ) педагогов и сотрудников образовательной организации (например: запретить нахождение обучающихся в кабинетах на перемене в отсутствие сотрудника образовательной организации, где есть АРМ с выходом в сеть «Интернет»);
- назначает заместителя директора, ответственного за организацию и обеспечение информационной безопасности в образовательной организации;
- назначает специалиста, ответственного за техническое сопровождение СКФ ресурсов сети «Интернет»;
- принимает решение о создании совета по обеспечению информационной безопасности обучающихся (далее – Совет) и утверждает его состав;
- разрабатывает план мероприятий образовательной организации по обеспечению информационной безопасности обучающихся при работе в сети «Интернет» на 2019-2020 годы (далее – План мероприятий) на основании примерного плана мероприятий по обеспечению информационной безопасности обучающихся при работе в сети «Интернет» на 2019-2020 годы;
- несет полную ответственность за качественное выполнение Плана мероприятий.

## 2.2. Ответственный заместитель директора образовательной организации:

- исполняет План мероприятий;
- контролирует деятельность сотрудников образовательной организации, в том числе технического специалиста по исполнению Плана мероприятий;
- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети «Интернет»;
- осуществляет хранение в сейфе логинов и паролей, установленных на операционную систему и программу, осуществляющую КФ на персональных компьютерах обучающихся, и предоставляет их сотрудникам МАУ «ИМЦ» для выполнения функциональных обязанностей.

## 2.3. Технический специалист:

- исполняет План мероприятий;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательной деятельности.

## 2.4. Совет по обеспечению информационной безопасности обучающихся:

- принимает участие в реализации Плана мероприятий.

## 2.5. Сотрудники образовательной организации:

- соблюдают в своей профессиональной деятельности законодательство РФ в области информационной безопасности, в том числе КФ при работе с обучающимися в сети «Интернет»;
- исполняют План мероприятий;
- принимают меры по пресечению обращений, обучающихся к ресурсам, не имеющим отношения к образовательной деятельности.

## 3. СОТРУДНИКАМ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ РАЗРЕШАЕТСЯ:

- отключать СКФ на своих персональных устройствах или устройствах, предоставленных педагогическому работнику, только после осуществления образовательной деятельности и отсутствия обучающихся на территории образовательной организации, а также получения письменного согласия от директора или заместителя директора образовательной организации

с указанием или пояснением целей отключения СКФ и временных сроках отключения СКФ с занесением информации в журнал работы КФ.

#### 4. СОТРУДНИКАМ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ЗАПРЕЩАЕТСЯ:

##### 4.1. При работе на автоматизированном рабочем месте:

- работать в сети «Интернет», без прохождения соответствующего инструктажа;
- подключать оборудование, проводить настройку сети и СКФ самостоятельно (кроме технического специалиста, отвечающего за техническое сопровождение СКФ ресурсов сети «Интернет»);
- отключать СКФ во время нахождения на территории образовательной организации обучающихся;
- использовать поисковые системы Yandex, Google, Rambler, Mail.ru и т.д., кроме поисковых систем сервиса ООО «СкайДНС», <http://search.skydns.ru>;
- обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- осуществлять любые сделки через сеть «Интернет»;
- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы;
- загружать и распространять:
  - ✓ материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности компьютерного или телекоммуникационного оборудования;
  - ✓ программы, для осуществления несанкционированного доступа, серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети «Интернет», а также размещать ссылки на вышеуказанную информацию;
- пользоваться чужими учетными данными при использовании сетевых сервисов, предполагающих авторизацию.

4.2. Работать на своих персональных (личных) устройствах без СКФ в присутствии обучающихся на территории образовательной организации.

План мероприятий по информационной безопасности  
при работе в сети «Интернет» на 2022–2025 годы

№	Мероприятие	Сроки	Сроки предоставления отчетов в МАУ «ИМЦ»
I. Деятельность руководителя образовательной организации, заместителя руководителя образовательной организации			
1.	Изучение нормативных правовых документов, методических рекомендаций и издание (актуализация) организационно-распорядительных документов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет»	Август	-
2.	Ознакомление работников образовательной организации: -об ответственности за нарушение требований законодательства Российской Федерации в частности доступа к информации, причиняющей вред здоровью и (или) развитию учащихся, а также не соответствующей задачам образования; -с образовательного учреждения и планом мероприятий по информационной безопасности при работе в сети «Интернет» на 2022-2025 годы	Август	-
3.	Организация проведения мероприятий для учащихся и родителей(законных представителей) по: -информированию об ответственности за нарушение требований законодательства РФ в части доступа к информации, причиняющей вред здоровью и (или) развитию учащихся, а также не соответствующей задачам образования; - ознакомление с организационно- распорядительными документами образовательного учреждения и планом мероприятий по информационной безопасности при работе с сети «Интернет» на 2022-2025годы	сентябрь	До 30 сентября-
4.	Организация проведения просветительской работы с учащимися и их родителями (законными представителями) по повышению цифровой культуры и информационной безопасности (по отдельному перечню мероприятий согласно разделу V)	В течении года	-
5.	Оформление и обновление стенда «Информационная безопасность»	В течение учебного года	-
6.	Обеспечение ведения информационной работы через: 1. Официальный сайт образовательного учреждения (страница	В течение учебного года	Мониторинг ведения web-страниц по информационной

	<p>«Информационная безопасность» в разделе «Официально», на которую осуществляется ссылка со страницы «Информационная безопасность» в разделе «Родителям и ученикам»)</p> <p>2. Государственная информационная система ХМАО - Югры «Цифровая образовательная платформа Ханты-Мансийского автономного округа Югры (ГИС Образование Югры) в муниципальном общеобразовательном учреждении» (администратор – в разделе «Объявления», класный руководитель – использую инструмент «Сообщения»).</p>		<p>безопасности осуществляет МАУ «ИМЦ» (по отдельному графику)</p>
<p>II. II. Деятельность технического специалиста</p>			
1.	<p>Обеспечение:</p> <p>1. Установки, настройки и работы на персональных компьютерах общеобразовательного учреждения антивирусного обеспечения</p> <p>2. Отдельного доступа каждого педагога общеобразовательного учреждения для работы на автоматизированном рабочем месте (установка/смена пароля для входа в операционную систему)</p>	<p>По мере обновления лицензии</p>	-
		<p>Не реже чем 1 раз в квартал</p>	
2.	<p>Ведение журнала регистрации случаев обнаружения образовательной организацией сайтов, причиняющих вред здоровью и развитию обучающихся, а также не соответствующих задачам образования</p>	<p>В течение учебного года</p>	-
3.	<p>Составление докладной записки на имя директора общеобразовательного учреждения и председателя Совета по обеспечению информационной безопасности учащихся по каждому выявленному факту доступа к ресурсам, не имеющим отношения к образовательной деятельности</p>	<p>По мере необходимости</p>	
4.	<p>Осуществлять взаимодействие с технической службой ПАО «Ростелеком» по:</p> <ul style="list-style-type: none"> <li>- исключению(в случае обнаружения) выявленных интернет - ресурсов, содержащих информацию, причиняющую вред здоровью и развитию обучающихся, а также не соответствующих задачам образования;</li> <li>- организация доступа к необходимым для обеспечения качественного образовательного процесса интернет – ресурсам.</li> </ul>	<p>По мере необходимости</p>	
5.	<p>Размещение материалов по информационной безопасности на официальном сайте образовательного учреждения на странице «Информационная безопасность» в разделе «Официально», на которую осуществляется ссылка со страницы «Информационная безопасность» в разделе «Родителям и ученикам».</p>	<p>В течение учебного года</p>	

III. Деятельность Совета по обеспечению информационной безопасности обучающихся			
1.	Участие в реализации плана мероприятий по информационной безопасности при работе в сети «Интернет» на 2022-2025 годы	В течение учебного года	-
IV. Деятельность сотрудников образовательной организации			
1.	Изучение актуальных материалов по вопросам информационной безопасности при работе в сети «Интернет»	По мере необходимости	
2.	Инструктаж учащихся о правилах использования сети «Интернет» в общеобразовательном учреждении, в том числе средствами мобильной сотовой связи. Ведение журнала инструктажа учащихся	сентябрь	
3.	Осуществление контроля за использованием учащимися ресурсов сети «Интернет» средствами мобильной сотовой связи на территории общеобразовательного учреждения в период урочной деятельности, внеклассных мероприятий, классных часов и др.)	В течение учебного года	
4.	Информирование о фактах нарушения учащимися установленных правил пользования сети «Интернет» в ОУ	По мере необходимости	-
5.	Организация просветительской работы с обучающимися и их родителями (законными представителями) по повышению культуры и информационной безопасности (по перечню мероприятий согласно разделу V)	В течение учебного года	В течение 3 рабочих дней с даты проведения мероприятия
V. Мероприятия по повышению культуры и информационной безопасности.			
1.	«День Интернета»	30 сентября	В течение 3 рабочих дней с даты проведения мероприятия
2.	Мероприятия проекта «Цифровой ликбез» <a href="https://digital-likbez.dataiesson.ru/">https://digital-likbez.dataiesson.ru/</a>	В течение учебного года	В течение 3 рабочих дней с даты проведения мероприятия
3.	Мероприятия проекта «Урок Цифры» <a href="https://xn--hladlhdnlo2c.xn--plai/">https://xn--hladlhdnlo2c.xn--plai/</a>	По графику «Урок цифры»	В течение 3 рабочих дней с даты проведения мероприятия
4.	«День цифры» <a href="https://xn--hladlhdnlo2c.xn--plai/camp">https://xn--hladlhdnlo2c.xn--plai/camp</a>	каникулы	В течение 3 рабочих дней с даты проведения мероприятия
5.	Проведение мероприятий по ознокамлению с программными продуктами, отвечающими за контроль использования ресурсов сети «Интернет» (в том числе Kaspersky Safe kids)	сентябрь	До 30 сентября