Приложение № 10

к приказу руководителя комитета труда и социальной защиты населения администрации города Ставрополя
от «__»_____ 20__ г. № ___

И Н С Т Р У К Ц И Я
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ КОМИТЕТА ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ АДМИНИСТРАЦИИ ГОРОДА СТАВРОПОЛЯ

г. Ставрополь

СПИСОК СОКРАЩЕНИЙ

ИСПДн	Информационная система персональных данных
ИБ	Информационная безопасность
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
САЗ	Система антивирусной защиты
СВТ	Средства вычислительной техники

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по организации антивирусной защиты информационных систем персональных данных комитета труда и социальной защиты населения администрации города Ставрополя (далее – Комитет) определяет требования к организации защиты информационных систем персональных данных (далее ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО) и устанавливает ответственность руководителей и сотрудников отделов Комитета, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников отделов Комитета, использующих в работе ИСПДн Комитета.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые Администратором безопасности ИСПДн семинары и персональные инструктажи (при необходимости) пользователей ИСПДн Комитета.

1.4. Доведение Инструкции до сотрудников Комитета в части их касающейся осуществляется Администратором безопасности ИСПДн под роспись в журнале или на самом документе.

1.5. В случае невозможности исполнения требований настоящей Инструкции в полном объеме, например:

- в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;
- злоумышленных действий,

практическая «глубина» исполнения настоящей Инструкции определяется Администратором безопасности ИСПДн по согласованию с ответственным за обеспечение безопасности ПДн Комитета.

2. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

2.4. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн Комитета».

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. ФУНКЦИИ АДМИНИСТРАТОРА ИСПДН ПО ОБЕСПЕЧЕНИЮ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ

Администратор безопасности ИСПДн обязан:

3.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. При необходимости производить обновление антивирусных программных средств.

3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.

3.6. При необходимости разрабатывать инструкции по работе пользователей с программными средствами САЗ.

3.7. Проводить работы по обнаружению и обезвреживанию вирусов.

3.8. Участвовать в работе комиссии по расследованию причин заражения ПЭВМ и серверов.

3.9. Хранить эталонные копии антивирусных программных средств.

3.10. Осуществлять периодический контроль за соблюдением пользователями ПЭВМ требований настоящей Инструкции;

3.11. Разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации.

3.12. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПЭВМ (серверах).

4. ФУНКЦИИ ПОЛЬЗОВАТЕЛЕЙ

Пользователи ИСПДн:

4.1. Получают по ЛВС или от Администратора безопасности ИСПДн носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.2. Проводят обновления антивирусных баз на ПЭВМ (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.3. 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.) сотрудник подразделения самостоятельно или вместе с администратором безопасности ИСПДн должен провести внеочередной антивирусный контроль ПЭВМ. При необходимости он должен привлечь Администратора безопасности ИСПДн для определения факта наличия или отсутствия компьютерного вируса.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя отдела Комитета и Администратора безопасности ИСПДн, а также смежные отделы, использующие эти файлы в работе;
- провести анализ необходимости дальнейшего использования зараженных вирусом файлов;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь Администратора безопасности ИСПДн);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору безопасности ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору безопасности ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

5. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

5.1. Инструкция подлежит полному пересмотру в случае приобретения Комитетом новых средств защиты, существенно изменяющих порядок работы с ними.

5.2. В остальных случаях Инструкция подлежит частичному пересмотру.

5.3. Полный пересмотр данной Инструкции проводится с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Комитета.

5.4. Изменения в Инструкции (сведения о них) фиксируется в листе регистрации изменений (Приложение 2).

5.5. Вносимые изменения не должны противоречить другим положениям Инструкции. При получении изменений к данному Инструкции, руководители отделов Комитета в течение трех рабочих дней вносят свои предложения и/или замечания к поступившим изменениям.

6. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

6.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Комитета.

6.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на Администратора безопасности ИСПДн.

6.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн Комитета.

ПРИЛОЖЕНИЕ 1 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

ЛИСТ № _____ регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Лист ознакомления
с «Инструкцией по организации антивирусной защиты информационных систем персональных данных Комитета труда и социальной защиты населения администрации города Ставрополя»

№ п/п	Фамилия И.О. сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении