УТВЕРЖДАЮ
Директор
ГБПОУ РК «РКИГ»
_____ Пальчук М. И.

_____ _____ 202__ г.

Инструкция
о порядке изменения состава и конфигурации технических и программных средств в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ

Настоящей инструкцией регламентируется порядок проведения модификации программного обеспечения и технического обслуживания средств вычислительной техники «Информационная система персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ» (далее - ИСПДн ОИ ФЦТ).

Все изменения в конфигурации технических и программных средств ИСПДн ОИ ФЦТ должны производиться только после их согласования с органом по аттестации, выдавшим «Аттестат соответствия» на ИСПДн ОИ ФЦТ.

В заявке могут указываться следующие виды необходимых изменений в составе технических и программных средств ИСПДн ОИ ФЦТ:

- добавление устройства (узла, блока) в состав ИСПДн ОИ ФЦТ;
- замена устройства (узла, блока) в составе ИСПДн ОИ ФЦТ;
- изъятие устройства (узла, блока) из состава ИСПДн ОИ ФЦТ;
- обновление (замена) программных средств;
- удаление с ИСПДн ОИ ФЦТ программных средств.

Право внесения изменений в конфигурацию технических и программных средств ИСПДн ОИ ФЦТ предоставляется администратору безопасности на основании распоряжения руководителя Учреждения.

Все добавляемые технические и программные средства должны быть предварительно установленным порядком проверены на работоспособность, а также на отсутствие опасных функций.

После установки (обновления) ПО, администратор безопасности должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром и проверить работоспособность ПО и правильность настройки средств защиты.

После завершения работ по внесению изменений в состав аппаратных средств, системный блок должен закрываться администратором безопасности и опечатываться (пломбироваться, защищаться специальной наклейкой).

Внесение изменений в составе технических и программных средств происходит с обязательным документированием, уведомлением каждого сотрудника, кого касается изменение; выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

Ведущий специалист по защите информации А. О. Грибенников