|  |  |
| --- | --- |
|  | Приложение №21 к распоряжению администрациимуниципального образования Первомайский поссоветОренбургского района Оренбургской областиот \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_ |

**Инструкция по антивирусной защите в информационных системах персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района**

1. **Общие положения**
	1. Настоящая Инструкция по антивирусной защите в информационных системах персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района (далее – Инструкция) разработана с целью защиты персональных данных в администрации муниципального образования Первомайский поссовет Оренбургского района от несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.
	2. Установка и настройка средств антивирусного контроля на серверах и рабочих станциях, включенных в состав информационных систем персональных данных (далее – ИСПДн) администрации муниципального образования Первомайский поссовет Оренбургского района, осуществляется администратором безопасности, назначенным настоящим распоряжением, в соответствии с руководством по применению конкретных антивирусных средств.
	3. Данные требования не распространяются на рабочие станции с установленными операционными системами, для которых отсутствуют какие-либо средства антивирусного контроля.
2. **Применение средств антивирусного контроля**
	1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов рабочих станций.
	2. Обязательному антивирусному контролю подлежит любая информация (файлы любых форматов), информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
	3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.
	4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка на защищаемых серверах и рабочих станциях.
	5. Пользователи ИСПДн администрации муниципального образования Первомайский поссовет Оренбургского района, указанные в Матрице доступа к информационным системам персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района (приложение № 11 к настоящему распоряжению) при работе со съемными носителями обязаны перед началом работы осуществить их проверку на предмет наличия компьютерных вирусов.
	6. Администратор безопасности настраивает антивирусное средство на автоматическое обновление и ведет за ним контроль.
	7. Администратор безопасности проводит периодическое тестирование всех элементов ИСПДн администрации муниципального образования Первомайский поссовет Оренбургского района и установленного программного обеспечения на предмет наличия компьютерных вирусов.
	8. Использование для обработки и хранения персональных данных неучтенных носителей запрещается.
	9. При обнаружении компьютерного вируса пользователи ИСПДн администрации муниципального образования Первомайский поссовет Оренбургского района обязаны немедленно поставить в известность администратора безопасности и прекратить какие-либо действия в соответствующей информационной системе персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района.
	10. Администратор безопасности при обнаружении компьютерного вируса принимает меры для «лечения» зараженного файла и удаления вируса и после этого вновь проводит антивирусный контроль.
	11. В случае обнаружения на учтенном в Журнале учета съемных носителей, содержащих персональные данные (приложение № 28 к настоящему распоряжению) носителе вируса, не поддающегося лечению, администратор безопасности обязан:
		1. запретить использование носителя;
		2. поставить в известность ответственное лицо за организацию обработки персональных данных, назначенное настоящим распоряжением;
		3. запретить работу в информационной системе персональных данных, в которой применялся зараженный съемный носитель;
		4. в возможно короткие сроки обновить пакет антивирусных программ;
		5. провести антивирусное сканирование информационной системы персональных данных, в которой применялся зараженный съемный носитель.
3. **Ответственность**
	1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности администрации муниципального образования Первомайский поссовет Оренбургского района.
	2. Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности и всех сотрудников, являющихся пользователями ИСПДн администрации муниципального образования Первомайский поссовет Оренбургского района согласно Матрице доступа к информационным системам персональных данных администрации муниципального образования Первомайский поссовет Оренбургского района (приложение № 11 к настоящему распоряжению).
	3. Периодический контроль за состоянием антивирусной защиты в ИСПДн администрации муниципального образования Первомайский поссовет Оренбургского района, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется администратором безопасности.

\_\_\_\_\_\_\_\_\_