Приложение № 10

Утверждено

постановлением Администрации

Ельцовского района

от 07.10.2024 № 220

Инструкцияпо организации антивирусной защиты в информационных системах персональных данных Администрации Ельцовского района Алтайского края

* + - 1. Общие положения.

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты в информационных системах персональных данных (далее - ИСПДн) Администрации Ельцовского района Алтайского края (далее – Администрация) и устанавливает ответственность за их выполнение.

* + - 1. Основные определения.

Вредоносное программное обеспечение (далее ПО) - специально разработанное программное обеспечение, программный модуль, блок, группа команд, имеющая способность к самораспространению, которая может попадать в общее и специальное программное обеспечение ИСПДн и приводить к:

* дезорганизации вычислительного процесса (нарушению или существенному замедлению обработки информации);
* модификации или уничтожению программ, или данных;
* приведению в негодность носителей информации и других технических средств;
* нарушению функционирования средств защиты информации.
  1. Инструкция по применению средств антивирусной защиты.

Защита ПО ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

* К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.
* Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах Администрации (далее – Ответственный).
* Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
* Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль, осуществляемый Ответственным.
* Средства антивирусной защиты устанавливаются на всех рабочих станциях сотрудников Администрации.
* Еженедельно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций сотрудников Администрации.
* Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
* Контроль входящей информации необходимо проводить непосредственно после ее приема.
* Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
* Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
* 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.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции и обратиться к Ответственному.
* В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:
* приостановить работу;
* немедленно поставить в известность Ответственного о факте обнаружения вируса;
* провести лечение зараженных файлов;
* в случае невозможности лечения обратиться к Ответственному.
* По факту обнаружения зараженных вирусом файлов Ответственный должен составить служебную записку на имя главы района, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.
* Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
* Настройка параметров средств антивирусной защиты осуществляется Ответственным, в соответствии с руководствами по применению конкретных антивирусных средств.