Приложение 7
Утверждены
постановлением Администрации
Ребрихинского района Алтайского края

от 28.12.2018 №745

ИНСТРУКЦИЯ
по проведению антивирусного контроля в информационных системах Администрации Ребрихинского района Алтайского края

1. Общие положения

1.1. Инструкция по проведению антивирусного контроля в информационных системах Администрации Ребрихинского района Алтайского края (далее – «Инструкция») предназначена для пользователей информационных систем Администрации Ребрихинского района Алтайского края (далее – «организация»).

1.2. В целях обеспечения антивирусной защиты в информационных системах органов исполнительной власти Алтайского края, органов местного самоуправления Алтайского края и подведомственных им организаций (далее – «ИС») производится антивирусный контроль.

1.3. Ответственность за поддержание установленного в Инструкции порядка возлагается на администратора безопасности ИС.

1.4. К применению в ИС допускается лицензионное антивирусное программное обеспечение.

2. Порядок проведения антивирусного контроля в ИС

2.1. Антивирусный контроль должен осуществляться на ПЭВМ в постоянном режиме.

2.2. Пользователи ИС при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет наличия вредоносного программного обеспечения.

2.3. Администратор безопасности ИС осуществляет контроль обновления антивирусных баз и функционирования антивирусной защиты информации.

2.4. Администратор безопасности ИС проводит периодическое тестирование установленного программного обеспечения на предмет наличия вирусов.

2.5. При обнаружении вредоносного программного обеспечения пользователь ИС обязан немедленно поставить в известность администратора безопасности ИС и прекратить какие-либо действия в ИС.

2.6. Администратор безопасности ИС проводит в случае необходимости лечение зараженных файлов с помощью антивирусного программного обеспечения и после этого вновь проводит антивирусный контроль.

2.7. В случае обнаружения на носителе информации вредоносного программного обеспечения, неподдающегося лечению, администратор

безопасности ИС обязан запретить использование данного носителя информации, а также обязан поставить в известность руководителя подразделения или лицо, ответственное за обеспечение информационной безопасности, запретить работу в ИС и принять меры по восстановлению работоспособности ИС.