Приложение № 7

к распоряжению главы

городского округа Истра

от 18.08.2021 № 251-Р

**Инструкция**

**по организации антивирусной защиты**

**в сегменте «Истра-2» государственной информационной системы «Единая информационная система оказания государственных и муниципальных услуг Московской области»**

**1. Общие положения**

1. Настоящая инструкция определяет требования к организации антивирусной защиты в сегменте «Истра-2» государственной информационной системы «Единая информационная система оказания государственных и муниципальных услуг Московской области» администрации городского округа Истра (далее – Сегмент ЕИСОУ) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность государственных гражданских служащих, эксплуатирующих и сопровождающих Сегмент ЕИСОУ, за их выполнение.
2. В Сегменте ЕИСОУ к использованию допускаются только лицензионные антивирусные средства прошедшие, в установленном порядке, процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.
3. Под антивирусным средством в данной инструкции понимается специализированное программное средство защиты информации, предназначенное для обнаружения фактов вирусного воздействия на компоненты вычислительной техники объектов информатизации.
4. Администрирование и обновление автономных клиентов антивирусной защиты производятся администратором информационной безопасности информационных систем и информационных систем персональных данных Сегмента ЕИСОУ.
5. Обновление антивирусных баз должно производиться ежедневно.
6. Ответственность за организацию и установление порядка проведения антивирусной защиты в Сегменте ЕИСОУ возлагается на администратора информационной безопасности информационных систем и информационных систем персональных данных Сегмента ЕИСОУ.
7. Ответственность за выполнение положений данной Инструкции возлагается на ответственного за защиту персональных данных Сегмента ЕИСОУ и администратора информационной безопасности информационных систем и информационных систем персональных данных Сегмента ЕИСОУ.
8. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая от сторонних лиц и организаций.
9. Устанавливаемое системное и прикладное программное обеспечение на средствах вычислительной техники должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на ПЭВМ лицом, установившим (изменившим) программное обеспечение.
10. При работе с машинными носителями информации, полученными из сторонних организаций, пользователи на рабочих местах обязаны перед началом работы с машинными носителями информации проверить их на наличие компьютерных вирусов.
11. При возникновении подозрения наличия компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, исчезновение файлов, частое появление сообщений о системных ошибках и т.п.) пользователей Сегмента ЕИСОУ должны самостоятельно провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь системного администратора Сегмента ЕИСОУ (или сотрудника организации, с которой у Сегмента ЕИСОУ заключено соглашение на оказание услуг по системному администрированию Сегмента ЕИСОУ) либо администратора информационной безопасности информационных систем и информационных систем персональных данных Сегмента ЕИСОУ для определения им факта наличия или отсутствия компьютерного вируса.
12. В случае обнаружения компьютерного вируса пользователи Сегмента ЕИСОУ обязаны:

- приостановить работу на ПЭВМ;

- немедленно поставить в известность о факте обнаружения файлов, зараженных вирусом, руководителя подразделения и администратора информационной безопасности информационных систем и информационных систем персональных данных Сегмента ЕИСОУ, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

- провести «лечение» зараженных вирусом файлов штатными антивирусными средствами;

- при невозможности «лечения» уничтожить зараженные вирусом файлы способом, исключающим их восстановление.

1. В случае обнаружения на съемных носителях нового вируса, не поддающегося «лечению», пользователь Сегмента ЕИСОУ, обязан запретить их использование и поставить в известность администратора информационной безопасности информационных систем и информационных систем персональных данных Сегмента ЕИСОУ.
2. Ответственные за обеспечение безопасности информации проводят периодическое (не реже 1 раза в неделю) полное тестирование компьютера на вирусы.