Приложение № 1
к приказу МБОУ ООШ № 9
от 21.06.2015 № 55

Должностная инструкция
лица, ответственного за использование преподавателями и обучающимися доступа к образовательным ресурсам сети Интернет

I. Общие положения

1.1. Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам (ответственный за использование преподавателями и обучающимися доступа к образовательным ресурсам сети Интернет) назначается на должность и освобождается от должности руководителем общеобразовательного учреждения.

1.2. Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам подчиняется непосредственно руководителю или заместителю руководителя, курирующего вопросы информатизации образования.

1.3. Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам руководствуется в своей деятельности Конституцией и законами РФ, государственными нормативными актами органов управления образования всех уровней; Правилами и нормами охраны труда, техники безопасности и противопожарной защиты; Уставом и локальными правовыми актами общеобразовательного учреждения, а также настоящей должностной инструкцией.

II. Основные задачи и обязанности

Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам в общеобразовательном учреждении обеспечивает доступ сотрудников школы и учащихся к Интернету, а именно:

- ✓ планирует использование ресурсов сети Интернет в образовательном учреждении на основании заявок преподавателей и других работников образовательного учреждения;
- ✓ систематически повышает свою профессиональную квалификацию, общепедагогическую предметную компетентность, включая ИКТ-компетентность, компетентность в использовании возможностей Интернета в учебном процессе;
- ✓ следит за состоянием компьютерной техники и Интернет-канала точки доступа к Интернету;
- ✓ находится в помещении точки доступа к Интернету на протяжении всего времени ее работы;
- ✓ ведет учет пользователей точки доступа к Интернету, в случае необходимости лимитирует время работы пользователя в Интернете;
- ✓ оказывает помощь пользователям точки доступа к Интернету во время сеансов работы в Сети;
- ✓ участвует в организации повышения квалификации сотрудников школы по использованию Интернета в профессиональной деятельности;
- ✓ осуществляет регулярное обновление антивирусного программного обеспечения, контролирует проверку пользователями внешних электронных носителей информации (дискет, CD-ROM, флеш-накопителей) на отсутствие вирусов;
- ✓ принимает участие в создании (и актуализации) школьного сайта.

III. Права

Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам в общеобразовательном учреждении имеет право:

✓ определять ресурсы сети Интернет, используемые обучающимися в учебном процессе на основе запросов преподавателей;

✓ участвовать в административных совещаниях при обсуждении вопросов, связанных с использованием Интернета в образовательном процессе и управлении школой;

✓ отдавать распоряжения пользователям точки доступа к Интернету в рамках своей компетенции;

✓ информировать руководителя общеобразовательного учреждения о нарушении пользователями точки доступа к Интернету правил техники безопасности, противопожарной безопасности, поведения, регламента работы в Интернете.

VI. Ответственность

Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет-ресурсам в общеобразовательном учреждении несет полную ответственность за:

✓ надлежащее и своевременное выполнение обязанностей, возложенных на него настоящей должностной инструкцией;

✓ соблюдение Правил техники безопасности, противопожарной безопасности и норм охраны труда в школе;

✓ состояние делопроизводства по вверенному ему направлению работы.

Приложение № 2
к приказу МБОУ ООШ № 9
от 21.06.2015 № 55

**Должностные обязанности лица,
ответственного за работу точки доступа к сети Интернет**

I. Общие положения

1.1. Ответственный за работу точки доступа к Интернету назначается приказом руководителя образовательного учреждения.

1.2. Непосредственным руководителем ответственного за работу точки доступа к Интернету является заместитель руководителя.

1.3. Ответственный за работу точки доступа к Интернету в своей деятельности руководствуется:

- ✓ Конституцией Российской Федерации;
- ✓ Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации";
- ✓ Федеральным законом от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию";
- ✓ Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных";
- ✓ иными нормативными правовыми актами, действующими на территории РФ;
- ✓ правилами по охране труда и пожарной безопасности;
- ✓ уставом и локальными нормативными актами ОУ;
- ✓ настоящими должностными обязанностями.

II. Должностные обязанности

Ответственный за работу точки доступа к Интернету обеспечивает доступ работников и учащихся образовательного учреждения к Интернету, а именно:

- ✓ следит за состоянием компьютерной техники и Интернет-канала точки доступа к Интернету. В случае необходимости инициирует обращение в ремонтную организацию или поставщику Интернет-услуг. Контролирует проведение ремонтных работ;
- ✓ ведет учет пользователей точки доступа к Интернету. В случае необходимости лимитирует время работы пользователя в Интернете;
- ✓ оказывает помощь пользователям точки доступа к Интернету во время сеансов работы в Сети;
- ✓ участвует в организации повышения квалификации работников образовательного учреждения по использованию Интернета в профессиональной деятельности;
- ✓ организует оформление стендов наглядными материалами по тематике Интернета (советами по работе с программным обеспечением (браузером, электронной почтой), обзором интересных Интернет-ресурсов, новостями педагогического Интернет-сообщества и т.п.);
- ✓ осуществляет регулярное обновление антивирусного программного обеспечения;
- ✓ контролирует проверку пользователями внешних электронных носителей информации (дискет, CD-ROM, флеш-накопителей) на отсутствие вирусов;
- ✓ принимает участие в создании и актуализации сайта образовательного учреждения;
- ✓ сообщает своему непосредственному руководителю либо руководителю образовательного учреждения о фактах нарушения пользователями точки доступа к Интернету правил техники безопасности, пожарной безопасности, использования Интернета, а также правил внутреннего трудового распорядка образовательного учреждения.

III. Права

Ответственный за работу точки доступа к Интернету имеет право:

- ✓ получать от администрации образовательного учреждения информацию, необходимую для осуществления своей деятельности;
- ✓ участвовать в административных совещаниях при обсуждении вопросов, связанных с использованием Интернета в образовательном процессе и управлении образовательным учреждением;
- ✓ представлять на рассмотрение руководителя образовательного учреждения предложения по вопросам своей деятельности;
- ✓ отдавать распоряжения пользователям точки доступа к Интернету в рамках своей компетенции;
- ✓ повышать свою квалификацию.

IV. Ответственность

Ответственный за работу точки доступа к Интернету несет ответственность за:

- ✓ надлежащее и своевременное исполнение обязанностей, возложенных на него настоящими должностными обязанностями;
- ✓ соблюдение правил техники безопасности, пожарной безопасности и использования Интернета в образовательном учреждении;
- ✓ состояние делопроизводства по вверенному ему направлению работы.

Приложение № 3
к приказу МБОУ ООШ № 9
от 21.06.2015 № 55

Инструкция
по организации антивирусной защиты средств информатизации

I. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты средств информатизации от разрушающего воздействия компьютерных вирусов, порядок организации работ по антивирусной защите средств информатизации в образовательном учреждении (далее – ОУ), устанавливает ответственность пользователей и должностных лиц ОУ по антивирусной защите средств информатизации.

1.2.Руководитель УО назначает лицо, ответственное за организацию антивирусной защиты средств информатизации. В противном случае вся ответственность за обеспечение антивирусной защиты средств информатизации ложится на руководителя образовательного учреждения.

1.3. К использованию в ОУ допускается только лицензионное антивирусное программное обеспечение в соответствии с требованиями действующего законодательства Российской Федерации (Norton Antivirus, Dr. Web, Kaspersky Antivirus, NOD 32 и т.п.).

1.4. При наличии в ОУ локальной компьютерной сети и сервера рекомендуется использовать версию антивирусного программного обеспечения, позволяющую организовать централизованное управление: установка, настройка, обновление антивирусных баз, антивирусное сканирование и сбор отчетов на всех компьютерах должны осуществляться удаленно на сервере учреждения (Kaspersky Work Space Security, Symantec Antivirus Corporate Edition, Symantec Endpoint Protection и т.п.)

1.5. Требования инструкции являются обязательными для всех работников ОУ, имеющих доступ к информационным ресурсам.

II. Требования к проведению мероприятий по антивирусной защите средств информатизации

2.1. Обязательному антивирусному контролю подлежит:

- ✓ любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам;
- ✓ информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.);
- ✓ входящая и исходящая информация (перед записью на носители информации, архивированием и отправкой);
- ✓ файлы, помещаемые в электронный архив;
- ✓ устанавливаемое (изменяемое) программное обеспечение.

2.2. Ежедневно в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

2.3. Модуль антивирусной защиты должен загружаться автоматически при загрузке компьютера. Закрытие модуля или остановка его работы на всех компьютерах должна быть отключена или закрыта паролем.

2.4. Периодические антивирусные проверки всех компьютеров образовательного учреждения должны проводиться не реже одного раза в неделю.

2.5. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться 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.).

III. Профилактика заражения

3.1. Одним из основных методов борьбы с вирусами является своевременная профилактика, состоящая из соблюдения следующих правил:

3.1.1. Защитить компьютер с помощью антивирусных программ и программ безопасной работы в Интернете. Для этого:

- ✓ Установить антивирусную программу.
- ✓ Обновлять регулярно сигнатуры угроз, входящие в состав программы.
- ✓ Не выгружать из памяти и не останавливать работу антивирусной программы.

3.1.2. Проявлять осторожность при записи новых данных на компьютер:

- ✓ Проверить на присутствие вирусов все съемные диски (дискеты, CD-диски, флеш-накопители и пр.) перед их использованием.
- ✓ Не запускать никаких файлов, пришедших по почте, не проверенных с помощью антивирусной программы.
- ✓ Обратить внимание на наличие сертификата безопасности при установлении новой программы с какого-либо веб-сайта.
- ✓ Проверить с помощью антивирусной программы копируемый из Интернета или локальной сети исполняемый файл.

3.1.3. Пользоваться сервисом Windows Update и регулярно устанавливать обновления операционной системы Microsoft Windows.

3.1.4. Создать диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя «чистую» операционную систему.

3.1.5. Просматривать регулярно список установленных программ.

IV. Должностные обязанности пользователей по антивирусной защите средств информатизации

4.1. Не прерывать процесс обновления антивирусных баз и антивирусный контроль всех дисков и файлов персонального компьютера.

4.2. При отправке и получении электронной почты пользователь обязан проверить электронные письма на наличие вирусов.

4.3. При использовании съемных носителей, осуществлять их антивирусную проверку.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

4.4.1. Приостановить работу.

4.4.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в ОУ, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе.

4.4.3. Совместно с лицом, ответственным по антивирусной защите принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

V. Должностные обязанности лица, ответственного за организацию антивирусной защиты средств информатизации

5.1. Лицо, ответственное за организацию антивирусной защиты средств информатизации, обязано:

5.1.1. Устанавливать средства антивирусного контроля на персональных компьютерах и серверах.

5.1.2. Настраивать параметры средств антивирусного контроля на персональных компьютерах и серверах.

5.1.3. Своевременно обновлять антивирусные базы на персональных компьютерах и серверах.

5.1.4. Еженедельно проверять компьютеры на вирусы.

5.1.5. Проводить внеочередную проверку в случае подозрения на наличие вирусов или по просьбе пользователей персональных компьютеров.

5.1.6. Проводить в установленном порядке инструктаж по антивирусной защите пользователей персональных компьютеров.

5.2. В случае обнаружения компьютерного вируса ответственное лицо за антивирусную защиту (или действия при обнаружении вируса):

5.2.1. принимает все необходимые меры для обеспечения сохранности информации;

5.2.2. принимает все необходимые меры по локализации и удалению вируса:

5.2.2.1. отключает компьютер от Интернета и локальной сети, если он к ней был подключен;

5.2.2.2. если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку при подключении), загружается в режиме защиты от сбоев или с диска аварийной загрузки Microsoft Windows, который был создан при установке операционной системы на компьютер;

5.2.2.3. сохраняет результаты работы на внешнем носителе (дискете, CD-диске, флеш-накопителе и пр.);

5.2.2.4. обновляет сигнатуру угроз программы;

5.2.2.5. запускает полную проверку компьютера;

5.2.2.6. проводит лечение или уничтожение зараженных файлов;

5.2.2.7. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, обязан направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования.

5.2.3. уведомляет руководителя ОУ об обнаружении вируса и последствиях его воздействия.

VI. Ответственность

6.1. Ответственность за организацию антивирусной защиты средств информатизации возлагается на руководителя ОУ или лицо им назначенное.

6.2. Ответственность за проведение мероприятий антивирусного контроля в ОУ и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты средств информатизации.

6.3. Периодический контроль за состоянием антивирусной защиты средств информатизации в ОУ осуществляется руководителем.

Приложение № 4
к приказу МБОУ ООШ № 9
от 21.06.2015 № 55

Регламент работы в сети Интернет
(инструкция по организации работы для учителей и обучающихся)

I. Общие положения

Точка доступа к сети Интернет предназначена для обслуживания учителей и учеников школы. Сотрудники и учащиеся школы допускаются к работе на бесплатной основе**.**

К работе в Интернет допускаются пользователи, прошедшие предварительную регистрацию у лица, ответственного за обеспечение работы точки доступа к сети Интернет и внедрение системы контентной фильтрации в школе (далее – ответственное лицо).

Ответственное лицо ведёт журнал регистрации случаев обнаружения Интернет-ресурсов, не совместимых с задачами образования и воспитания учащихся, а также создаёт учетные записи пользователей.

Выход в Интернет осуществляется с 8^{30} до 15^{30} (кроме воскресенья). Предоставление сеанса работы в Интернет осуществляется, как правило, на основании предварительной записи в журнале регистрации работы в Интернет и при наличии свободных мест в зависимости от категории пользователя:

- ✓ учащимся предоставляется доступ в Интернет в компьютерных классах согласно расписанию занятий;
- ✓ учителям предоставляется доступ в Интернет в течение рабочего дня;
- ✓ остальным пользователям предоставляется доступ при наличии резерва пропускной способности канала передачи.

По всем вопросам, связанным с доступом в Интернет, следует обращаться к ответственному лицу.

II. Правила работы

При входе в компьютерный класс, необходимо обратиться к ответственному лицу за разрешением для работы. При наличии свободных мест, после регистрации в журнале учета, посетителю предоставляется в классе рабочая станция. Для доступа в Интернет и использования электронной почты установлен программный продукт "Google Chrome", «Outlook Express». Отправка электронной почты с присоединенной к письму информацией, запись информации на внешние накопители информации и наоборот осуществляется у ответственного лица. Дополнительно установлено программное обеспечение Open Office.

1. Пользователь обязан выполнять все требования ответственного лица.
2. В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации (логин) и пароль. После окончания работы необходимо завершить свой сеанс работы, вызвав в меню «Пуск» команду «Завершение сеанса <имя>» «Выход».
3. За одним рабочим местом должно находиться не более одного пользователя.
4. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль.
5. Каждому пользователю предоставляется возможность хранения личных файлов общим объемом не более 50 Мб, а также возможность работы с почтовым ящиком для отправки и получения электронной почты.

6. Разрешается использовать оборудование только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов. Любое использование оборудования в коммерческих целях запрещено.

7. Пользователю запрещается пользоваться внешними накопителями информации. При необходимости записи информации на внешние накопители либо на жесткий диск рабочей станции пользователь обязан обратиться к ответственному лицу. Внешние накопители информации предварительно проверяются на наличие вирусов.

8. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на сервере.

9. Запрещена передача информации, представляющей коммерческую или государственную тайну, распространение информации, порочащей честь и достоинство граждан.

10. Запрещается работать с объемными ресурсами (video, audio, chat, игры и др.) без согласования с ответственным лицом.

11. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.

12. Пользователь обязан сохранять оборудование в целости и сохранности.

13. Пользователь обязан помнить свой пароль. В случае утраты пароля пользователь обязан сообщить ответственному лицу.

В случае нарушения правил работы пользователь лишается доступа в сеть. За нарушение правил работы пользователь получает первое предупреждение. При повторном нарушении пользователь лишается доступа в Интернет без права восстановления.

При возникновении технических проблем пользователь обязан поставить в известность ответственное лицо.

Приложение № 5
к приказу МБОУ ООШ № 9
от 21.06.2015 № 55

Муниципальное бюджетное общеобразовательное учреждение
«Основная общеобразовательная школа № 9 города Кандалакша Мурманской области»

**Журнал регистрации случаев обнаружения Интернет-ресурсов,
не совместимых с задачами образования и воспитания учащихся**

Начат _____
Окончен _____

Ф.И.О. пользователя	Дата и время работы в Интернете	Цель работы в Интернете	Обнаруженный ресурс	Предпринятые меры	Подпись ответственного лица	Примечание