АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
«ХИСЛАВИЧСКИЙ МУНИЦИПАЛЬНЫЙ ОКРУГ»
СМОЛЕНСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

23.06.2025 П-612

Об утверждении Положения об организации антивирусной защиты в Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области

В соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с целью организации антивирусной защиты Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области,

Администрация муниципального образования «Хиславичский муниципальный округ» Смоленской области п о с т а н о в л я е т:

1. Утвердить Положение об организации антивирусной защиты в Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области (приложение №1).

Глава муниципального образования
«Хиславичский муниципальный округ»
Смоленской области **С.А. Шапкин**

Документ подписан
электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 00AE011655ED4F585324B47EB530FB1139
Владелец: Шапкин Сергей Александрович
Действителен с 13-01-2025 до 08-04-2026

Приложение №1
к постановлению Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области
от 23.06.2025 № П-612

ПОЛОЖЕНИЕ
об организации антивирусной защиты в Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области

I. Общие положения.

Настоящее Положение разработано в целях осуществления антивирусной защиты информационных ресурсов, определения системы мер, направленных на защиту информационных систем в Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области (далее – Администрация) от несанкционированного копирования, модификации и разрушения, а также нарушения работы программного обеспечения (далее – ПО) Администрации при воздействии вирусов и других вредоносных программ.

Настоящее Положение определяет порядок применения средств антивирусной защиты в Администрации, задачи, обязанности, права и ответственность пользователей средств антивирусной защиты, порядок установки, обновления и применения средства антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов и других вредоносных программ.

Требования настоящего Положения обязательны для выполнения всеми лицами, использующими средства компьютерной техники Администрации, входящие в сегмент РМС СО (далее – устройства подсети).

II. Цель организации антивирусной защиты.

Целью организации антивирусной защиты является:

– защита информационных ресурсов Администрации от несанкционированного копирования, искажения и разрушения;
– минимизация риска сбоев и отказов в работе технологических и информационных процессов, при воздействии вирусов и других вредоносных программ;
– минимизация финансовых потерь и трудовых затрат при устранении последствий воздействия вредоносного кода.

III. Основные требования к системе антивирусной защиты.

Основными требованиями к системе антивирусной защиты являются:

– решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие только конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего неизвестно;

– решение задачи антивирусной защиты должно осуществляться в реальном времени.

Мероприятия, направленные на решение задач по антивирусной защите:

– установка только лицензированного антивирусного программного обеспечения российского производства;

– регулярное обновление и регулярные профилактические проверки;

– непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИС;

– ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в информационных системах (далее – ИС) операционного программного обеспечения и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб;

– проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;

– проведение регулярных проверок целостности критически важных программ и данных;

– внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

– необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

Во избежание заражения ИС вредоносным ПО всем пользователям необходимо соблюдать следующие правила:

- В случае сомнений в наличии или в корректной работе на компьютере антивирусного ПО необходимо незамедлительно сообщить об этом непосредственному руководителю.

- Никогда не открывайте никакие файлы, находящиеся во вложениях к электронным письмам, которые отправлены с подозрительных или неизвестных Вам адресов. Не пересылайте их другим адресатам. В случае получения таких писем следует немедленно их удалить из папки «Входящие», а затем удалить их из папки «Удаленные» для того, чтобы исключить возможность их восстановления.

- В случае возникновения подозрений на наличие зараженных файлов во вложениях к сообщениям электронной почты (к примеру, подозрительные имена или расширения файлов вложений, подозрительный источник сообщения, неизвестный отправитель с адресом электронной почты публичного почтового сервиса), которые, при этом, могут быть полезны, необходимо незамедлительно сообщить об этом специалисту по защите информации для проведения проверки подозрительного сообщения.

- Запрещается загружать файлы и соглашаться на предложения загрузить или установить программное обеспечение из непроверенных источников.

- Следует избегать использования на рабочих местах съемных носителей информации без служебной необходимости, особенно если эти носители получены из неизвестных или подозрительных источников или могли использоваться на других компьютерах, потенциально незащищенных антивирусными программами. Допускается самостоятельно осуществлять антивирусные проверки при помощи штатного антивирусного программного обеспечения, установленного на рабочих местах.

- Для совместной работы или хранения важной, конфиденциальной информации, рекомендуется использовать сетевые ресурсы на файловом хранилище, специально для этого предназначенные. В случае появления сообщений антивирусного программного обеспечения об обнаружении угрозы необходимо убедиться, что угроза успешно предотвращена.

При заражении компьютера вредоносным ПО характерны следующие признаки:

– значительное увеличение времени отклика компьютера на Ваши действия в любых программах;
– появление сообщений об ошибках;
– необъяснимая потеря файлов, изменение дат обновления и увеличение размера файлов;
– системные сбои (включая случаи, когда операционная система перестает загружаться);
– любые другие необычные явления в работе компьютера.

В случае возникновения подозрений в заражении компьютера вирусом сотрудник структурного подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения должен провести внеочередной антивирусный контроль на своем рабочем месте. При необходимости привлечь ответственного за защиту информации в Администрации для определения им факта наличия или отсутствия компьютерного вируса.

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

– приостановить работу;
– немедленно поставить в известность о факте обнаружения зараженных вирусами файлов руководителя и ответственного за обеспечение информационной безопасности своего подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
– совместно с владельцем зараженных вирусами файлов провести анализ необходимости дальнейшего их использования;
– провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за защиту информации в Администрации);
– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе ответственному за защиту информации в Администрации для дальнейшей отправки его в отдел защиты информации Министерства цифрового развития Смоленской области; по факту обнаружения зараженных вирусом файлов составить служебную записку отделу защиты информации Министерства цифрового развития Смоленской области, 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.

Пользователю средствами антивирусной защиты запрещается отключать средства антивирусной защиты информации.

Каждый работник Администрации несет ответственность за невыполнение или недобросовестное выполнение перечисленных выше обязанностей.

IV. Порядок применения средств антивирусной защиты информации.

Средства антивирусной защиты устанавливаются на всех средствах вычислительной техники, эксплуатируемой в Администрации.

Все средства антивирусной защиты работают в режиме мониторинга в реальном времени. Проверяются все файлы на локальных и сетевых жестких дисках, съемных

носителях, в приложениях к письмам электронной почты, загружаемые из Интернета и др. Не допускается отключение работы средства антивирусной защиты.

Производится еженедельная полная проверка жестких дисков и твердотельных накопителей.

В случае подозрения на наличие вредоносных программ проводится внеплановая проверка жестких дисков и съемных носителей.

Обновление антивирусных баз производится автоматически. Не допускается отключение автоматического обновления средства антивирусной защиты.

Выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на устройствах подсети, а также проверки на отсутствие вредоносного кода после установки или изменения программного обеспечения.

При обнаружении вредоносного кода средства антивирусной защиты должны немедленно известить об этом пользователя и удалить вредоносный код или заблокировать его работу.

V. Порядок инсталляции и настройки средств антивирусной защиты информации.

Установка средств антивирусной защиты на компьютерах, серверах и рабочих станциях осуществляется уполномоченным сотрудником Администрации.

Инсталляция и настройка средства антивирусной защиты производится в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

После инсталляции средства антивирусной защиты конфигурируются в соответствии со следующими требованиями:

– загрузка средства антивирусной защиты должна выполняться автоматически при включении компьютера;
– средство антивирусной защиты должно постоянно работать в режиме фонового монитора;
– периодически средство антивирусной защиты должно запускаться на сканирование всех жестких дисков;
– обновление антивирусных баз производится автоматически;
– при обнаружении вируса пользователь должен быть немедленно извещен об этом антивирусной программой;
– протоколы работы средства антивирусной защиты должны храниться не менее 30 суток.

Каждый компьютер, работающий в Администрации, должен быть настроен следующим образом:

- отключена функция автозапуска съемных носителей;
- настроено автоматическое обновление операционной системы;
- пользователь в домене не должен иметь администраторских прав на локальном компьютере.

При технологической необходимости на отдельные устройства подсети средства антивирусной защиты могут быть настроены иным образом.

VI. Ответственность

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем подсистему АС, в соответствии с требованиями настоящего Положения возлагается на руководителя подразделения.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящего Положения возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями АС.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Положения сотрудниками подразделений организации осуществляется ответственным за защиту информации.

VII. Заключительные положения.

Положение вступает в силу с момента его утверждения.