Приложение № 3
к Приказу № 29 от 11.02.2 2022 г.

МИНИСТЕРСТВО КУЛЬТУРЫ СВЕРДЛОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ СВЕРДЛОВСКОЙ ОБЛАСТИ
«УРАЛЬСКИЙ ЦЕНТР НАРОДНОГО ИСКУССТВА ИМЕНИ Е.П.РОДЫГИНА»

ПОРЯДОК
резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в государственном автономном учреждении культуры Свердловской области «Уральский центр народного искусства имени Е.П.Родыгина»

Екатеринбург
2022

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации (далее – Инструкция) определяет действия, связанные с функционированием ИСПДн ГАУК СО УрЦНИ (далее Оператор), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Задачей данной Инструкции является:

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

Действие настоящей Инструкции распространяется на всех пользователей Оператора, 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.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящим к потере защищаемой информации и контроль обеспечения мероприятий по предотвращению инцидентов безопасности, назначается Администратор безопасности ИСПДн.

2. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

В настоящем документе 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.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Оператора предпринимают 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 НЕПРЕРЫВНОЙ 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;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, могут 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.

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;
- резервные линии электропитания.

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

Организационные меры.

Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемых персональных данных – не реже раза в месяц;

– для технологической информации – не реже раза в год;

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

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

Носители, на которые произведено резервное копирование, должны быть пронумерованы.

Носители должны храниться в несгораемом шкафу.