Государственное казенное учреждение здравоохранения
Детский санаторий «ТОПОЛЁК»
Министерства Здравоохранения Краснодарского края

УТВЕРЖДАЮ
Главный врач
ГКУЗ «Детский санаторий «Тополек»
_____ / М. А. Мугу /
«14» 12 2021 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

Настоящая Инструкция определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) ГКУЗ «Детский санаторий «Тополек» от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИСПДн ГКУЗ «Детский санаторий «Тополек», за их выполнение.

К использованию в ГКУЗ «Детский санаторий «Тополек» допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению комитетом информатизации и связи.

Установка и настройка средств антивирусного контроля на рабочих станциях ИСПДн ГКУЗ «Детский санаторий «Тополек» осуществляется уполномоченными лицами (лицензиатами Федеральной службы по техническому и экспортному контролю, имеющими разрешение на осуществление деятельности по технической защите конфиденциальной информации или уполномоченными ГКУЗ «Детский санаторий «Тополек» в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн ГКУЗ «Детский санаторий «Тополек».

2. Применение средств антивирусного контроля

Ежедневно в начале работы при загрузке компьютера (для серверов локальной вычислительной сети при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов рабочей станции.

Обязательному антивирусному контролю подлежит 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.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо «чистой» (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и 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.

Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн». Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором безопасности ИСПДн на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера

(локальной вычислительной сети), должна быть выполнена антивирусная проверка:

- на защищаемых серверах и рабочих станциях - ответственным за обеспечение информационной безопасности;

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

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.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения (технологического участка) должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь Администратора безопасности ИСПДн для определения ими 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 вирусом 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 вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь Администратора безопасности ИСПДн);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл Администратору безопасности ИСПДн и связи для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости, для выполнения требований данного пункта привлечь специалистов по защите информации сторонних организаций – лицензиатов ФСТЭК, имеющих разрешение на осуществление деятельности по технической защите конфиденциальной информации);
- по факту обнаружения зараженных вирусом файлов составить 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.

3. Ответственность

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем ИСПДн ГКУЗ «Детский санаторий «Тополек», в соответствии с требованиями настоящей Инструкции возлагается на Администратора безопасности.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников

подразделения, являющихся пользователями ИСПДн ГКУЗ «Детский санаторий «Тополек».

Периодический контроль за состоянием антивирусной защиты в ИСПДн ГКУЗ «Детский санаторий «Тополек», а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений ГКУЗ «Детский санаторий «Тополек» осуществляется Администратором безопасности и ответственными за обеспечение безопасности ИСПДн.