УТВЕРЖДЕН
распоряжением администрации
округа «Усинск»
от 11 июня 2025 г. № 103-р
(приложение № 3)

РЕГЛАМЕНТ
настройки и эксплуатации системы антивирусной защиты

1. Общие положения

1.1. Регламент настройки и эксплуатации системы антивирусной защиты (далее – Регламент) разработан в целях обеспечения безопасности персональных данных, обрабатываемых в администрации муниципального округа «Усинск» Республики Коми (далее – Администрация) с использованием средств автоматизации в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказом ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Целью Регламента является регулирование использования средств антивирусной защиты в Администрации, а также определение стандарта настройки антивирусной защиты для рабочих станций и серверов Администрации.

2. Основные требования и ответственные лица

2.1. Основные требования к системе антивирусной защиты:

2.1.1.На каждом сервере и всех рабочих станциях должна быть установлена система антивирусной защиты.

2.1.2.Должна быть настроена проверка средством антивирусной защиты всех электронных сообщений (e-mail) и вложений к ним.

2.1.3.Должно быть обеспечено автоматическое обновление вирусных баз антивирусной защиты не реже чем 1 (один) раз в 3 (три) часа.

2.1.4.Должен быть организован централизованный мониторинг и управление всеми средствами антивирусной защиты серверов и рабочих станций.

2.1.5.Должно быть организовано оповещение ответственных лиц об обнаружении вирусов и других событиях в работе антивирусной защиты.

2.1.6.Для защиты доступа к настройкам антивирусной защиты на автоматизированном рабочем месте пользователей должен быть использован пароль защиты, выбираемый в соответствии с инструкцией по организации парольной защиты.

3. Используемые аппаратные средства и программное обеспечение

3.1. Для антивирусной защиты рабочих станций под управлением операционной системы семейства Windows используется Kaspersky Endpoint Security.

4. Требования и рекомендации по настройке аппаратных средств и программного обеспечения

4.1.Перед инсталляцией Kaspersky Endpoint Security необходимо удалить все прочее антивирусное программное обеспечение, включая старые версии.

4.2.Основной контроллер домена должен иметь выход в сеть Интернет.

4.3.На рабочей станции ответственного лица должен быть установлен Агент администрирования и Kaspersky Endpoint Security.

4.4.На серверах установить Kaspersky Endpoint Security for Windows Server, а на рабочих станциях установить Kaspersky Endpoint Security.

4.5.Не рекомендуется применять дистанционную установку для серверов.

4.6.Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

4.7.В свойствах подключения по локальной сети удаленного клиента должны быть активны Клиент для сетей Microsoft и Служба доступа к файлам и принтерам сетей Microsoft.

4.8.Убедиться, что Ваши имя и пароль установлены для доступа ко всем Вашим серверам и рабочим станциям – рекомендуется использовать учетную запись с правами администратора домена.

4.9.Службы Remote Registry и Remote Procedure Call на серверах и рабочих станциях должны запускаться автоматически.

4.10.Параметры типовой настройки защиты для рабочих станций приведены в приложении 1 к настоящему Регламенту.

4.11.Параметры настройки защиты для серверов приведены в приложении 2 к настоящему Регламенту.

Приложение 1
к Регламенту настройки и эксплуатации
системы антивирусной защиты

Настройки параметров защиты для рабочих станций

1.Типовые параметры настройки области защиты антивируса для рабочих станций должны контролироваться:

- оперативная память компьютера и активность запущенных приложений.

2.Полная проверка локальных дисков компьютера должна проводиться 1 (один) раз в месяц с низким приоритетом процесса сканирования.

3.Сетевые диски должны быть исключены из области контроля.

4.При запуске антивируса должна проводиться проверка объектов автозапуска.

Приложение 2
к Регламенту настройки и эксплуатации
системы антивирусной защиты

Настройки параметров защиты для серверов

1.В связи с высокой нагрузкой на сервера и особенностями данных, обрабатываемых серверами, производится дополнительная настройка области защиты антивируса на серверах.

2.Должен проводиться постоянный контроль оперативной памяти компьютера и активность запущенных приложений.

3.Полная проверка жестких дисков должна проводиться исключительно в ночное время 1 (один) раз в месяц.

4.При запуске антивируса должна проводиться проверка объектов автозапуска.

5.В случае установки антивируса на сервер электронной почты удалить из сканирования в режиме реального времени файлы с расширениями: EDB, EML и TMP.

6.При настройке антивируса на сервере управления базами данных сами файлы баз данных должны быть исключены из области сканирования.