Приложение 1

к приказу №135/2 от 01.09.2014г

**Инструкция по обеспечению безопасного доступа учащихся к ресурсам сети Интернет в МБОУ Речицкой ООШ**

**Пояснительная записка**

В настоящей инструкции рассматриваются наиболее значимые направления организации безопасного использования ресурсов сети Интернет (РСИ) в образовательном учреждениии (ОУ): контентная фильтрация, техническое и административное ограничение доступа к опасным и вредоносным РСИ, антивирусная защита, обучение пользователей безопасной работе с РСИ, формирование пользовательской культуры, одним из показателей которой может служить навык предпочтительного обращения к доброкачественным ресурсам, что особенно важно в отношении учащихся ОУ.

Предлагаемая инструкция содержит предписания административного, организационного и технического характера, исполнение которых поможет существенно обезопасить образовательную среду ОУ, повысить эффективность и качество освоения учащимися РСИ, современных информационных технологий и способствовать созданию психологически благоприятной обстановки на уроках, учебных занятиях, на переменах.

Исполнение инструкции предполагает распределение между работниками ОУ функционала ответственности за информационную безопасность ОУ, за точку доступа к Интернету, за антивирусную защиту компьютерной техники, за защиту персональных данных, функционала системного администратора локальной информационной сети, однако на практике в ОУ принято совмещать некоторые обязанности в исполнении одного должностного лица, что централизует организацию процесса пользования РСИ и не противоречит действующему законодательству.

**1. Мероприятия по контентной фильтрации**

1.1. Ознакомить лицо, ответственное за информационную безопасность ОУ, с «Методическими и справочными материалами для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания», подготовленными Экспертным педагогическим сообществом в соответствии с рекомендациями Министерства образования и науки РФ (<http://www.skf.edu.ru/Help.aspx>).

1.2. Установить наличие/ отсутствие локальных контентных фильтров (ЛКФ) Единой системы контентной фильтрации — **СКФ** (техническое ограничение доступа к информации) на всех персональных компьютерах, находящихся в ОУ и имеющих доступ к сети Интернет.

1.3. В случае отсутствия СКФ необходимо предпринять меры по её установке и пройти регистрацию ОУ на сайте, рекомендованном Министерством образования и науки РФ: [http://www.skf.edu.ru](http://www.skf.edu.ru/HowToRegister.aspx) .

**2. Мероприятия по антивирусной защите компьютерной техники в ОУ**

2.1. Приказом директора ОУ утвердить Инструкцию по запуску и обновлению антивирусного программного обеспечения в ОУ; назначить ответственного за антивирусную защиту компьютерной техники ОУ .

2.2. Установить соответствие автоматизированных рабочих мест в ОУ Спецификации автоматизированного рабочего места, предоставляемого субъектами Российской Федерации в образовательные учреждения, подключаемые к сети Интернет, утверждённой Приказом Минобрнауки России и Мининформсязи России от 30 июня 2006 г. N 176/85: <http://mon.gov.ru/pro/pnpo/int/2772/> .

2.3. Составить список используемого программного обеспечения (ПО) в ОУ.

2.4. Ознакомиться с комплектацией лицензионных программных продуктов на сайте Некоммерческого партнёрства поставщиков программных продуктов: <http://www.npppp.ru/complect/spisok/soderzhanie.htm> .

2.5. Проверить комплектацию ПО в ОУ по списку.

2.6. При обнаружении факта использования нелицензионного ПО необходимо прекратить его использование и предпринять действия по закупке необходимых лицензий или по согласованию с методическими центрами (в зависимости от подчинения ОУ) использовать аналогичные программные продукты, распространяемые бесплатно — на основании [Распоряжения Правительства РФ от 17 декабря 2010 г. №2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения ( 2011 – 2015 годы )»](http://government.ru/gov/results/13617/).

**3. Регламентация пользования личными средствами коммуникации**

**(мобильными телефонами и т.п.) и личной компьютерной техникой в ОУ**

3.1. Не допускать использование в ОУ работниками и учащимися личной компьютерной техники (ноутбуков, нетбуков и т.п.), предоставляющей доступ к сети Интернет, без личного согласования с ответственным за информационную безопасность; поручить ответственному за информационную безопасность составить список сотрудников, использующих в связи со служебной необходимостью в ОУ личную компьютерную технику, предоставляющую доступ к сети Интернет.

**4. Мероприятия с учащимися по основам культуры работы и информационной безопасности в сети Интернет**

4.1. Рекомендовать учителю информатики составить и реализовать на учебных занятиях и во внеклассной работе План повышения уровня безопасности детей в сети Интернет при помощи технических и технологических средств.

4.2. Поручить ответственному за информационную безопасность совместно с классными руководителями организовать проведение классных часов по тематике, раскрывающей правила безопасного поведения детей в сети Интернет

4.3. В рамках внеклассной работы поручить классным руководителям организовать проведение тематических семинаров обучающихся по обмену информацией об интересных и полезных ресурсах сети Интернет.

4.4. Поручить ответственному за информационную безопасность регулярно публиковать результаты вышеуказанной работы на официальном сайте ОУ.

4.5. Поручить ответственному за информационную безопасность составить памятку или информационную страницу по вопросам культуры работы и информационной безопасности обучающихся в сети Интернет и разместить её на официальном сайте ОУ.

4.6. По возможности организовать полиграфическое издание и распространение информационных буклетов по проблеме безопасности детей в Интернете с приложением каталога сайтов, интересных и полезных для учащихся.

**5. Мероприятия с родителями по основам информационной безопасности**

**детей в сети Интернет**

5.1. С периодичностью не реже 1 раз в учебный год необходимо проводить общешкольное и/или классные тематические родительские собрания, посвящённые вопросам информационной безопасности детей в сети Интернет (по возможности с участием специалистов в области компьютерной коммуникации).

5.2. Рекомендовать классным руководителям проводить в рамках родительских собраний семинары по обмену опытом обеспечения безопасности ребенка в информационном обществе.

**6. Об использовании в ОУ доступа к сети Интернет, предоставляемого**

**сторонним провайдером**

6.1. По возможности отказаться от использования в ОУ доступа к сети Интернет, предоставляемого сторонним провайдером, в контракте с которым не предусмотрена организация безопасного трафика.

6.2. Установить личную ответственность директора за возможные нежелательные последствия использования в ОУ доступа к сети Интернет, предоставляемого сторонним провайдером, в контракте с которым не предусмотрена организация безопасного трафика.

**7. Мероприятия по защите персональных данных**

7.1. Приказом директора утвердить Положение о порядке обработки персональных данных в образовательном учреждении; назначить сотрудника, ответственного за защиту персональных данных в ОУ; определить перечень лиц, допущенных к обработке персональных данных; ознакомить с вышеуказанным Положением лиц, допущенных к обработке персональных данных, с подписанием ими обязательства о неразглашении информации, содержащей персональные данные **.**

7.2.Поручить ответственному за информационную безопасность взять на особый контроль порядок размещения персональных данных на официальном сайте ОУ и передачи их посредством сети Интернет.

**8. Мероприятия по осуществлению контроля за использованием**

**ресурсов сети Интернет в ОУ**

8.1. С периодичностью не реже 1 раза в полугодие заслушивать лиц, ответственных за использование РСИ, с публичным отчётом на заседаниях педагогического совета ОУ по вопросам:

 - выявления случаев нарушения безопасности использования РСИ с анализом причин, предпринятых мер и их результатов;

 - технической исправности компьютерной техники и аксессуаров;

 - состояния воспитательной работы по формированию пользовательской культуры работы обучающихся в сети Интернет.

**Список нормативно-правовых актов и материалов,**

**на которых основываются положения Инструкции**

1. Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания. — М.: ООО «МегаВерсия», 2006.

2. Письмо Руководителя Федерального агентства по образованию № 15-51-46 ин/01-10.

3. Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки РФ (№ АФ-12/07 (вн) от 11.05.2011г.).

4. Распоряжение Правительства РФ от 17 декабря 2010 г. №2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011 – 2015 годы )».

5. Федеральный закон РФ от 26.07.2006 № 152-ФЗ «О персональных данных».