Наименование структурного подразделения:	**Все структурные подразделения**		
Названия документа:	**СОП «Инструкция по организации антивирусной защиты информационных систем»**		
Утвержден:	Руководитель ГКП на ПХВ «ЛГП» Чалкаров А.Б.		
Дата утверждения:			
Разработчик:	*Должность*	*Ф.И.О.*	*Подпись*
	Заместитель гл.врача по контролю качества мед.услуг	Рысбаев С.Т.	
	Программист	Сопов А. Сухинин А.	
Согласовано:	Заместитель гл.врача по лечебному делу	Анаркулова У.О.	
	Заместитель гл.врача по ОМД	Кабылбеков Г.К.	
	Врач эксперт		
Дата согласования:	04.01.2024г.		
Дата введения в действие	04.01.2024г.		
Версия №	**Копия №_____**	04 /01 / 2024г. Ф.И.О. _____ Подпись _____	

Дата последнего пересмотра «04» «01.» 2024г
Дата следующего пересмотра «_____» «_____» 2027г

1. СОДЕРЖАНИЕ

1. Область применения э
2. Нормативные ссылки 3
3. Определения, обозначения и сокращения 3
4. Общие положения 3
5. Требования 3
5.1 Установка и обновление антивирусных средств 3
5.2 Порядок проведения антивирусного контроля 4
5.3 Рекомендация по организации антивирусной безопасности на персональных компьютерах пользователей ИС (администраторов ИС) 4
5.4 Защита от злонамеренного и мобильного кода 4
6. Ответственность 5
7. Указание условий пересмотра СОП 5

1. Область применения

1.1 Настоящая Инструкция по организации антивирусной защиты серверов информационных систем (далее - Инструкция) определяет требования к организации антивирусной защиты серверов информационных систем (далее - ИС) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность работников ГКП на ПХВ "Ленгерская Городская Поликлиника " (далее Городская Поликлиника), ответственных за эксплуатацию системза обеспечение антивирусной безопасности ИС.

2. Нормативные ссылки

2.1 В настоящей Инструкции использованы ссылки на следующие нормативные документы:

1. Закон Республики Казахстан «Об информатизации» от 11 января 2007 года;
2. СТ РК 34.005-2002 Информационная технология. Основные термины и определения;
3. СТ РК 34.006-2002 Информационная технология. Базы данных. Основные термины и определения;
4. СТ РК 34.007-2002 Информационная технология. Телекоммуникационные сети. Основные термины и определения;
5. СТ РК ИСО/МЭК 27001-2008 Информационная технология. Методы и средства обеспечения безопасности системы управления информационной безопасностью. Требования.

3. Определения, обозначения и сокращения.

3.1. В настоящей Инструкции приведены следующие определения, обозначения и сокращения:

Администраторы ИС - Сотрудники, осуществляющие системно-техническое обслуживание программно-аппаратных средств и сопровождение ИС;
ИБ - Информационная безопасность;
ОС - Операционная система;
ИС - Информационные системы;
ПО - Программное обеспечение.

4. Общие положения

4.1 Настоящая ИНструкция содержит описание по организации антивирусной защиты ИС, направленных на поддерживание технического оборудования, прикладного программного обеспечения и программного обеспечения ИС в рабочем состоянии, а также обеспечения информационной безопасности ИС.
4.2 Настоящая Инструкция распространяется на администраторов ИС в Городской поликлиники.

5. Требования

5.1. Установка и обновление антивирусных средств.

1. К использованию на серверах ИС допускается толко лицезионные антивирусные средства, рекомендованные специалистами за информационную безопастность и за эксплуатацию систем, которые централизованно закуплены владельцем ИС у поставщиков указанных средств.
2. Антивирусные программы устанавливаются специалистами эксплуатации систремна сервера ИС.

Настройка антивирусных средств должна обеспечитвать:

1. При каждом перезапуске сервера ИС авоматический запуск антивирусного монитора;
2. По расписанию проводить полную антивирусную проверку (сканирование) локальных дисков сервера и дисковых массивов, подключенных к серверам;
3. Автоматическое обновление антивирусных баз по расписанию
4. Лечение зараженных вирусов файлов или удаление « по разрешению! При невозможности лечения.

В случае если невозможно настроить автоматическое обновление антивирусных баз, специалисту эксплуатации систем необходимо осуществлять обновление антивирусного ПО не менее двух раз в месяц, посредством копирования баз данных антивирусного ПО на сервера ИС.

5.2. Порядок проведения антивирусного контроля.

1. Устанавливаемое (изменяемое) на сервере ПО должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (Изменения) ПО, должна быть выполнена антивирусная проверка.
2. Обязательному антивирусному контролю подлежит любая информация (файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация со съемных носителей (USB накопители).
3. Контроль информации на съемных носителях производится непосредственно перед ее использованием.
4. В обязанности ответственных специалистов за эксплуатацию систем входит:
    1. установка антивирусных программ на сервера ИС;
    2. предварительнаяантивирусная проверка ПО, устанавливаемого на сервера, непосредственно перед его установкой, а также повторная внеплановая проверка — по окончанию установки;
    3. Настройка средств антивирусной защиты;
    4. Составление расписания полных проверок и проверка их выполнения;
    5. Анализ отчетов, формируемых средством антивирусной защиты.

5.3. Рекомендация по организации антивирусной безопасности на персональных компьютерах пользователей ИС (администраторов ИС).

1. Антивирусные программные средства обнаружения вирусов следует применять для проверки рабочих станций ИС и носителей информации на наличие вирусов. Антивирусные программные средства должны регулярно обновляться и использоваться в соответствии с инструкциями поставщика на рабочих станциях Фонда.

2. Особое внимание следует обратить на съемные носители (флэш-диски компакт- диски), принадлежащие лицам, временно допущенных к работе на ЭВМ (студенты- практиканты, временно замещающие и т.п.). Работа этих лиц должна проводиться под непосредственным контролем со стороны руководителя подразделения Центра, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

3. Пользователям ИС (администратору ИС) на своем персональном компьютере запрещено:
   1. Изменять настройки и конфигурацию антивирусных приложений;
   2. Удалять или добавлять какие-либо антивирусные программы;
   3. Работать со съемными дисками, без предварительной их проверки, установленной на персональном компьютере антивирусной программы;
   4. Запускать неизвестные приложения, полученные по электронной почте.

4. Пользователь ИС (администратор ИС) обязан:
   1) Ежедневно в начале работы при загрузке компьютера убедиться в наличии резидентного антивирусного монитора (справа на панели задач должен быть значок с логотипом программы антивирусной защиты и всплывающим над ним наименованием этой программы), и в случае его отсутствия уведомить специалистов по эксплуатации систем;
   2) Самостоятельно запускать внеплановую антивирусную проверку локальных дисков своего персонального компьютера при получении уведомления от специалиста эксплуатации систем, а также 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.);
   3) В случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, незамедлительно сообщить об этом специалисту эксплуатации систем.

5. Защита от злонамеренного и мобильного кода.

1. С целью защиты информации и программных средств от несанкционированного доступа и действия вредоносных программ при разработке и эксплуатации системы должны быть предприняты организационные, правовые, технические и технологические меры, направленные на предотвращение возможных

несанкционированных действий по отношению к программным средствам и устранение последствий этих действий. При этом руководство должно обеспечить неукоснительное выполнение следующих мероприятий:

2. Сертификация - действия третьей стороны, цель которых - подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга, прямо или косвенно взаимодействующая с системой, соответствует определенным стандартам или другим нормативным документам в области защиты информации.
3. Профилактика - систематические действия эксплуатационного персонала, цель которых - выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и (или) вновь полученные программные средства на наличие компьютерных вирусов.
3. Ревизия - проверка вновь полученных программ специальными средствами, проводимая путем их запуска в контролируемой среде.

6. Ответственность

1. Специалисты по эксплуатации систем несут ответственность занадлежащее выполнение своих функциональных обязанностей по обеспечению антивирусной безопасности серверовИС и ПК работников Фонда.
2. Ответственность по антивирусной защите ПК пользователей ИС определяется соответствии с внутренними нормативными документами Цетра.
3. Администраторы ИС и пользователи ИС несут ответственность за обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.
4. Администраторы ИС несут ответственность за соблюдение требований Инструкции и утвержденных в ее рамках НД по ИБ.
5. Специалист по ИБ несет ответственность за разработку, актуализацию и контроль за исполнением требований, изложенных в настоящей Инструкции.

7. Указание условий пересмотра СОП:

Пересмотр СОП проводиться 1 раз в 3 года или при появлении новых требовании.

2. Нормативные ссылки:

1. Приказ и.о. Министра здравоохранения Республики Казахстан от 30 октября 2020 года «Об утверждении форм учетной документации в области здравоохранения, а также инструкций по их заполнению» № КР ДСМ-175/2020;
2. Приказ и.о. Министра здравоохранения Республики Казахстан от 5 ноября 2021 года «Об утверждении стандартов аккредитации медицинских

организаций» № КР ДСМ – 111;

3. Приказ Министра здравоохранения Республики Казахстан от 24 августа 2021 года № «Об утверждении «Правил оказания первичной медико-санитарной помощи» КР ДСМ-90;

Лист регистрации изменений

№	№ раздела, пункта стандарта, в которое внесено изменение	Дата внесения изменения	ФИО лица, внесшего изменения

Лист ознакомления

№	Фамилия И.О.	Должность	Дата	Подпись
	Сухинин А.А.	программист	04.01.2024	[подпись]
	Семов А.В.	программист	04.01.2024	[подпись]