Приложение 1
к приказу
от 08.10.2019 № Ш12-13-743/9

Положение
об организации и обеспечении информационной безопасности обучающихся при работе в сети «Интернет» в МБОУ СШ №12

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 экстремисткой 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 молодёжной политики ХМАО – Югры от 19.08.2013 № 798 «О контроле за Интернет-ресурсами, используемыми в деятельности образовательными учреждениями».

1.2. Настоящие положение разработано с целью ограничения доступа в общеобразовательных организациях и организациях дополнительного образования, подведомственных департаменту образования (далее – образовательные организации) к информации, причиняющей вред здоровью и (или) развитию обучающихся, а также не соответствующей целям и задачам образования.

1.3. Контроль организации контентной фильтрации (далее – КФ) ресурсов сети «Интернет» в образовательных организациях 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 отсутствии 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 информационный 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.