МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ «ГОРОД АРХАНГЕЛЬСК»
«ГИМНАЗИЯ № 21»

УТВЕРЖДАЮ
ДИРЕКТОР МБОУ ГИМНАЗИЯ № 21
_____ /Т.Н. Боровикова
«__» _____ 2015 года

4/2 от 31.03.2015

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Инструкция по организации антивирусной защиты (далее - Инструкция) разработана в соответствии с Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 29.12.2010 г. № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», письмом Минобразования России от 13 августа 2002 г. № 01-51-088ин «Об организации использования информационных и коммуникационных ресурсов в общеобразовательных учреждениях», письмом Минобразования России от 11 мая 2011 г. № АФ-12/07вн «Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации».

1.2 Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в муниципальном бюджетном общеобразовательном учреждении муниципального образования "Город Архангельск" "Гимназия № 21" (далее по тексту – Гимназия) с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы учреждения и возникновения фактов заражения программного обеспечения (далее по тексту - ПО) гимназии.

1.3 В настоящей Инструкции использованы следующие термины и определения:

- ✓ **Антивирусное ПО** - набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для профилактики - предотвращения заражения файлов или операционной системы вредоносным кодом.
- ✓ **Антивирусные базы** - файлы, используемые антивирусным ПО при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО.
- ✓ **Антивирусный контроль** - проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

- ✓ **Вредоносная программа** - компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационные ресурсы.
- ✓ **Защищаемый компьютер** - электронно-вычислительная машина (персональный компьютер), используемая для обработки данных.
- ✓ **Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
- ✓ **Съемный носитель информации** - носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (съемные винчестеры, флэш- память, CD, DVD, дискеты и др.).

1.4 Требования настоящей Инструкции обязательны для выполнения всеми участниками образовательного процесса гимназии.

2. УСТАНОВКА АНТИВИРУСНОГО ПО

2.1 Директором гимназии назначается лицо, ответственное за антивирусную защиту гимназии.

2.2 В гимназии могут использоваться только лицензионное антивирусное ПО.

2.3 Установка антивирусного ПО производится только лицом (лицами), ответственным за установку, удаление, отладку антивирусного ПО гимназии.

2.4 Установка антивирусного ПО производится индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

2.5 Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.

2.6 Антивирусное ПО запускается автоматически при запуске системы.

3. ПОРЯДОК ОБНОВЛЕНИЯ АНТИВИРУСНЫХ БАЗ

3.1 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети гимназии, должна осуществляться ежедневно в автоматическом режиме.

3.2 Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети гимназии, должно осуществляться с использованием маркированных съемных носителей информации, в обязательном порядке проверяемых антивирусным ПО перед их использованием или принудительным подключением к локальной сети гимназии.

3.3 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети, контролируется пользователем самостоятельно ежедневно и в случае нарушения пользователь должен не принимать никаких мер и срочно сообщить лицу (лицам), ответственному за установку, удаление, отладку антивирусного ПО гимназии.

4. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ АНТИВИРУСНОГО КОНТРОЛЯ

4.1 Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

4.2 Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также данные на съемных носителях информации. Контроль входящей и исходящей информации на защищаемых компьютерах должен осуществляться непрерывно посредством постоянно работающего компонента антивирусного ПО («монитора»).

4.3 Все программное обеспечение, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ.

4.4 Не реже одного раза в четыре недели должна проводиться полная проверка всех файлов, хранящихся на жестких дисках защищаемого компьютера.

4.5 Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера должен выполняться:

- ✓ сразу после установки или изменения ПО;
- ✓ после подключения автономного компьютера к локальной сети;
- ✓ при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4.6 В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь лицо (лица), ответственное за установку, удаление, отладку антивирусного ПО гимназии.

5. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ ПРИ ОБНАРУЖЕНИИ ВРЕДОНОСНЫХ ПРОГРАММ

5.1 В случае обнаружения при проведении антивирусной проверки вредоносных программ пользователи обязаны:

- ✓ приостановить все операции, связанные с обработкой файлов на защищаемом компьютере;
- ✓ немедленно поставить в известность о факте обнаружения вредоносных программ владельцев зараженных или поврежденных вредоносными программами файлов, а также лицо (лица), ответственное за установку, удаление, отладку антивирусного ПО гимназии;
- ✓ совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- ✓ провести лечение зараженных файлов (при необходимости привлечь лицо (лица), ответственное за установку, удаление, отладку антивирусного ПО гимназии);
- ✓ в случае обнаружения не поддающегося лечению вируса, пользователь обязан удалить инфицированный файл в соответствующую папку антивирусного ПО, и проверить работоспособность компьютера (при необходимости привлечь лицо (лица), ответственное за установку, удаление, отладку антивирусного ПО гимназии).

6. ОТВЕТСТВЕННОСТЬ ЗА ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ИНСТРУКЦИИ

6.1 Ответственность за организацию антивирусной защиты информации на компьютерах, эксплуатируемых участниками образовательного процесса, и их ознакомление с Инструкцией несет заместитель директора по ИКТ.

6.2 Ответственность за соблюдение требований Инструкции на своих рабочих местах несут пользователи.

6.3 Периодический контроль за состоянием антивирусной защиты в школе осуществляется лицом (лицами), ответственным за установку, удаление, отладку антивирусного ПО гимназии.

6.4 Ответственность за своевременное обновление антивирусных баз и получение новых лицензионных ключей при истечении их срока действия несет заместитель директора по ИКТ.