Утверждено приказом
Главного врача
Республиканского Центра СПИД
От «10» января 2023 г. № ___
_____/Санчы И.Д./

Инструкция
по организации антивирусной защиты в информационных системах Государственного бюджетного учреждения здравоохранения Республики Тыва «Республиканский Центр по профилактике и борьбе со СПИД и инфекционными заболеваниями» (Республиканский Центр СПИД)

г. Кызыл
2023 год

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты информационных систем Республиканского Центра СПИД от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Республиканского Центра СПИД, эксплуатирующих и сопровождающих информационные системы, за выполнение требований настоящей Инструкции.

1.2. Для обеспечения информационной безопасности к использованию в ИС Республиканского Центра СПИД допускаются только лицензионные и сертифицированные ФСБ России и ФСТЭК России антивирусные средства, закупленные у официальных разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля, контроль за состоянием антивирусной защиты в ИС Республиканского Центра СПИД осуществляется администратором информационной безопасности, в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. После установки и настройки средств антивирусного контроля администратором информационной безопасности в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.

1.5. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

1.6. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИС Республиканского Центра СПИД и своевременное информирование администратора информационной безопасности в случае обнаружения действий вредоносных программ возлагается на сотрудников Республиканского Центра СПИД.

2. Применение средств антивирусного контроля

2.1. Обязательному антивирусному контролю подлежат все рабочие станции (далее – РС) сотрудников Республиканского Центра СПИД, а также любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

2.2. Антивирусный контроль рабочих станций сотрудников Республиканского Центра СПИД должен проводиться ежедневно в автоматическом режиме при начальной загрузке РС (для серверов Республиканского Центра СПИД – при перезапуске).

2.3. Настройка средств антивирусной защиты должна реализовывать следующие функции:

– непрерывный автоматический мониторинг информационного обмена в ИС с целью выявления программно-математического воздействия (далее – ПМВ);

– автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИС всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

– реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

– автоматическая проверка критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы «system» и «system32» при каждом запуске операционной системы;

– полная автоматическая проверка носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю;

– регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты. Для чего администратором информационной безопасности должен быть организован доступ к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, ответственному специалисту необходимо один раз в неделю осуществлять установку пакетов обновлений вирусных баз, контроль их подключения к антивирусному пакету и проверку РС на наличие вирусов;

– автоматическое документирование состояния системы антивирусной защиты ИС.

2.4. Антивирусный контроль входящей информации (в т.ч. разархивирование) должен проводиться непосредственно после получения информации на выделенном автономном компьютере. Антивирусный контроль исходящей информации должен проводиться непосредственно перед отправкой (записью на съемный носитель).

2.5. Пользователи ИС Республиканского Центра СПИД при работе со съемными носителями информации (flash-накопители, CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ выполнив следующие действия:

- Подключить съемный носитель информации.
- Открыть значок Рабочего стола «Мой компьютер».
- Установить курсор мыши на имя выбранного носителя.
- По правой клавише мыши открыть контекстное меню Microsoft Windows и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

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

2.7. Установка (изменение) системного и прикладного программного обеспечения должна осуществляться только в присутствии администратора

информационной безопасности. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) системного программного обеспечения должна проводиться антивирусная проверка. В ИС Республиканского Центра СПИД запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

2.8. При возникновении подозрения на наличие в системе компьютерного вируса, (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) сотрудником Республиканского Центра СПИД должен быть проведён внеочередной антивирусный контроль рабочей станции (самостоятельно или вместе с администратором информационной безопасности). Для проведения контроля должны использоваться актуальные версии антивирусных сканеров (cureit, avz и др.), запускаемых без установки в системе.

2.9. В случае обнаружения при проведении антивирусной проверки наличия в системе компьютерного вируса сотрудники Республиканского Центра СПИД обязаны:

– немедленно поставить в известность администратора информационной безопасности и прекратить какие-либо действия на персональном компьютере приостановить работу;

– Поставить в известность владельца зараженных файлов.

2.10. В случае обнаружения наличия в системе компьютерного вируса необходимо:

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

– провести локализацию вируса в системе;

– обеспечить удаление вируса из системы;

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, необходимо направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку;

– по факту обнаружения вируса должна быть составлена служебная записка администратору информационной безопасности, в которой требуется указать предположительный источник (отправителя, владельца и т.д.) вируса, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.11. Пользователю ИС Республиканского Центра СПИД запрещается:

– использовать на СВТ съемные носители информации без предварительной проверки установленными средствами антивирусной защиты;

– запускать неизвестные приложения, пришедшие по электронной почте.

2.12. Пользователь обязан:

– ежедневно при начальной загрузке РС убедиться в наличии резидентного антивирусного монитора и в случае его отсутствия уведомить об этом администратора информационной безопасности;

– самостоятельно запускать внеплановую антивирусную проверку РС при получении уведомления о наличии в системе вируса, а также при возникновении подозрения на наличие вируса.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в Республиканском Центре СПИД, в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

3.2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности и всех сотрудников, являющихся пользователями ИС Республиканского Центра СПИД.

3.3. Периодический контроль за состоянием антивирусной защиты в Республиканском Центре СПИД, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками Республиканского Центра СПИД осуществляется администратором информационной безопасности.

3.4. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора информационной безопасности.

3.5. Сотрудники Республиканского Центра СПИД, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации

Разработал
Администратор информационной безопасности _____ / З.Н. Сандаков

«10» января 2023 г.