АДМИНИСТРАЦИЯ ТРОИЦКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЧЕЛЯБИНСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 22.09.2017 № 627р

Об утверждении инструкции по организации антивирусной защиты в информационной системе персональных данных администрации Троицкого муниципального района

В целях исполнения Федерального закона от 27 июля 2006 года № 152 – ФЗ «О персональных данных», в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 01 ноября 2012 года № 1119:

1. Утвердить прилагаемую инструкцию по организации антивирусной защиты в информационной системе персональных данных администрации Троицкого муниципального района.
2. Контроль за исполнением настоящего распоряжения возложить на управляющего делами администрации Троицкого муниципального района Валееву Э.Ш.

Глава администрации
Троицкого муниципального района Л.В. Шаталова

УТВЕРЖДЕНА
Распоряжением администрации
Троицкого муниципального района
от «22.09.2017г.» № 627-р

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационной системе персональных данных администрации Троицкого муниципального района

1. Общие положения

1.1. Данная инструкция определяет требования к организации защиты в информационной системе персональных данных (далее – ИСПДн) администрации Троицкого муниципального района (далее – Администрация) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносного ПО), устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. К использованию в Администрации допускаются только лицензионные и сертифицированные Федеральной службой по техническому и экспортному контролю средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на компьютерах (серверах локальной вычислительной сети ИСПДн Администрации) осуществляется администратором безопасности ИСПДн, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов локальной вычислительной сети – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов автоматизированных рабочих мест (далее – АРМ).

2.2. 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. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием, отправкой или записью на съемный носитель.

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором безопасности ИСПДн на предмет отсутствия вредоносного ПО. Непосредственно после установки

(изменения) программного обеспечения должна быть выполнена антивирусная проверка:

2.4.1. На защищаемых серверах и АРМ – администратором безопасности ИСПДн.

2.4.2. На других серверах и АРМ ИСПДн Администрации, не требующих защиты, – лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем начальника данного отдела или сотрудника, им уполномоченного.

2.5. При возникновении подозрения на наличие вредоносного ПО (ошибки в работе программ, появление графических и звуковых эффектов, искажения данных, пропадание файлов, частое появление сообщений о системных ошибках, замедление работы компьютера и т.п.) сотрудник самостоятельно или вместе с администратором безопасности ИСПДн должен провести внеочередной антивирусный контроль своего АРМ. При необходимости привлечь ответственного за обеспечение безопасности персональных данных для определения им факта наличия или отсутствия вредоносного ПО.

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

2.6.1. Приостановить работу.

2.6.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе.

2.6.3. Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

2.6.4. Провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за обеспечение безопасности персональных данных).

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в ИСПДн Администрации в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИСПДн.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на администратора безопасности ИСПДн и всех сотрудников, являющихся пользователями ИСПДн Администрации.

3.3. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а так же проверка работоспособности программы) в ИСПДн Администрации, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками Администрации осуществляется администратором безопасности ИСПДн.

Управляющий делами администрации
Троицкого муниципального района Э.Ш. Валеева