Приложение № 10

Утверждено

приказом государственной

инспекции по охране объектов

культурного наследия

Новосибирской области

от \_\_\_\_\_\_ 2023 г. № \_\_\_\_\_

Инструкция

о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных

**1. Общие положения**

**1.1. Настоящая Инструкция** о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных **(далее – Инструкция) определяет порядок действий по резервированию и восстановлению работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), баз данных и средств защиты информации (далее – СЗИ), связанных с функционированием** информационных систем персональных данных **(далее – ИСПДн) государственной инспекции по охране объектов культурного наследия Новосибирской области (далее –** ГИО ОКН НСО)**, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.**

**1.2. Целью Инструкции является превентивная защита элементов ИСПДн от потери защищаемой информации.**

**1.3. Задачами данной Инструкции является:**

**определение мер защиты от потери информации;**

**определение действий восстановления в случае потери информации.**

**1.4. Действие настоящей Инструкции распространяется на всех сотрудников** ГИО ОКН НСО**, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:**

**системы жизнеобеспечения;**

**системы обеспечения отказоустойчивости;**

**системы резервного копирования и хранения данных;**

**системы контроля физического доступа.**

**1.5. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности информации.**

**1.6. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается администратор безопасности информации или ответственный по обеспечению безопасности персональных данных.**

**2. Порядок реагирования на инцидент**

**2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.**

**2.2. Происшествие, вызывающее инцидент, может произойти:**

**в результате непреднамеренных действий пользователей;**

**в результате преднамеренных действий пользователей и третьих лиц;**

**в результате нарушения правил эксплуатации технических средств ИСПДн;**

**в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.**

**2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником.**

**2.4. В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности информации, предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.**

**3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов**

**3.1. Технические меры:**

**3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:**

**системы жизнеобеспечения;**

**системы резервного копирования и хранения данных;**

**системы контроля физического доступа.**

**3.1.2. Системы жизнеобеспечения ИСПДн включают:**

**пожарные сигнализации и системы пожаротушения;**

**системы вентиляции и кондиционирования;**

**системы резервного питания.**

**3.1.3. Все критичные помещения** ГИО ОКН НСО **(помещения, в которых размещаются элементы ИСПДн и средства защиты информации) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.**

**3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:**

**локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;**

**источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;**

**резервные линии электропитания в пределах комплекса зданий.**

**3.1.5. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на носителе информации (жесткий диск, оптический диск, флэш накопитель и т.п.).**

**3.2. Организационные меры:**

**3.2.1. Резервное копирование данных должно осуществлять на периодической основе:**

**для обрабатываемых персональных данных – не реже раза в неделю;**

**для технологической информации – не реже раза в месяц;**

**эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в 6 месяцев, и каждый раз при внесении изменений в эталонные копии (выход новых версий).**

**3.2.2. Данные о проведение процедуры резервного копирования и восстановления, должны отражаться в специально созданном журнале учета (приложение).**

**3.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.**

**3.2.4. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.**

**3.2.5. Носители должны храниться не менее года, для возможности восстановления данных.**

**4. Порядок восстановления работоспособности информационных систем**

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы, в общем случае, осуществляются в следующей последовательности:

проверка исправности и работоспособности средств обеспечения функционирования ИСПДн;

восстановление работоспособности (ремонт или замена) средств обеспечения функционирования ИСПДн, при необходимости;

проверка правильности функционирования общего программного обеспечения ИСПДн;

восстановление нормального функционирования общего программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним или резервных копий настроек, при необходимости;

проверка правильности функционирования средств защиты информации;

восстановление нормального функционирования средств защиты информации с использованием дистрибутивов и обновлений к ним, при необходимости;

проверка правильности функционирования специального программного обеспечения ИСПДн;

восстановление нормального функционирования специального программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним, при необходимости;

восстановление баз персональных данных с использованием резервной копии в течении одного рабочего дня.

Данные работы осуществляются в соответствии с эксплуатационной документацией на технические и программные средства до полного восстановления работоспособности.

Восстановление персональных данных, созданных после их последнего резервирования, осуществляется пользователями, осуществившими их внесение в базы персональных данных.

Работы по техническому обслуживанию технических и программных средств ИСПДн осуществляется в соответствии с правилами, установленными в «Инструкции 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 ГИО ОКН НСО».

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными, а также несанкционированного копирования на машинные носители информации. Ответственность за выполнение данного требования возлагается на администратора безопасности информации.

**Приложение к Инструкции** о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных ГИО ОКН НСО

**Форма**

**журнала резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных систем персональных данных ГИО ОКН НСО**

|  | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | Дата | Вид операции | Устройство | Каталог накопителя | Наименование резервной копии | Место хранения резервной копии | ФИО, проводившего резервирование / восстановление | Подпись, проводившего резервирование / восстановление |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |