УТВЕРЖДЕНА

Приказом директора областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»

от 09. 01. 2019 г. № 19

ИНСТРУКЦИЯ
по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ОГБУ «КЦСО ЕАО»

1. Общие положения

1.1. Настоящая инструкция (далее – Инструкция) по резервированию и восстановлению работоспособности технических средств (далее – ТС), программного обеспечения (далее – ПО), баз данных (далее – БД), средств защиты информации (далее – СЗИ)и средств криптографической защиты информации (далее – СКЗИ) информационной системы персональных данных (далее – АИС) в ОГБУ «КЦСО ЕАО» определяет действия, связанные с функционированием технических и программных средств АИС и системы защиты персональных данных (далее – СЗПДн).

1.2. Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»; Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Приказа ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Целью данной инструкции является превентивная защита элементов АИС и СЗПДн от предотвращения потери защищаемой информации.

1.4. Задачами данной инструкции являются:

- определение мер защиты от потери информации;
- определение действий восстановления технических и программных средств АИС и СЗПДн в случае потери информации.

1.5. Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам АИС, в том числе уполномоченных имеющих доступ к техническим и программным средствам СЗПДн в рамках своих полномочий, при возникновении аварийных ситуаций, в том числе:

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

1.6. Пользователем АИС (далее – Пользователь) является сотрудник ОГБУ «КЦСО ЕАО», участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и СЗИ АИС .

1.7. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС или СЗПДн, предоставляемых пользователям, а также потерей защищаемой информации.

2. Порядок реагирования на инцидент

2.1. 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 АИС и СЗПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2. Все действия в процессе реагирования на Инцидент должны документироваться ответственным за обеспечение безопасности персональных данных информационных систем персональных данных ОГБУ «КЦСО ЕАО» в Журнале учета событий информационной безопасности.

2.3. В кратчайшие сроки, не превышающие одного рабочего дня ответственный за обеспечение безопасности персональных данных информационных систем персональных данных предпринимает меры по восстановлению работоспособности.

2.4. Предпринимаемые меры, по возможности, согласуются с руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Технические меры

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

3.2. Системы жизнеобеспечения АИС включают:

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

3.3. Все помещения учреждения, в которых размещаются элементы АИС и СЗПДн) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АИС и СЗПДн, сетевое

и коммуникационное оборудование, а также наиболее критичные АРМ 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;
- дублированные системы электропитания в устройствах (серверы, активное сетевое оборудование и т.д.);

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

4. Организационные меры

4.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых ПДн – согласно инструкции по обеспечению безопасности ПДн;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (ОС, штатное и специальное ПО, программные СЗИ), с которых осуществляется их установка на элементы АИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

4.3. Носители должны храниться не менее года для возможности восстановления данных.

Подготовил:
Специалист по технической поддержке

Согласовано:
Администратор
информационной безопасности