УТВЕРЖДЕНА
приказом ЦДТ «Хибины»
от 31.08.2018 № 285

ИНСТРУКЦИЯ
по организации антивирусной защиты средств информатизации в ЦДТ «Хибины»

1. 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 муниципальной автономной организации дополнительного образования детей «Центр детского творчества «Хибины» г. Кировска» (далее ЦДТ «Хибины»), порядок применения средств антивирусной защиты средств информатизации в ЦДТ «Хибины», порядок установки и применения обновлений, подключение средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных продуктов.

1.2. Настоящая инструкция по организации антивирусной защиты средств информатизации разработана на основе Типовой инструкции по организации антивирусной защиты средств информатизации в образовательных учреждениях, утвержденной приказом Комитета по образованию и науке Мурманской области от 01.08.2008 №1333 «Об утверждении Типовой инструкции по организации антивирусной защиты средств информатизации в образовательных учреждениях».

1.3. Руководитель ЦДТ «Хибины» назначает лицо, ответственное за организацию антивирусной защиты средств информатизации. В противном случае вся ответственность за обеспечение антивирусной защиты средств информатизации ложится на руководителя Образовательной организации.

1.4. К использованию в ЦДТ «Хибины» 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.).

1.5. Передача средств антивирусной защиты пользователям на объекты, не входящие в ЦДТ «Хибины», запрещена.

1.6. Требования инструкции являются обязательными для всех работников ЦДТ «Хибины», имеющих доступ к информационным ресурсам.

2. 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.

— Удаленное решение проблем, возникающих в процессе использования средств антивирусной защиты информации;

— Инсталляция и настройка средств антивирусной защиты средств информатизации осуществляется с программой и эксплуатационной документацией, поступающей в

комплекте с ними;

— Копирование любой информации, переносимой с любых съемных носителей средств информатизации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя;

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 ЦДТ «Хибины» должны проводиться не реже одного раза в квартал.

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.).

2.6. 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), необходимо провести внеплановую проверку жестких магнитных дисков и съемных носителей средств информатизации на наличие программных вирусов;

2.7. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов ответственный за антивирусную защиту обязан совместно с пользователями зараженных вирусом файлов определить необходимость дальнейшего их использования и провести лечение или уничтожение зараженных файлов.

3. Профилактика заражения

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

3.2. Защитить компьютер с помощью антивирусных программ и программ безопасной работы в Интернете.

3.3. Для этого:

— установить антивирусную программу;

— обновлять регулярно сигнатуры угроз, входящие в состав программы;

— не выгружать из памяти и не останавливать работу антивирусной программы.

3.4. Проявлять осторожность при записи новых данных на компьютер:

— проверить на присутствие вирусов все съемные диски (дискеты, CD-диски, флеш-карты 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 исполняемый файл.

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

3.6. Обновление баз данных средств антивирусной защиты средств информатизации на рабочих станциях ЦДТ «Хибины» должно осуществляться централизовано через сервер ЦДТ «Хибины» в автоматическом режиме.

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

3.8. Просматривать регулярно список установленных программ.

4. 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:

4.5. Приостановить работу.

4.6. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в ЦДТ «Хибины», владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе.

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

5. Должностные обязанности ответственного лица за организацию антивирусной защиты средств информатизации.

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

- Устанавливать средства антивирусного контроля на всех персональных компьютерах.
- Настраивать параметры средств антивирусного контроля на всех персональных компьютерах.
- Своевременно обновлять антивирусные базы на всех персональных компьютерах.
- Еженедельно проверять компьютеры на вирусы.
- Проводить внеочередную проверку в случае подозрения на наличие вирусов или по просьбе пользователей персональных компьютеров.
- 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):

- принимает все необходимые меры для обеспечения сохранности информации;
- принимает все необходимые меры по локализации и удалению вируса:
- отключает компьютер от Интернета;

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

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

— обновляет сигнатуру угроз программы;

— запускает полную проверку компьютера;

— проводит лечение или уничтожение зараженных файлов;

— 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;

— уведомляет директора ЦДТ «Хибины» об обнаружении вируса и последствиях его воздействия.

6. Ответственность администратора за обеспечение антивирусной защиты средств информатизации

6.1. К задачам администратора средств информатизации относится организация процесса установки и обновления средств антивирусной защиты средств информатизации на рабочих местах пользователей и обеспечение технического сопровождения действий пользователей в случае обнаружения программных вирусов, а также осуществление контроля за состоянием антивирусной защиты.

6.2. За невыполнение или ненадлежащее выполнение поставленных задач администратор защиты средств информатизации несет ответственность за:

- своевременную установку средств антивирусной защиты средств информатизации;
- эксплуатацию системы антивирусной защиты средств информатизации;
- своевременное обновление лицензий на средства антивирусной защиты средств информатизации;
- своевременное обновление баз данных средств антивирусной защиты средств информатизации.
- проведение мероприятий антивирусного контроля в ЦДТ «Хибины» 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 ЦДТ «Хибины» осуществляется заместителем директора ЦДТ «Хибины».

6.4. Ответственность за организацию антивирусной защиты средств информатизации несет директор ЦДТ «Хибины» или лицо им назначенное