Наименование структурного подразделения:	**Все структурные подразделения**		
Названия документа:	**СОП «Инструкция по защите информации электронного формата»**		
Утвержден:	Руководитель ГКП на ПХВ «ЛГП» Чалкаров А.Б.		
Дата утверждения:			
Разработчик:	*Должность*	*Ф.И.О.*	*Подпись*
	Заместитель гл.врача по лечебному делу	Анаркулова У.О.	
	Программист	Сопов А. Сухинин А.	
	Заведующий отделением	Садыков Г.Б.	
Согласовано:	Заместитель гл.врача по ОМД	Кабылбеков Г.К.	
	Заместитель гл.врача по контролю качества мед.услуг	Рысбаев С.Т.	
	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

СОП «Инструкция по защите информации электронного формата»

1. Определение:

1) Информационная безопасность – это состояние защищенности информационной среды, защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Информационная безопасность организации – целенаправленная деятельность ее органов и должностных лиц с использованием разрешенных сил и средств по достижению состояния защищенности информационной среды организации, обеспечивающее ее нормальное функционирование и динамичное развитие.

Информационная безопасность – защита конфиденциальности, целостности и доступности информации.

2) Конфиденциальность: свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.

3) Целостность: неизменность информации в процессе ее передачи или хранения.

4) Доступность: свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Утеря информации бывает по разным причинам:

- эксплуатационные поломки носителей информации;
- стихийные и техногенные бедствия;
- вредоносные программы;
- человеческий фактор.

2. Ресурсы:

1) Компьютор
2) Ноутбуки

3. Процедуры:

Эксплуатационные поломки носителей информации

Описание: случайные поломки в пределах статистики отказов, связанные с неосторожностью или выработкой ресурса. Конечно же, если какая-то важная информация уже потеряна, то можно обратиться в специализированную службу - но надежность этого не стопроцентная. Хранить всю информацию (каждый файл) минимум в двух экземплярах (причем каждый экземпляр на своем носителе данных). Для этого применяются:

1) RAID 1, обеспечивающий восстановление самой свежей информации. Файлы, расположенные на сервере с RAID, более защищены от поломок, чем хранящиеся на локальной машине;

2) Ручное или автоматическое копирование на другой носитель. Для этого может использоваться система контроля версий, специализированная программа резервного копирования или подручные средства наподобие периодически запускаемого cmd-файла.

Стихийные и техногенные бедствия

Описание: шторм, землетрясение, кража, пожар, прорыв водопровода – все это приводит к потере всех носителей данных, расположенных на определенной территории.

Единственный способ защиты от стихийных бедствий – держать часть резервных копий в другом помещении.

Вредоносные программы

Описание: в эту категорию входит случайно занесенное ПО, которое намеренно портит информацию – вирусы, черви, «троянские кони». Иногда факт заражения обнаруживается, когда немалая часть информации искажена или уничтожена:

1) Установка антивирусных программ на рабочие станции. Простейшие антивирусные меры – отключение автозагрузки, изоляция локальной сети от Интернета, и т. д.

2) Обеспечение централизованного обновления: первая копия антивируса получает обновления прямо из Интернета, а другие копии настроены на папку, куда первая загружает обновления; также можно настроить прокси-сервер таким образом, чтобы обновления кешировались (это все меры для уменьшения трафика).

3) Иметь копии в таком месте, до которого вирус не доберется – выделенный сервер или съемные носители.

4) Если копирование идет на сервер: обеспечить защиту сервера от вирусов (либо установить антивирус, либо использовать ОС, для которой вероятность заражения мала). Хранить версии достаточной давности, чтобы существовала копия, не контактировавшая с зараженным компьютером.

5) Если копирование идет на съемные носители: часть носителей хранить (без дописывания на них) достаточно долго, чтобы существовала копия, не контактировавшая с зараженным компьютером.

Человеческий фактор

Описание: намеренное или ненамеренное уничтожение важной информации – человеком, специально написанной вредоносной программой или сбойным ПО.

1) Тщательно расставляются права на все ресурсы, чтобы другие пользователи не могли модифицировать чужие файлы. Исключение делается для системного администратора, который должен обладать всеми правами на все, чтобы быть способным исправить ошибки пользователей, программ и т.д.

2) Обеспечить работающую систему резервного копирования - то есть, систему, которой люди реально пользуются и которая достаточно устойчива к ошибкам оператора. Если пользователь не пользуется системой резервного копирования, вся ответственность за сохранность ложится на него.

3) Хранить версии достаточной давности, чтобы при обнаружении испорченных данных файл можно было восстановить.
4) Перед переустановкой ОС следует обязательно копировать все содержимое раздела, на которой будет установлена ОС, на сервер, на другой раздел или на CD/DVD.
5) Оперативно обновлять ПО, которое заподозрено в потере данных.

1. Указание условии пересмотра СОП: Пересмотр СОП проводиться 1 раз в 3 года или при появлении новых требовании.
2. Нормативные ссылки:
- 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;
-Приказ и.о. Министра здравоохранения Республики Казахстан от 5 ноября 2021 года «Об утверждении стандартов аккредитации медицинских организаций» « № КР ДСМ – 111.
- 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	Сух.