Приложение № 6

Утверждено

приказом государственной

инспекции по охране объектов

культурного наследия

Новосибирской области

от \_\_\_\_\_\_ 2023 г. № \_\_\_\_\_

Инструкция

**о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации,** в информационных системах персональных данных

**1. Общие положения**

**1.1. Настоящая Инструкция о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации,** в информационных системах персональных данных (далее – Инструкция) **определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных системах персональных данных (далее – ИСПДн) государственной инспекции по охране объектов культурного наследия (далее – ГИО ОКН НСО), защищенных от несанкционированного доступа и предназначенных для обработки и хранения персональных данных.**

**1.2. Данные работы проводятся только с разрешения руководства ГИО ОКН НСО или лица, исполняющего его обязанности, после согласования с ответственным за обеспечение безопасности персональных данных.**

**2. Порядок проведения работ по техническому обслуживанию, ремонту, модернизации технических средств**

**2.1. В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав ИСПДн, ответственный за обеспечение безопасности персональных данных представляет служебную записку, в которой:**

указывает название и номер автоматизированного рабочего места (далее – АРМ) (технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;

обосновывает необходимость технического обслуживания (модернизации);

указывает планируемые место и сроки работ, режим их проведения;

перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

**2.2. В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе на АРМ или в помещение, составляется список лиц, который согласовывается с руководством ГИО ОКН НСО.**

**2.3. Запрещается выносить технические средства, входящие в состав ИСПДн, из помещений, занимаемых ГИО ОКН НСО, без согласования с ответственным за обеспечение безопасности персональных данных и разрешения руководства ГИО ОКН НСО.**

**2.4. Вскрытие печатей на корпусах АРМ или других технических средств и последующее опечатывание производится комиссионно в присутствии ответственного за обеспечение безопасности персональных данных, о чём составляется акт.**

В акте указывается:

номер (название) помещения, в котором проводились работы;

дата и время начала и окончания работ;

лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации);

наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия АРМ (технического средства, системы);

установленные неисправности;

виды и результаты проведенных работ;

замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков;

какими печатями (пломбами и т.д.) и в каких местах АРМ (устройство) опечатано по окончании работ;

иная необходимая для дальнейшей работы и обеспечения безопасности информация.

**2.5. Если для ремонта (модернизации) ИСПДн (другого технического средства, системы, элемента АРМ в составе ИСПДн) необходимо направить в специализированную организацию, то комиссией составляется заключение.**

**2.6. Перед отправкой АРМ (другого технического средства, системы, элемента АРМ) ответственный за обеспечение безопасности персональных данных обязан гарантированно удалить персональные данные с жесткого диска и иных устройств памяти АРМ (другого технического средства, системы) сертифицированными средствами, о чем составляется акт. По запросу из специализированной организации копия акта передаётся и ей.**

**2.7. В случае если не имеется возможности гарантированно удалить персональные данные с жесткого диска и иных устройств памяти АРМ (другого технического средства, системы) сертифицированными средствами или произвести обезличивание персональных данных, эти устройства опечатываются и хранятся у ответственного за обеспечение безопасности персональных данных с соблюдением требований, предъявляемым к хранению персональных данных.**

**2.8. Ремонт и замена жесткого диска производится с соблюдением требований п.п. 2.5-2.7 настоящей Инструкции в присутствии ответственного за обеспечение безопасности персональных данных. При диагностике и ремонте жесткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.**

**3. Порядок обновления общесистемного и прикладного программного обеспечения.**

**3.1. Установку, обновление и модификацию общесистемного и прикладного программного обеспечения АРМ ИСПДн проводит администратор безопасности информации.**

**3.2. Изменение конфигурации программных средств ИСПДн кем-либо, кроме администратора безопасности информации запрещено.**

**3.3. Установка или обновление программного обеспечения ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций данного программного обеспечения.**

**3.4. Установка и обновление программного обеспечения (системного, прикладного, тестового и т.п.) на АРМ ИСПДн производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), если иной порядок установки и обновления не предусмотрен разработчиком программного обеспечения.**

**3.5. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.**

**3.6. Программное обеспечение, устанавливаемое на АРМ ИСПДн, а также его обновления, перед установкой должны пройти антивирусный контроль.**

**4. Порядок обновления программного обеспечения средств защиты информации**

**4.1. Внесение изменений в конфигурацию аппаратно-программных и программных средств защиты информации проводит администратор безопасности информации.**

4.2. Обновление баз данных, необходимых для реализации функций безопасности средства защиты информации (обновление баз сигнатур вирусов средств антивирусной защиты, баз сигнатур уязвимостей средств контроля (анализа) защищенности, баз решающих правил систем обнаружения вторжений и других) выполняется в автоматическом режиме по расписанию со специальных серверов обновления производителей средств защиты информации.

4.3. Обновление программного обеспечения средств защиты информации, направленное на устранение уязвимостей средства защиты информации осуществляется после получения информации от производителя средства защиты информации о необходимости обновления в порядке, установленном производителем средства защиты информации.

4.4. Обновление, направленное на добавление функции (функций) безопасности средства защиты информации, на совершенствование реализации функции (функций) безопасности средства защиты информации, на расширение числа поддерживаемых программных и аппаратных платформ, а также обновление, не влияющее на безопасность средства защиты информации (изменение интерфейса средства защиты информации, иных функций, не влияющее на функции безопасности средства защиты информации) осуществляются по решению руководства ГИО ОКН НСО в порядке, определенном производителем средства защиты информации.