

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

На основании инструкции по обеспечению безопасного доступа обучающихся к ресурсам сети Интернет и определению методов контроля процесса работы в сети Интернет

Приказываю:

Провести:

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>). – **ответственная Быкова О.С.**

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.). – **ответственная Быкова О.С.**

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>). – **ответственная Быкова О.С.**

1.4. Уведомить Комитет по образованию Администрации Усть-Пристанского района об установке СКФ в ОУ с указанием количества подключённых устройств, наименования и количества СКФ, используемых в ОУ. – **ответственная Быкова О.С.**

1.5. Рекомендовать педагогическому совету ОУ повторно обсудить Правила использования сети Интернет в ОУ, Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, рекомендуемый для применения в образовательном учреждении, Инструкцией для сотрудников ОУ по вопросам регламентации доступа к информации в сети Интернет. Должностной инструкцией ответственного за работу «точки доступа к Интернету» в ОУ.

2. Мероприятия по антивирусной защите компьютерной техники в ОУ

2.1. Утвердить Инструкцию по организации антивирусной защиты компьютерной техники в ОУ; назначить ответственного за антивирусную защиту компьютерной техники ОУ – **ответственная Быкова О.С.**

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/> - **ответственная Быкова О.С.**

2.3. Составить список используемого программного обеспечения (ПО) в ОУ.-
ответственная Быкова О.С.

2.4. Проверить комплектацию ПО в ОУ по списку – **ответственная Быкова О.С.**

2.5. При обнаружении факта использования нелегального 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)» - **ответственная Быкова О.С.**

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 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.

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

5.1. Рекомендовать методическому объединению учителей математики и 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.- **ответственные Наумкина Е.И. Быкова О.С.**

5.2. Поручить ответственному за информационную безопасность совместно с классными руководителями организовать проведение классных часов по тематике, раскрывающей правила безопасного поведения детей в сети Интернет – **ответственная Быкова О.С.**

5.3. В рамках внеклассной работы поручить классным руководителям организовать проведение тематических семинаров обучающихся по обмену информацией об интересных и полезных ресурсах сети Интернет – **ответственные классные руководители.**

5.4. 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. – **ответственная Быкова О.С.**

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).- **ответственные классные руководители, Быкова О.С.**

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

7. Мероприятия по защите персональных данных

7.1. 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 – **Пенц С.В., Быкова О.С.**

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 отчетом 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.

Директор школы: *И.А.Петрова* И.А.Петрова

Ознакомлены: *О.С.Быкова* О.С.Быкова

С.В.Пенц С.В.Пенц

Е.И.Наумкина Е.И.Наумкина

**ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОГО ДОСТУПА
ОБУЧАЮЩИХСЯ К РЕСУРСАМ СЕТИ ИНТЕРНЕТ И ОПРЕДЕЛЕНИЮ
МЕТОДОВ КОНТРОЛЯ РАБОТЫ В СЕТИ ИНТЕРНЕТ
в филиале МКОУ «Красноярская СОШ»- «Усть-Журавлихинская
ООШ»**

На основании инструкции по обеспечению безопасного доступа обучающихся к ресурсам сети Интернет и определению методов контроля процесса работы в сети Интернет

Приказываю:

Провести:

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>). – **ответственный Баева О.С.**

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.) – **ответственный Баева О.С.**

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>). – **ответственный Баева О.С.**

1.4. Уведомить Комитет по образованию Администрации Усть-Пристанского района об установке СКФ в ОУ с указанием количества подключённых устройств, наименования и количества СКФ, используемых в ОУ.- **ответственный Баева О.С.**

1.5. Рекомендовать педагогическому совету ОУ повторнообсудить Правила использования сети Интернет в ОУ, Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, рекомендуемый для применения в образовательном учреждении, Инструкцией для сотрудников ОУ по вопросам регламентации доступа к информации в сети Интернет, Должностной инструкцией ответственного за работу «точки доступа к Интернету» в ОУ.

2. Мероприятия по антивирусной защите компьютерной техники в ОУ

2.1. Утвердить Инструкцию по организации антивирусной защиты компьютерной техники в ОУ; назначить ответственного за антивирусную защиту компьютерной техники ОУ – **ответственный Баева О.С.**

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/pnpou/int/2772/> -ответственный **Баева О.С.**

2.3. Составить список используемого программного обеспечения (ПО) в ОУ.-
ответственный Казаков С.А.

2.4. Проверить комплектацию ПО в ОУ по списку – **ответственный Баева О.С.**

2.5. При обнаружении факта использования нелегального 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)» - **ответственный Баева О.С.**

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 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.

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

5.1. Рекомендовать методическому объединению учителей математики и 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.- **ответственные Терре Т.Г., Баева О.С.**

5.2. Поручить ответственному за информационную безопасность совместно с классными руководителями организовать проведение классных часов по тематике, раскрывающей правила безопасного поведения детей в сети Интернет– **ответственный Баева О.С.**

5.3. В рамках внеклассной работы поручить классным руководителям организовать проведение тематических семинаров обучающихся по обмену информацией об интересных и полезных ресурсах сети Интернет – **ответственные классные руководители.**

5.4. 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 сайте филиала ОУ. – **ответственный Баева О.С.**

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).- **ответственные классные руководители, Баева О.С.**

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

7. Мероприятия по защите персональных данных

7.1. 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 – **Терре Т.Г., Баева О.С.**

7.2. Поручить ответственному за информационную безопасность взять на особый контроль порядок размещения персональных данных на сайте филиала 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.

Директор школы:  И.А.Петрова

Ознакомлены:

 О.С.Баева

 Т.Г.Терре