



**АДМИНИСТРАЦИЯ
АНУЧИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
ПРИМОРСКОГО КРАЯ**

РАСПОРЯЖЕНИЕ

18.01 2021 г.

с. Анучино

№ 09 - р

**Об утверждении инструкций по организации антивирусной защите и
парольной защите в информационных системах персональных данных в
администрации Анучинского муниципального округа
Приморского края**

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», руководствуясь Федеральным законом от 06.10.2003 г. № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», Уставом Анучинского муниципального округа Приморского края

1. Утвердить инструкцию по организации антивирусной защиты в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края (Прилагается).

2. Утвердить инструкцию по парольной защите в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края (Прилагается).

3. Ознакомить сотрудников администрации Анучинского муниципального округа Приморского края с прилагаемыми инструкциями (Федчикова А.А.).

4. Контроль за исполнением настоящего распоряжения возложить на А.Я. Янчука, первого заместителя главы администрации Анучинского муниципального округа.

Глава Анучинского
муниципального округа



С.А. Понуровский

УТВЕРЖДЕНА
Распоряжением администрации Анучинского
муниципального округа
Приморского края
от « 18 » 01 2021 г. № 09-р

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах персональных данных в администрации Анучинского муниципального округа Приморского края

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в администрации Анучинского муниципального округа Приморского края (далее - Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

1.2. Данная инструкция распространяется на всех пользователей и администраторов информационных систем персональных данных (далее – ИСПДн) в Администрации.

2. Установка и обновление антивирусных средств

2.1. Установка и настройка антивирусных средств осуществляются только Администратором информационной системы персональных данных.

2.2. Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, flash дисках,

CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.2. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.

3.3. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

3.4. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ (электронно-вычислительная машина). Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность.

3.5. Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.

3.6. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.7. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной системы персональных данных;

- провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса пользователь или администратор информационной системы персональных данных должны провести внеочередной антивирусный контроль.

5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусной защиты возлагается на администратора информационной системы персональных данных.

5.2. Ответственность за выполнение требований данной Инструкции возлагается на пользователей и администратора информационной системы персональных данных.

5.3. Периодический контроль за соблюдением положений данной инструкции возлагается на администратора информационной системы персональных данных.