Приложение 2

УТВЕРЖДЕНА
решением Пелымской
поселковой территориальной
избирательной комиссии
от 27 июня 2025 г. № 4/19

ИНСТРУКЦИЯ
по организации антивирусной защиты в Пелымской поселковой территориальной избирательной комиссии

1. Общие положения

Настоящая Инструкция по организации антивирусной защиты (далее – Инструкция) разработана в соответствии со ст. 18.1 Федерального закона № 152-ФЗ «О персональных данных» и определяет порядок реализации антивирусного контроля в информационных системах персональных данных (далее – ИСПДн) Пелымской поселковой территориальной избирательной комиссии (далее – Комиссия).

Действие настоящего документа распространяется на всех работников Комиссии, выполняющих обработку персональных данных (далее – ПДн) в ИСПДн, и на администратора ИСПДн.

Непосредственное руководство проведением работ по антивирусной защите осуществляет специалист информационного управления, назначенный Администратором безопасности.

Ответственность за проведение мероприятий антивирусного контроля в Комиссии, выполнение мероприятий по антивирусной защите ПДн на эксплуатируемых средствах вычислительной техники возлагается на администратора ИСПДн.

Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты ПДн и требований настоящей Инструкции несут работники, за которыми закреплены соответствующие рабочие станции.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в три года.

2. Правила проведения антивирусного контроля

В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на рабочих станциях.

В случае если пользователю ИСПДн разрешено применение съемных машинных носителей информации, он обязан перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.

Ярлык для запуска антивирусной программы должен быть вынесен на «Рабочий стол» операционной системы.

При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Администратора ИСПДн или Администратора безопасности и прекратить какие-либо действия с информационными ресурсами в ИСПДн.

Администратор безопасности проводит расследование факта заражения ИСПДн компьютерным вирусом. Лечение зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы, после этого вновь проводится антивирусный контроль.

Обо всех фактах заражения Администратор ИСПДн обязан ставить в известность Администратора безопасности.

Установка и настройка параметров средств антивирусного контроля на средствах вычислительной техники ИСПДн осуществляется в соответствии с программной и эксплуатационной документацией, поставляемой вместе с ними.

Обязательному входному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, входящие в состав ИСПДн, программные средства общего и специального назначения, любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по каналам передачи данных, а также информация на съемных носителях (CD-ROM, Flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед ее отправкой (записью на съемный носитель).

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

Периодическая проверка жестких магнитных дисков на отсутствие программных вирусов должна проводиться не реже одного раза в неделю. Обязательная проверка используемых в работе съемных носителей должна осуществляться перед началом работы с ними.

При повреждении программных средств и информационных массивов программными вирусами должны выполняться мероприятия по восстановлению их работоспособности.

3. Правила обновления баз данных вирусных описаний

Обновление баз данных вирусных описаний средств антивирусной защиты, используемых для защиты рабочих станций, а также периметральных средств защиты информации (средств межсетевого экранирования при наличии технической возможности установки антивирусной программы на данные средства) должно осуществляться в автоматическом режиме, без участия пользователей.

Процедура обновления антивирусных баз должна проводиться не реже одного раза в неделю.

4. Правила проведения антивирусной проверки

Установка (изменение) системного и прикладного программного обеспечения должна осуществляться в соответствии с программной и эксплуатационной документацией, поставляемой вместе с ним. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором ИСПДн или Администратором безопасности. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена полная антивирусная проверка компьютера Администратором ИСПДн или Администратором безопасности.

Сканирование рабочих станций пользователей средствами антивирусной защиты производится централизовано, не реже одного раза в неделю.

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 самостоятельно или совместно с Администратором ИСПДн или Администратором безопасности должен провести внеочередной антивирусный контроль своего персонального компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- принять меры по локализации программного вируса (отключить персональный компьютер от локальной вычислительной сети);
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора ИСПДн или Администратора безопасности, руководителя, владельца зараженных файлов, а также других пользователей, использующих эти файлы в работе;
- совместно с Администратором ИСПДн или Администратором безопасности и владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- по возможности провести лечение зараженного файла. В случае невозможности вылечить зараженный файл, необходимо поместить его в карантин, и выполнить процедуру по восстановлению незараженной копии исходного файла из имеющегося архива.

В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, Администратор ИСПДн или Администратор безопасности должен:

- заархивировать зараженные файлы с внедренными программными вирусами и направить данный архив в организацию, с которой заключен договор технической поддержки эксплуатации средств антивирусной защиты (при необходимости, для выполнения требований данного пункта привлечь специалиста по защите информации);

- при необходимости осуществить переустановку программного обеспечения на зараженном компьютере.

По факту обнаружения зараженных вирусом файлов Администратор безопасности должен составить в адрес председателя Комиссии служебную записку, 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.