|  |
| --- |
| Утверждено приказом  главного врача ОГБУЗ «Братская городская больница № 2»  Гаськова А.Ю. |
| От « 26 » июля 2018 г. № 539-Р |

**Инструкция по организации антивирусной защиты в информационных системах в ОГБУЗ «Братская городская больница № 2»**

г. Братск

2018год

1. **Общие положения**
   1. Настоящая Инструкция определяет требования к организации защиты в информационных системах согласно перечню на основе программного обеспечения в информационных системах согласно перечнюот разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников организации, эксплуатирующих и сопровождающих в информационных системах согласно перечню за выполнение требований настоящей Инструкции.
   2. Для обеспечения информационной безопасности к использованию в информационных системах согласно перечню на основе программного обеспечения в информационных системахсогласно перечнюдопускаются только лицензионные исертифицированные ФСБ России и ФСТЭК Россииантивирусные средства, закупленные у официальных разработчиков (поставщиков) указанных средств.
   3. Установка и настройка средств антивирусного контроля,контроль за состоянием антивирусной защиты в информационных системах согласно перечню осуществляется администратором информационной безопасности, в соответствии с руководствами по применению конкретных антивирусных средств.
   4. После установки и настройки средств антивирусного контроля администратором информационной безопасности в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.
   5. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.
   6. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации в информационных системах согласно перечнюи своевременное информирование администратора информационной безопасности в случае обнаружения действий вредоносных программ возлагается на сотрудников организации.
2. **Применение средств антивирусного контроля**
   1. Обязательному антивирусному контролю подлежат все рабочие станции (далее - РС)в информационных системах согласно перечню, а также информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).
   2. Антивирусный контроль рабочих станцийв информационных системах согласно перечню должен проводиться ежедневно в автоматическом режиме при начальной загрузке РС.
   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.
  1. 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. Пользователи в информационных системах согласно перечнюпри работе со съемными носителями информации (flash-накопители, дискеты 3,5”, CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ.
  3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.
  4. 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.Вв информационных системах согласно перечнюзапрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.
  5. При возникновении подозрения на наличие в системе компьютерного вируса, (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) сотрудником организации 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, avzи др.), запускаемых без установки в системе
  6. В случае обнаружения при проведении антивирусной проверки наличия в системе компьютерного вируса сотрудники организации обязаны:
* немедленно поставить в известность администратора информационной безопасностии прекратить какие-либо действия на персональном компьютере приостановить работу;
* Поставить в известность владельца зараженных файлов.
  1. 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.

Пользователю в информационных системах согласно перечню запрещается:

* использовать на СВТ съемные носители информации без предварительной проверки установленными средствами антивирусной защиты;
* запускать неизвестные приложения, пришедшие по электронной почте.

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.

1. **Ответственность**
   1. Ответственность за организацию антивирусного контроля в организации, в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.
   2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности и всех сотрудников, являющихся пользователямив информационных системах согласно перечню.
   3. Периодический контроль за состоянием антивирусной защиты в в информационных системах согласно перечню области, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции пользователем в информационных системах согласно перечню осуществляется администратором информационной безопасности.
   4. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора информационной безопасности.
   5. Пользователи в информационных системах согласно перечню, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации