

ИНСТРУКЦИЯ

по организации резервирования и восстановления программного обеспечения, баз данных информационных систем персональных данных в муниципальном бюджетном учреждении «Централизованная библиотечная система»

1. Общие положения

1.1. Настоящая инструкция по организации резервирования и восстановления программного обеспечения, баз данных информационных систем персональных данных в муниципальном бюджетном учреждении «Централизованная библиотечная система» (далее – Инструкция) разработана с целью обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Настоящая Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее - ИСПДн) в муниципальном бюджетном учреждении «Централизованная библиотечная система» (далее – Учреждение).

1.4. В ИСПДн резервированию подлежат:

- базы данных;
- специальное программное обеспечение;
- общее программное обеспечение;
- программное обеспечение средств защиты информации.

2. Порядок резервирования и хранения резервных копий баз данных и программного обеспечения

2.1. Обязательному резервированию подлежат:

- базы данных (текстовые и табличные файлы, а также файлы баз данных специализированных программных продуктов, хранящиеся на компьютере);
- специальное (прикладное) программное обеспечение, используемое для обработки персональных данных;
- программное обеспечение средств защиты информации, в том числе средств антивирусной и криптографической защиты;
- общее программное обеспечение (операционная система и программные драйверы устройств (принтеры, мониторы, видеокарты и тому подобное), поставляемые со средствами вычислительной техники, входящими в состав ИСПДн).

2.2. Резервирование баз данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком отчуждаемые носители информации.

2.3. Резервирование осуществляется не реже одного раза в месяц.

2.4. Носители информации, содержащие резервные копии данных ИСПДн, не могут быть переданы за пределы контролируемой зоны оператора и уполномоченной организации по обеспечению безопасности персональных данных без согласования с уполномоченной организацией по обеспечению безопасности персональных данных.

2.5. Копирование информации с носителей информации, содержащих резервные копии данных ИСПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.

2.6. Резервирование общего программного обеспечения осуществляется путем создания контрольной точки восстановления системы.

2.7. Резервирование программного обеспечения средств защиты информации обеспечивается путем хранения носителей дистрибутивов программного обеспечения средств защиты информации и обновлений к ним в уполномоченной организации по обеспечению безопасности персональных данных.

2.8. Носители обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны быть маркированы датой их получения (датой выхода обновления).

3. Порядок восстановления работоспособности ИСПДн

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

3.2. Работы по восстановлению работоспособности в общем случае осуществляются в следующей последовательности:

- проверка исправности и работоспособности средств обеспечения функционирования информационных систем;
- восстановление работоспособности (ремонт или замена) средств обеспечения функционирования информационных систем, при необходимости;
- проверка исправности и работоспособности средств вычислительной техники;
- восстановление работоспособности (ремонт или замена) средств вычислительной техники при необходимости;
- проверка правильности функционирования общего программного обеспечения ИСПДн;
- восстановление нормального функционирования общего программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним 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;
- проверка целостности баз данных ИСПДн;
- восстановление баз данных ИСПДн с использованием резервной копии при необходимости;

Данные работы осуществляются в соответствии с эксплуатационной документацией до полного восстановления работоспособности.

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

3.4. 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.

3.5. Ответственность за проведение мероприятий по обеспечению соблюдения требований настоящей инструкции возлагается на уполномоченную организацию по обеспечению безопасности персональных данных.