Обозначения и сокращения

АРМ – автоматизированное рабочее место
ИСПДн – информационная система персональных данных
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПК – персональный компьютер
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
РД – руководящие документы
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
УБПДн – угрозы безопасности персональных данных
ФСТЭК – Федеральная служба по экспортному и техническому контролю
ФСБ – Федеральная служба безопасности
Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

1. Общие положения.

1.1. Ответственный за обеспечение безопасности ПДн (Администратор информационной безопасности – далее ИБ) назначается приказом руководителя Управления государственного заказа и лицензирования Белгородской области (далее – Учреждение).

1.2. Администратор ИБ подчиняется непосредственно руководителю или лицу, замещающему руководителя.

1.3. Администратор ИБ в своей работе руководствуется настоящей инструкцией, законодательством РФ, руководящими и нормативными документами ФСТЭК России, ФСБ, Роскомнадзора, а также регламентирующими документами Учреждения.

1.4. Администратор ИБ отвечает за поддержание необходимого уровня безопасности объектов защиты, содержащих ПДн.

1.5. Администратор ИБ является должностным лицом Учреждения, уполномоченным на проведение работ по защите информации, содержащей персональные данные и поддержанию достигнутого уровня защиты персональных данных, обрабатываемых с использованием средств автоматизации и без использования таковых.

1.6. Администратор ИБ должен иметь специальное рабочее место, размещенное в здании Учреждения так, что бы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. На рабочем месте Администратора ИБ должны присутствовать средства физической защиты внешних электронных и бумажных носителей информации (личный сейф, железный шкаф).

1.8. Администратор ИБ осуществляет методическое руководство сотрудников, допущенных к обработке ПДн, к техническим средствам информационной системы персональных данных (ИСПДн) и иной конфиденциальной информации, в вопросах обеспечения безопасности информации.

1.9. Требования Администратора ИБ, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми сотрудниками имеющими доступ к ПДн и конфиденциальной информации.

1.10. Администратор ИБ несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

1.11. Администратор ИБ по согласованию с руководителем Учреждения для консультаций по выбору и реализации методов и способов защиты информации в информационной системе может привлекать организацию, имеющую оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

2. Должностные обязанности.

Администратор ИБ обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Осуществлять установку, настройку и сопровождение технических средств защиты, при необходимости может привлекать на договорных обязательствах по согласованию с руководителем организацию, имеющую оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Уточнять в установленном порядке обязанности пользователей и администраторов ИСПДн.

2.6. Вести контроль над процессом осуществления резервного копирования защищаемой информации.

2.7. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.8. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.9. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.10. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.

2.11. Контролировать исполнение пользователями парольной политики.

2.12. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.13. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.14. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.15. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.16. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.17. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.18. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.19. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.20. Контролировать обработку ПДн без использования средств автоматизации согласно принятому в учреждении порядку обработки персональных данных без использования средств автоматизации и Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного Постановлением правительства РФ № 687 от 15.09.2008г.