УТВЕРЖДЕНА
решением Пелымской
поселковой территориальной
избирательной комиссии
от 27 июня 2025 г. № 4/15

Инструкция администратора информационной безопасности Пелымской поселковой территориальной избирательной комиссии

1. Общие положения

1.1. Администратор информационной безопасности (далее – Администратор ИБ) назначается решением Пелымской поселковой территориальной избирательной комиссии.

1.2. Администратор ИБ в своей работе руководствуется требованиями Федерального Законодательства, руководящими и нормативными документами ФСТЭК РФ, регламентирующими документами Избирательной комиссии Свердловской области, Пелымской поселковой территориальной избирательной комиссии и настоящей инструкцией.

1.3. Администратор ИБ отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационных систем персональных данных (ИСПДн) и ее ресурсов на этапах эксплуатации и модернизации.

1.4. Администратор ИБ осуществляет методическое руководство администратора и пользователей ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.5. Требования администратора ИБ, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми администраторами и пользователями ИСПДн.

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

2. Должностные обязанности

Администратор ИБ обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и руководства о порядке организации и проведении работ по защите информации.

2.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

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

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечить доступ к защищаемой информации Пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Уточнять в установленном порядке обязанности Пользователей ИСПДн по обработке объектов защиты.

2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.8. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

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

2.10. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.11. Контролировать исполнение Пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

2.12. Контролировать исполнение пользователями парольной политики.

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 носителей ПДн, 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 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.