МУНИЦИПАЛЬНОЕ КАЗЁННОЕ УЧРЕЖДЕНИЕ АНЖЕРО-СУДЖЕНСКОГО ГОРОДСКОГО ОКРУГА «ФУНКЦИОНАЛЬНО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

ПРИКАЗ

от 23.08.2018г. **№ 81**

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

Руководствуясь требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановления Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" и в целях защиты персональных данных граждан, обрабатываемых в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных муниципального казённого учреждения Анжеро-Судженского городского округа «Функционально-аналитический центр» (далее - Порядок).
2. Главному специалисту отдела информационной и кадровой работы МКУ «ФАЦ» Белоусовой А.С. ознакомить сотрудников с настоящим порядком и обеспечить его исполнение.
3. Контроль за исполнением приказа возложить на начальника юридического отдела МКУ «ФАЦ» Модель А.В.

Директор МКУ «ФАЦ» С.А. Вейс

МКУ «ФАЦ»

С приказом ознакомлена А.В. Модель

А.С. Белоусова

Утверждено
приказом МКУ «ФАЦ»
от 23.08.2018 № 81

Положение
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр»

Назначение и область действия

Положение о порядке резервирования и восстановления работоспособности технических средств (далее ТС) и программного обеспечения (далее ПО), баз данных и средств защиты информации (далее СЗИ) информационных систем персональных данных (далее ИСПДн) (далее – Инструкция) определяет действия, связанные с функционированием ИСПДн в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей муниципального казённого учреждения Анжеро-Судженского городского округа «Функционально-аналитический центр», 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.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, а так же за контроль обеспечения мероприятий по предотвращению инцидентов

безопасности, приводящих к потере защищаемой информации назначается Администратор ИСПДн.

Порядок реагирования на инцидент

В данной Инструкции под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

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.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники муниципального казённого учреждения Анжеро-Судженского городского округа «Функционально-аналитический центр» (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

Технические меры

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 обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все помещения муниципального казённого учреждения Анжеро-Судженского городского округа «Функционально-аналитический центр», в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

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.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (жесткий диск и т.п.).

Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – ежедневные автоматические копии на глубину 2 недель с дополнительным ручным копированием перед началом каждого отчетного периода (по запросу руководителя структурного подразделения эксплуатирующего ИСПДн);

- 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 месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Резервные копии создаваемые вручную по запросу должны храниться не менее трех лет, для возможности восстановления данных.

Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на Администратора безопасности информации в муниципальном казённом учреждении Анжеро-Судженского городского округа «Функционально-аналитический центр».