УТВЕРЖДЕНО
директором Центра «Поиск»
О. А. Томилиной
приказ № 514
от «28» декабря 2024 г.

И Н С Т Р У К Ц И Я

по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы Государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск»

1. Общие положения

1.1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств 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 05.12.2016 г. № Пр-646.

1.2. Настоящая Инструкция регламентирует организацию мероприятий по обеспечению безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники и при возникновении нештатных ситуаций в работе автоматизированной системы Государственного автономного образовательного учреждения

дополнительного образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск»).

1.3. Непосредственную ответственность за надлежащее выполнение инструкции всеми сотрудниками Центра «Поиск» несет директор Центра.

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

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

2. Основания для изменения конфигурации

2.1. Все изменения конфигурации технических и программных средств рабочих станций и серверов АС Центра «Поиск» должны производиться только на основании решения заместителя директора по ИКТ.

2.2. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций и серверов АС Центра «Поиск» предоставляется только сотрудникам, ответственными за техническое обслуживание компьютерной техники (далее – уполномоченным сотрудникам).

2.3. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме уполномоченных сотрудников, строго запрещено.

2.4. Заключение о технической возможности осуществления затребованных изменений выдается уполномоченным сотрудником или администратором информационной безопасности на основании новых задач и технических возможностей соответствующих рабочих станций или серверов.

2.5. Заключение о возможности совмещения решения новых задач (обработки информации) на указанных рабочих станциях или серверах в соответствии с требованиями по безопасности выдается администратором информационной безопасности. Одновременно с этим производится определение новых категорий защищенности указанных рабочих станций или серверов.

2.6. После принятия решения о возможности осуществления новых задач на рабочих станциях или серверах уполномоченному сотруднику выдается указание от заместителя директора по ИКТ для непосредственного исполнения работ по внесению изменений в конфигурацию.

3. Изменения конфигурации технических и программных средств

3.1. Администратор информационной безопасности допускает уполномоченных сотрудников сторонних организаций к внесению изменений в состав аппаратных средств и программного обеспечения только по предъявлении последними утвержденной заявки на осуществление данных изменений.

3.2. Установка, изменение (обновление) и удаление системных и прикладных программных средств рабочих станций и серверов производится уполномоченными сотрудниками Центра.

3.3. Если рабочая станция или сервер относится к защищаемым рабочим станциям, то установка, снятие и внесение необходимых изменений в настройки средств защиты и средств контроля целостности файлов осуществляется администратором информационной безопасности.

3.4. После проведения модификации программного обеспечения на рабочих станциях уполномоченный сотрудник проводит антивирусный контроль.

3.5. Установка и обновление общего ПО (системного, тестового и т.п.) на рабочие станции и серверы производится с оригинальных лицензионных

дистрибутивных носителей или лицензионных интернет-источников, полученных установленным порядком.

3.6. После установки (обновления) ПО уполномоченный сотрудник должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) и совместно с пользователем должен проверить работоспособность ПО и правильность настройки средств защиты.

3.7. Уполномоченные исполнители работ должны произвести соответствующую запись в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств РС подразделения».

4. Техническое обслуживание и ремонт

4.1. При изъятии рабочей станции из состава рабочих станций учреждения, ее передача на техническое обслуживание, склад, в ремонт осуществляется только после того, как уполномоченный сотрудник предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

4.2. Факт уничтожения защищаемых данных, находившихся на диске компьютера, оформляется актом за подписью администратора информационной безопасности (Приложение 1).

4.3. О факте выполнения данных работ администратор информационной безопасности учреждения делает соответствующую отметку в журнале «Нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств РС подразделения» с указанием признаков проявления ситуации, содержания выполненных работ по ее устранению или о необходимости привлечения к ремонту сотрудников сторонних организаций.

ПРИЛОЖЕНИЕ 1

А К Т

о затирании остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД системного блока с инвентарным №_____, передаваемого с целью _____

_____
(цель передачи)

_____

_____
(куда и / или кому)

уничтожены посредством программы _____.

«___» _____ 20__ г.

Администратор
информационной безопасности _____ _____
(подпись) (фамилия, инициалы)