МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ПРЕДПРИЯТИЕ
«ТЕПЛОСЕТЬ» ГОРОДА СЕРДОБСКА СЕРДОБСКОГО РАЙОНА

П Р И К А З

16.03.2010 г. Сердобск № 06

О назначении администраторов безопасности информационных систем персональных данных в МКП «Теплосеть»

В целях исполнения в МКП «Теплосеть» требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями),

ПРИКАЗЫВАЮ:

1. Утвердить список работников, определенных администраторами безопасности информационных систем персональных данных Предприятия и закрепить за ними информационные системы персональных данных Предприятия, согласно приложению № 1.
2. Утвердить инструкцию администратора безопасности информационной системы персональных данных на Предприятии, согласно приложению № 2.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор В.Э. Мавровский

Приложение № 1

УТВЕРЖДЕН
приказом МКП «Теплосеть»
от 16.03.2020 № 06

В.Э. Мавровский

СПИСОК
работников, определенных администраторами безопасности информационных систем персональных данных Предприятия

№ п/п	Фамилия, имя, отчество	Должность	Информационные системы персональных данных структурного подразделения Предприятия
1	Иванова О.В.	Инспектор по кадрам	Персональные данные сотрудников МКП «Теплосеть»
2	Маринина Н.М.	Специалист абонентского отдела	База данных абонентского отдела МКП «Теплосеть»

Приложение № 2

УТВЕРЖДЕН
приказом МКП «Теплосеть»
от 16.03.2020 № 06

В.Э. Мавровский

ИНСТРУКЦИЯ
администратора безопасности информационной системы персональных данных на Предприятии

1. Общие положения

1.1. Инструкция является руководящим документом администратора безопасности информационной системы персональных данных (далее – ИСПДн) в МКП «Теплосеть».

1.2. Требования администратора безопасности ИСПДн Предприятия, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками, допущенными к обработке персональных данных.

1.3. Работа с персональными данными (далее – ПДн) строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ, содержащий ПДн (не зависимо от типа носителя: бумажный, электронный), должен отвечать конкретный работник;
- принцип контроля и учета – все операции с документами, содержащими ПДн, должны отражаться в соответствующих журналах и карточках.

2. Обязанности администратора безопасности

2.1. В своей повседневной деятельности администратор руководствуется данной Инструкцией и другими документами, регламентирующими защиту персональных данных от утечки по техническим каналам и несанкционированного доступа (далее – НСД), эксплуатационной документацией на установленные на объекте информатизации системы защиты информации от НСД и от утечки информации по техническим каналам.

2.2. Администратор безопасности:

- обеспечивает поддержку подсистем управления доступом, регистрации и учета информационных ресурсов;
- контролирует целостность программно-аппаратной среды, хранимой и обрабатываемой информации;
- контролирует доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации.

2.3. На администратора безопасности возлагаются следующие обязанности:

- знать уровень конфиденциальности обрабатываемой информации и класс ИСПДн, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных и несъемных носителей информации;

- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;

- обеспечивать доступ к защищаемой информации пользователям согласно их прав доступа;

- незамедлительно докладывать директору Предприятия о всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;

- контролировать правильность применения пользователями сети средств защиты информации;

- участвовать в испытаниях и проверках ИСПДн;

- не допускать к работе на рабочих местах посторонних лиц;

- осуществлять контроль монтажа оборудования специалистами сторонних организаций;

- участвовать в приемке новых программных средств;

- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию;

- вести журнал учета работы с ИСПДн.

2.4. Регистрации в журнале учета работ ИСПДн подлежат:

- обновление программного обеспечения ИСПДн;

- обновление антивирусных баз;

- вскрытие системного блока с целью модернизации или ремонта с указанием цели вскрытия и проводимых работ;

- создание резервной копии базы данных и иной служебной информации;

- замена системного блока с указанием факта гарантированного удаления информации с жесткого магнитного диска;

- отклонения в нормальной работе системных и прикладных программных средств затрудняющих эксплуатацию ПЭВМ;

- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.);

- перебои в системе электроснабжения.

2.5. При выявлении утечки информации администратор безопасности обязан немедленно прекратить работы в ИСПДн, подать служебную записку руководству и занести соответствующую запись в журнал учета работы ИСПДн с изложением факта нарушения, предпринятые и(или) рекомендуемые им действия.

2.6. Форма журнала регистрации работ ИСПДн (образец заполнения):

Дата	Наименование работ	Ф.И.О. исполнителя работ	ИСПДн	Роспись
1	2	3	4	5
03.02.2020	Обновление антивирусной базы, сканирование дисков	ФИО	ИСПДн работников	
03.02.2020	Переустановка операционной системы	ФИО	ИСПДн контрагентов	

3. Ответственность

Администратор безопасности несет ответственность за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей Инструкцией и нормативными документами по защите информации.