«Утверждаю»
Главный врач КГП на ПХВ
«Областной онкологический диспансер»
Абдримов Е.Г.

Инструкция по защите информации электронного формата

1. Определение

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

Информационная безопасность – защита конфиденциальности, целостности и доступности информации.

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

Целостность: неизменность информации в процессе ее передачи или хранения.

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) Кабинеты оснащенные компьютерами
2) Персонал

3. Документирование

1) Приказ о назначении ответственного лица по зашите информации
2) Защита информации. Меры защиты информации
3) Уровни защиты информации

4. 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 надёжность этого не стопроцентная.

1) хранить всю информацию (каждый файл) минимум в двух экземплярах (причём каждый экземпляр на своём носителе данных). Для этого применяются:

- RAID 1, обеспечивающий восстановление самой свежей информации. Файлы, расположенные на сервере с RAID, более защищены от поломок, чем хранящиеся на локальной машине;
- 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 – всё это приводит к потере всех носителей данных, расположенных на определённой территории.

1) единственный способ защиты от стихийных бедствий – держать часть резервных копий в другом помещении.

Вредоносные программы

Описание: в эту категорию входит случайно занесённое 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 всё меры для уменьшения трафика).

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

4) Если копирование идёт 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 заражённым компьютером.

5) Если копирование идёт на съёмные носители: часть носителей хранить (без дописывания на них) достаточно долго, чтобы существовала копия, не контактировавшая с заражённым 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 всё, 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 всё 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.

Программист **Незнахин П.Н.**