Приложение 6

к Положению информационной

безопасности об организации

и обеспечении безопасности

персональных данных в администрации

Нефтекумского муниципального округа

Ставропольского края

ИНСТРУКЦИЯ

по организации антивирусной защиты информационных систем персональных данных в администрации Нефтекумского муниципального округа Ставропольского края

1. Общие положения

Инструкция по организации антивирусной защиты информационных систем (далее - Инструкция) в администрации Нефтекумского муниципального округа Ставропольского края (далее по тексту - Администрации НМО СК), определяет требования к организации защиты информационных систем персональных данных (далее - ИСПДн) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность начальников отделов, руководителей отраслевых (функциональных органов) и работников, эксплуатирующих и сопровождающих информационную систему, за их выполнение.

Требования настоящей Инструкции распространяются на всех должностных лиц и работников Администрации НМО СК, использующих в работе ИСПДн Администрации НМО СК в целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые ответственным за обеспечение безопасности персональных данных в Администрации НМО СК семинары и персональные инструктажи (при необходимости) пользователей ИСПДн Администрации НМО СК.

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.

в случае программно-технических особенностей эксплуатируемых СВТ и/или ИСПДн.

Практическая "глубина" исполнения настоящей Инструкции в ИСПДн определяется Администратором ИБ по согласованию с ответственным за обеспечение безопасности обработки персональных данных.

2. Применение средств антивирусного контроля

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

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

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).

Обновление антивирусных баз должно проводиться регулярно, с периодичностью выпуска соответствующих обновлений производителем антивирусного программного обеспечения.

3. Функции работников, обеспечивающих работу САЗ

3.1. Администратор ИСПДн выполняет следующие функции:

по необходимости проводит инструктажи операторов ИСПДн по вопросам применения средств антивирусной защиты;

настраивает параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств;

предварительно проверяет устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов;

при необходимости производит обновление антивирусных программных средств;

производит получение и рассылку (при необходимости) с помощью почтовой системы и ЛВС обновлений антивирусных баз;

при необходимости разрабатывает инструкции по работе пользователей с программными средствами САЗ;

проводит работы по обнаружению и обезвреживанию вирусов;

при обнаружении программ типа "троянский конь", "логическая бомба" и т.п. немедленно ставит в известность ответственного за обеспечение безопасности персональных данных в Администрации НМО СК, а также администратора ИБ;

участвует в работе комиссии по расследованию причин заражения ПЭВМ и серверов;

хранит эталонные копии антивирусных программных средств и антивирусных баз.

3.2. Администратор ИБ выполняет следующие функции:

осуществляет периодический контроль за соблюдением пользователями ПЭВМ, а также администраторами ИСПДн требований настоящей Инструкции;

при необходимости проводит инструктаж пользователей ПЭВМ по работе с программными средствами САЗ;

участвует в разработке инструкций по функционированию системы антивирусной защиты информации;

проводит периодический контроль работы программных средств системы антивирусной защиты информации на ПЭВМ (серверах);

при необходимости участвует в работах по обнаружению и обезвреживанию вирусов;

участвует в работе комиссии по расследованию причин заражения ПЭВМ и серверов;

проводит анализ журналов антивирусной проверки ПЭВМ средствами централизованного контроля;

проводит ежемесячный анализ журналов антивирусной проверки ПЭВМ программными средствами САЗ на ПЭВМ не имеющих средств централизованного контроля;

проводит контроль настроек антивирусных средств.

3.3. Ответственный за обеспечение безопасности персональных данных в Администрации НМО СК выполняет следующие функции:

организует эксплуатацию программных средств системы антивирусной защиты информации на ПЭВМ (серверах);

организует антивирусный контроль информации, включая информацию поступающую из других подразделений и сторонних организаций на магнитных носителях или по электронной почте;

контролирует исполнение должностных обязанностей администратора ИБ и администраторов ИСПДн.

4. Функции пользователей (операторов)

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

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

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники администрации НМО СК обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов начальника отдела и администратора ИСПДн, владельца зараженных файлов;

совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора ИСПДн);

по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИСПДн и Администратору ИБ, 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

Инструкция подлежит полному пересмотру в при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Администрации НМО СК приводящих к существенным изменениям технологии обработки информации.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности персональных данных в Администрации НМО СК с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Администрации НМО СК.

Частичный пересмотр данного документа проводится ответственным за обеспечение безопасности персональных данных в Администрации НМО СК в остальных случаях с обязательным указанием оснований и внесенных изменений в "[Листе](#P7920) регистрации изменений в Инструкции" (Приложение 1) без переутверждения всей Инструкции.

Вносимые изменения не должны противоречить другим положениям Инструкции.

6. Ответственные за не выполнение инструкции

Ответственным за постоянный контроль выполнения требований данной Инструкции является:

Ответственный за обеспечение безопасности персональных данных в Администрации НМО СК.

Администратор ИБ.

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на Администратора ИСПДн и работников.

Приложение 1

к инструкции

по организации антивирусной защиты

информационных систем персональных данных

в администрации Нефтекумского муниципального округа

Ставропольского края

Лист

регистрации изменений в инструкции

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N п.п | Дата | Внесенное изменение | Основание (наименование, N и дата документа) | Кем внесено изменение (должность, подпись) |
|  |  |  |  |  |