ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОГО ДОСТУПА ОБУЧАЮЩИХСЯ К РЕСУРСАМ СЕТИ ИНТЕРНЕТ И ОПРЕДЕЛЕНИЮ МЕТОДОВ КОНТРОЛЯ ПРОЦЕССА РАБОТЫ В СЕТИ ИНТЕРНЕТ

Пояснительная записка

В настоящей инструкции рассматриваются наиболее значимые направления организации безопасного использования ресурсов сети Интернет (РСИ) в образовательных учреждениях (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 обучающихся ОУ.

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

Все административные предписания снабжены приложениями, в них приведены примеры типовых локальных актов (приказы директора) и относящихся к ним текстов соответствующих положений и инструкций, которые легко могут быть адаптированы к условиям конкретного ОУ. Особо отмечены те случаи, в которых локальные акты рекомендуется основывать на решениях общественного или педагогического совета ОУ.

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 .
1.4. Уведомить Департамент образования города Москвы об установке СКФ в ОУ с указанием количества подключённых устройств, наименования и количества СКФ, используемых в ОУ.
1.5. Рекомендовать педагогическому совету ОУ обсудить и по итогам обсуждения принять Правила использования сети Интернет в ОУ, Положение об Общественном совете ОУ по вопросам регламентации доступа к информации в сети Интернет и Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, рекомендуемый для применения в образовательном учреждении, которые затем совместно с составом Общественного совета ОУ, Инструкцией для сотрудников ОУ по вопросам регламентации доступа к информации в сети Интернет, Должностной инструкцией ответственного за работу «точки доступа к Интернету» в ОУ утвердить приказом директора (**Приложение №1, с. 1 - 8**) .
1.6. Рекомендовать Общественному совету ОУ по вопросам регламентации доступа к информации в сети Интернет обсудить и по итогам обсуждения принять Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, рекомендуемый для применения в образовательном учреждении, который затем утвердить приказом директора (**Приложение №1, с. 9 - 12**).

2. Мероприятия по антивирусной защите компьютерной техники в ОУ

2.1. Приказом директора ОУ утвердить Инструкцию по организации антивирусной защиты компьютерной техники в ОУ; назначить

ответственного за антивирусную защиту компьютерной техники ОУ (**Приложение №2**).

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 Мининформсвязи 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)».

3. Регламентация пользования личными средствами коммуникации (мобильными телефонами и т.п.) и личной компьютерной техникой в ОУ

3.1. Рекомендовать педагогическому совету ОУ обсудить и по итогам обсуждения принять Положение о регламенте пользования личными средствами коммуникации (мобильными телефонами и т.п.) в ОУ (**Приложение №3**).

3.2. Приказом директора утвердить вышеуказанное Положение.

3.3. Ознакомить с Положением всех работников ОУ и через классных руководителей всех обучающихся и их родителей (законных представителей).

3.4. Не допускать использование в ОУ работниками и обучающимися 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. Регламентация работы в локальной информационной сети ОУ, исключение возможности распространять через неё недоброкачественную информацию, полученную из сети Интернет

4.1. Приказом директора утвердить Положение о локальной информационной сети образовательного учреждения; назначить системного администратора локальной информационной сети ОУ (**Приложение №4**).

5. Мероприятия с обучающимися по основам культуры работы и информационной безопасности в сети Интернет

5.1. Рекомендовать методическому объединению учителей информатики (при отсутствии такового — учителям 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.
5.2. Поручить ответственному за информационную безопасность совместно с заместителем директора по воспитательной работе организовать проведение классных часов по тематике, раскрывающей правила безопасного поведения детей в сети Интернет (в качестве примера — уроки безопасного Интернета, разработанные Фондом развития Интернета совместно с МГУ им. М.В. Ломоносова при поддержке МТС: http//www.detionline.com/mts/lessons)
5.3. В рамках внеклассной работы поручить классным руководителям организовать проведение тематических семинаров обучающихся по обмену информацией об интересных и полезных ресурсах сети Интернет.
5.4. Поручить заместителю директора по воспитательной работе по итогам проведения тематических семинаров обучающихся организовать

- составление и ведение школьного каталога «Мой интересный Интернет» (примером может служить материал выпусков каталога «Образовательные ресурсы сети Интернет» Федерального агентства по образованию Министерства образования и науки РФ: http://catalog.iot.ru/index.php),
- проведение конкурсов на наиболее интересную и многостороннюю подборку веб-ссылок на полезные сайты сети Интернет.

5.5. Поручить ответственному за информационную безопасность и заместителю директора по воспитательной работе регулярно публиковать результаты вышеуказанной работы на официальном сайте ОУ.
5.6. Поручить ответственному за информационную безопасность совместно с заместителем директора по воспитательной работе составить памятку или информационную страницу по вопросам культуры работы и информационной безопасности обучающихся в сети Интернет и разместить её на официальном сайте ОУ.

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

6. Мероприятия с родителями по основам информационной безопасности детей в сети Интернет

6.1. 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).
6.2. Рекомендовать классным руководителям проводить в рамках родительских собраний семинары по обмену опытом обеспечения безопасности ребенка в информационном обществе.

7. Об использовании в ОУ доступа к сети Интернет, предоставляемого сторонним провайдером

7.1. По возможности отказаться от использования в ОУ доступа к сети Интернет, предоставляемого сторонним провайдером, в контракте с которым не предусмотрена организация безопасного трафика.
7.2. 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.

8. Мероприятия по защите персональных данных

8.1. 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 (**Приложение №5**).
8.2. Поручить ответственному за информационную безопасность взять на особый контроль порядок размещения персональных данных на официальном сайте ОУ и передачи их посредством сети Интернет.

9. Мероприятия по осуществлению контроля за использованием ресурсов сети Интернет в ОУ

9.1. 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».