УТВЕРЖДАЮ

Председатель кооператива
ЖКС «Энергетик»
_____ Ю.Ю. Золотов
«09» января 20 18 г.

Инструкция
по организации порядка резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных Кооператива ЖКС «Энергетик»

2018 г.

1. Общие положения

1.1 Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации определяет действия, связанные с функционированием информационных систем персональных данных (далее - ИСПДн Кооператив ЖКС «Энергетик» (далее – Кооператив), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

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

1.3 Задачей настоящего документа является:

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

1.4 Действие настоящего документа распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.

1.5 Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в три года.

1.6 Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор ИСПДн.

1.7 Ответственность за проведение мероприятий по проведению резервного копирования в ИСПДн, восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации возлагается на администратора ИСПДн.

2. Порядок реагирования на инцидент

2.1 В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2 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.

2.3 В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники 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 непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1 К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов.

3.2 Все помещения, в которых размещаются элементы ИСПДн и средства защиты информации должны быть оборудованы средствами охранно-пожарной сигнализации.

3.3 Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн должны подключаться к сети электропитания через источники бесперебойного питания.

3.4 Для защиты от потери информации и отказов машинных носителей информации должно осуществляться резервное копирование системного и прикладного

программного обеспечения, баз данных, средств защиты информации, а также документов, содержащих персональные данные.

3.5 Дистрибутивы системного и прикладного программного обеспечения, средств защиты информации должны храниться у администратора ИСПДн.

3.6 Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для обрабатываемых персональных данных в ИСПДн «Бухгалтерия», «Биллинг ЖКХ» – не реже одного раза в квартал на съемный носитель информации;

– 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 год с учетом проверки читаемости дистрибутивов, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в «Журнале учета процедуры резервного копирования».

3.7 Для создания резервной копии в ИСПДн допускаются только зарегистрированные носители конфиденциальной информации.

Носители должны быть пронумерованы: номером носителя, датой проведения резервного копирования и учтены в журнале учета машинных носителей.

По окончании процедуры резервного копирования электронные носители информации (CD, DVD-диски, USB-накопитель, другие) хранятся в сейфе (металлическом шкафу) у администратора ИСПДн, либо у директора Учреждения.

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

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