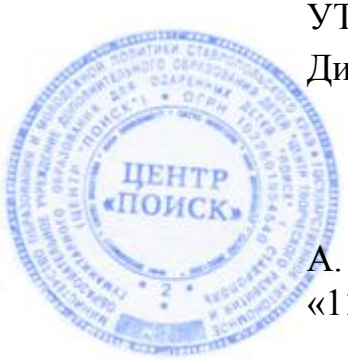
УТВЕРЖДАЮ
Директор Центра



А. В. Жигайлов
«11» января 2016 г.

И Н С Т Р У К Ц И Я

по организации антивирусной защиты автоматизированной системы Государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск»

1. Общие положения

1.1. Инструкция по организации антивирусной защиты автоматизированной системы (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в Государственном автономном образовательном учреждении дополнительного образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск») с целью предотвращения заражения компьютерными вирусами информационных ресурсов Центра.

1.3. Настоящая Инструкция определяет требования к организации защиты автоматизированной системы (далее – АС) Центра «Поиск» от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей, работников, эксплуатирующих автоматизированные рабочие места (далее – АРМ), и сопровождающих АС, за её выполнение.

1.4. Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему АРМ при выполнении работ в АС.

1.5. Техническое обслуживание средств вычислительной техники проводится сотрудниками, ответственными за техническое обслуживание компьютерной техники (далее – уполномоченными сотрудниками).

1.6. Непосредственную ответственность за надлежащее выполнение Инструкции всеми пользователями АС Центра «Поиск» несет директор Центра.

1.7. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности защищаемой информации в Центре «Поиск» и не исключает обязательного выполнения их требований.

1.8. Ознакомление сотрудников с настоящей Инструкцией осуществляется под роспись по форме согласно приложению.

1.9. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Установка антивирусного программного обеспечения

2.1. К использованию в Центре допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

2.2. Установка антивирусного ПО осуществляется уполномоченными сотрудниками Центра в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств» индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

2.3. Настройка параметров средств антивирусного контроля осуществляется уполномоченными сотрудниками Центра в соответствии с руководствами по применению конкретных антивирусных средств.

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

2.5. Ярлык для запуска антивирусного ПО должен быть вынесен на "Рабочий стол" операционной системы или на панель быстрого запуска.

3. Применение средств антивирусного контроля

3.1. Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме.

3.2. 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, лазерных дисках, USB флеш-накопителях, SSD-накопителях и т.п.).

3.3. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема.

3.4. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

3.6. Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

3.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

3.8. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на защищаемых серверах и АРМ уполномоченными сотрудниками Центра.

3.9. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение.

4. Порядок обновления антивирусных баз

4.1. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети Центра, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений.

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

4.3. Проверка критических областей защищаемого компьютера, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

4.4. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети, контролируется пользователем самостоятельно ежедневно. В случае нарушения актуализации пользователь, не предпринимая самостоятельно никаких мер, должен сообщить об этом администратору информационной безопасности или уполномоченному сотруднику Центра.

5. Действия при обнаружении вирусов

5.1. 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.) пользователь или уполномоченный сотрудник должен провести внеочередной антивирусный контроль рабочей станции.

5.2. В случае обнаружения файлов, зараженных компьютерными вирусами, работник Центра обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом ответственного за техническое обслуживание компьютерной техники специалиста Центра, владельца зараженных файлов, а также других работников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов самостоятельно или вместе с уполномоченным сотрудником.

6. Ответственность

6.1. Ответственность за организацию антивирусной защиты АС Центра возлагается на администратора информационной безопасности.

6.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями АС.

6.3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками Центра осуществляется администратором информационной безопасности.

ПРИЛОЖЕНИЕ
к инструкции по организации антивирусной
защиты автоматизированной системы
Центра «Поиск»

ЛИСТ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ

С инструкцией ознакомлен:

№ п/п	Фамилия, имя, отчество работника	Дата	Подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			