**ПРОГРАММА**

**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**МОУ СОШ с. Сара**

**Пояснительная записка**

В настоящей программе 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. Программа 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. Исполнение программы 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. 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.

1.5. 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.

**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 .

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. Проверить комплектацию ПО в ОУ по списку.

2.5. 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.

**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 .

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

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

5.1. Рекомендовать 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 .

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 основывается программа**

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.

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».

|  |  |
| --- | --- |
| **СОГЛАСОВАНО**Председатель профкома\_\_\_\_\_\_\_\_\_\_\_\_Фролова Ю.Я.«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г. | **УТВЕРЖДАЮ**Директор школы с.Сара\_\_\_\_\_\_\_\_\_\_\_\_\_Е.В. Щукина«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г. |

**Инструкция по организации антивирусной защиты компьютерной техники в ОУ**

**1. Общие положения**

1.1. В ОУ используется только лицензионное антивирусное программное обеспечение.

1.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

1.3. Файлы, помещаемые в электронный архив, в обязательном порядке должны подвергаться антивирусному контролю.

1.4. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вирусов.

1.5. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, ответственного за антивирусную защиту.

**2. Требования к проведению мероприятий по антивирусной защите**

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов локальной сети — при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

2.2. Периодические проверки электронных архивов проводятся не реже одного раза в неделю.

2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера выполняется:

• непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети); выполняется антивирусная проверка на серверах и персональных компьютерах образовательного учреждения. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего;

• при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

2.4. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов пользователи обязаны:

• приостановить работу;

• немедленно поставить в известность о факте обнаружения заражённых вирусом файлов ответственного за обеспечение информационной безопасности в учреждении;

• совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;

• провести лечение или уничтожение заражённых файлов;

• в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту направляет заражённый вирусом файл на гибком магнитном диске в организацию, с которой заключён договор на антивирусную поддержку для дальнейшего исследования.

**3. Ответственность**

3.1. Ответственность за организацию антивирусной защиты возлагается на ответственного за антивирусную защиту компьютерной техники, назначенного приказом директора ОУ.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящего Положения возлагается на ответственного за антивирусную защиту компьютерной техники

3.3. Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется директором.

|  |  |
| --- | --- |
| **СОГЛАСОВАНО**Председатель профкома\_\_\_\_\_\_\_\_\_\_\_\_Фролова Ю.Я.«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г. | **УТВЕРЖДАЮ**Директор школы с.Сара\_\_\_\_\_\_\_\_\_\_\_\_\_Е.В. Щукина«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г. |

**Положение**

**о регламенте пользования личными средствами коммуникации (мобильными телефонами и т.п.) в ОУ**

**1. Общие положения**

1.1. Настоящее Положение устанавливается для обучающихся, работников ОУ и призвано способствовать улучшению организации режима работы, защите личного достоинства и гражданских прав субъектов образовательного процесса.

1.2. Соблюдение правил Положения содействует повышению качества и эффективности учебно-воспитательного процесса, способствует созданию психологически благоприятных условий проведения уроков и учебных занятий, обеспечивает защиту образовательного пространства от попыток пропаганды культа насилия, жестокости и порнографии.

**2. Основные понятия**

Личное средство коммуникации ***(далее ЛСК)*** — личное беспроводное мобильное средство сотовой связи, основным предназначением которого является вербальная (речевая) коммуникация: мобильный телефон, смартфон, iPod и т.п. К ЛСК не относятся ноутбук, нетбук, планшетный компьютер, игровая приставка и т.д., т. к. имеют другие основные предназначения. Пользователь — работник ОУ и обучающийся, пользующиеся ЛСК. Пропаганда культа насилия, жестокости и порнографии посредством ЛСК — демонстрация окружающим видео- и фотосюжетов соответствующего содержания (в нарушение Закона «Об особых правилах распространения эротической продукции и запрете пропаганды культа насилия и жестокости»). Сознательное нанесение вреда имиджу ОУ посредством ЛСК — съёмка на ЛСК в стенах ОУ срежиссированных (постановочных) сцен насилия, вандализма с целью дальнейшей демонстрации сюжетов окружающим.

**3. Цели использования ЛСК в ОУ**

3.1. Цели использования ЛСК — установление и поддержания связи с абонентами сотовой сети в случае возникновения служебной необходимости у работников ОУ или в экстренных случаях у обучающихся и работников ОУ.

3.2. Нецелесообразным следует считать использование в ОУ не указанных выше возможностей ЛСК и сервисов, предоставляемых операторами мобильной связи: доступ к сети Интернет, видео- и фотосъёмка, видеопросмотр, игра, аудиозапись.

**4. Условия использования ЛСК в ОУ**

4.1. Каждый Пользователь обязан знать и соблюдать следующие условия и правила использования ЛСК в ОУ: - в здании ОУ необходимо переводить ЛСК в беззвучный режим вызова (виброзвонок); - во время проведения уроков и учебных занятий обучающимся и учителям необходимо отключать ЛСК, а обучающимся убирать ЛСК в портфели или в карманы одежды; - прослушивание во время перемен радио и музыки посредством ЛСК допускается только в наушниках; - ответственность за сохранность ЛСК несёт только его владелец (родители, законные представители владельца). Все случаи хищения имущества рассматриваются по заявлению и преследуются в соответствии с законодательством РФ.

4.2. Пользователям не рекомендуется нецелесообразное (см. п. 3.2.) использование ЛСК в ОУ.

4.3. Пользователям категорически запрещается:

- использовать ЛСК во время проведения уроков и учебных занятий в любом режиме (в том числе как калькулятор, записную книжку);

- на территории ОУ использовать ЛСК для доступа к сети Интернет;

- демонстрировать жестокость, насилие, порнографию посредством ЛСК;

- сознательно наносить вред имиджу ОУ посредством ЛСК.

**5. Ответственность за нарушение Положения**

5.1. За однократное нарушение Пользователем Положения, оформленное докладной запиской на имя директора ОУ, объявляется замечание, требующее объяснение поведения нарушителя в объяснительной записке.

5.2. При повторных фактах нарушения Положения со стороны работника ОУ директором может быть наложено административное взыскание в виде выговора или, в зависимости от характера нарушения, осуществлено привлечение к ответственности через правоохранительные органы в порядке, предусмотренном законодательством РФ.

5.3. При повторных фактах нарушения Положения со стороны обучающегося проводится собеседование администрации ОУ с родителями обучающегося (законными представителями) с целью полного запрета ношения обучающимся ЛСК в ОУ.

|  |  |
| --- | --- |
| **СОГЛАСОВАНО**Председатель профкома\_\_\_\_\_\_\_\_\_\_\_\_Фролова Ю.Я.«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г. | **УТВЕРЖДАЮ**Директор школы с.Сара\_\_\_\_\_\_\_\_\_\_\_\_\_Е.В. Щукина«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г. |

**Правила**

**использования сети Интернет в общеобразовательном учреждении**

**1. Обязанности обучающегося – пользователя сети Интернет**

1.1. Обучающийся обязан подчиняться лицу, уполномоченному контролировать использование сети Интернет.

1.2. Соблюдать тишину, порядок и чистоту в «точке доступа к Интернету», а также выполнять указания ответственного за «точку доступа к Интернету» по первому требованию.

1.3. Посещать Интернет-ресурсы только образовательной направленности.

1.4. Сообщить ответственному лицу о случайном попадании на ресурс, явно не соответствующий образовательной направленности и/или нарушающий законодательство РФ с указанием Интернет-адреса ресурса (URL), затем немедленно покинуть ресурс.

**2. Учащемуся – пользователю сети Интернет в ОУ запрещается:**

2.1. Посещать сайты, содержащие необразовательную (порнографическую и антигосударственную информацию, информацию со сценами насилия и т. п.), участвовать в нетематических чатах, форумах, конференциях, общаться в любых социальных сетях.

2.2. Распространять, пересылать и записывать хакерскую, коммерческую, рекламную, непристойную, клеветническую, антигосударственную, угрожающую информацию, а также информацию, порочащую честь и достоинство граждан.

2.3. Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое;

2.4. Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, картинку рабочего стола, стартовую страницу браузера).

2.5. Включать, выключать и перезагружать компьютер без согласования с ответственным за «точку доступа к Интернету».

2.6. Осуществлять действия, направленные на «взлом» любых компьютеров, находящихся как в «точке доступа к Интернету» ОУ, так и за его пределами.

**3. Права учащегося – пользователя сети Интернет**

3.1. Пользователи «точки доступа к Интернету» в ОУ имеют право работать в сети Интернет в течение одного часа, если ответственный за использование Интернет не определит иначе. При необходимости время работы может быть увеличено по согласованию с ответственным за «точку доступа к Интернету» и при отсутствии иных лиц, желающих воспользоваться доступом к Интернет-ресурсам.

3.2. Получить учетную запись электронной почты на самостоятельно выбранном Интернет-ресурсе. Ответственный за использование Интернет проверяет содержание входящей и исходящей почты на соответствие п. 2.2. Регламента;

3.3. Сохранять полученную информацию на съемном диске (дискете, CDROM, флеш-накопителе). Съемные диски должны предварительно проверяться на наличие вирусов. При необходимости пользователь может напечатать полученную информацию на принтере, оплатив стоимость использованных при этом расходных материалов и бумаги.

**4. Ответственность пользователя «точки доступа к Интернету»**

4.1. Пользователь «точки доступа к Интернету» в ОУ несет ответственность за содержание передаваемой, принимаемой и распечатываемой информации.

4.2. Лица, не соблюдающие настоящий регламент работ, лишаются права работы в «точке доступа к Интернету».

4.3. При нанесении любого ущерба «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

 **УТВЕРЖДАЮ**

Директор школы с.Сара

\_\_\_\_\_\_\_\_\_\_\_\_\_Е.В. Щукина

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.

**План мероприятий по кибербезопасности на 2014 г.**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование мероприятия | Дата проведения | Ответственные  |
| 1 | Классные часы о существующих киберугрозах и методах борьбы с ними | 03.02.201410.03.201414.03.2014.19.05.2014.15.09.201413.10.201417.11.201422.12.2014 | Кл. рук. |
| 2 | Акция в летнем оздоровительном лагере «Что я знаю о киберугрозах» | 16.06.2014 | Зам.дир. по ВР |
| 3 | Обновление «Уголка информационной безопасности» | 08.09.2014 | Зам.дир. по ВР |
| 4 | Участие в районном конкурсе сочинений, рисунков, поделок по теме «Безопасный Интернет» | 10.11.2014 | Кл.рук., учитель информатики |
| 5 | Общешкольное родительское собрание «Киберугрозы и методы борьбы с ними» | 13.10.2014 | Зам.дир. по ВР |
| 6 | Доводить информацию по вопросам кибербезопасности, видов Интернет и телефонного мошеничества при обучении в рамках проекта «Тимуровцы информационного общества» | 16.05.2014 | Учитель информатики |
| 7 | Размещать актуальную информацию о существующих киберугрозах и методах борьбы сними на официальном сайте школы sara61.okis.ru | 14.03.2014 | Учитель информатики |