Приложение 14
к приказу от 14.02.2022 № 8

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ»
КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ
(МАУ «ЦМИ»)
Адрес: 694020, Сахалинская область, г.Корсаков, ул.Восточная, 29/2,
телефон: 8(42435)4-00-59, e-mail: mbu_cmi2016@mail.ru

УТВЕРЖДАЮ:
и.о. директора МАУ «ЦМИ»
_____ Д.М. Шпачук
Приказ № 8 от 14.02.2022

ПОРЯДОК РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ РАБОТОСПОСОБНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В МУНИЦИПАЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ «ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ» КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ

Корсаков
2022

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности технических средств (далее - ТС) и программного обеспечения (далее - ПО), баз данных и средств защиты информации определяет действия, связанные с функционированием государственных информационных систем (далее - ГИС) в муниципальном автономном учреждении «Центр молодежных инициатив» Корсаковского городского округа Сахалинской области (далее - МАУ «ЦМИ»), меры и средства поддержания непрерывности работы и восстановления работоспособности.

Целью настоящего документа является превентивная защита элементов ГИС от предотвращения потери.

Задачи, решаемые данным Порядком, охватывают определение мер защиты от потери информации: определение действий восстановления в случае потери информации.

Действие настоящего Порядка распространяется на всех пользователей ГИС, имеющих доступ к ее ресурсам, 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 одного раза в два года.

Ответственным работником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор безопасности информационной системы персональных данных (далее - Администратор).

Ответственным работником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор.

2. Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ГИС, предоставляемых пользователям ГИС, а также 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 ГИС; в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться Администратором в «Журнале учета мероприятий по контролю обеспечения защиты информации» в ГИС МАУ «ЦМИ».

В кратчайшие сроки, не превышающие одного рабочего дня, Администратор предпринимает меры по восстановлению работоспособности. Предпринимаемые меры согласуются с директором МАУ «ЦМИ».

3. 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 ГИС включают: пожарные сигнализации и системы пожаротушения; системы вентиляции и кондиционирования; системы резервного питания.

Все критичные помещения в МАУ «ЦМИ» (помещения, в которых размещаются элементы ГИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации и (или) пожаротушения.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ГИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания (или встроенные аккумуляторы). 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;

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

Организационные меры

Резервное копирование данных, должно осуществлять на периодической основе не реже одного раза в месяц; эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ГИС - не реже одного раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Хранение резервных копий должно осуществляться на автоматизированном рабочем месте директора МАУ «ЦМИ».