УТВЕРЖДЕНО:
И.о. главного врача ГБУЗ «ЦРБ»
Майского муниципального района
_____ Т.В. Аникушина
ПРИКАЗ УЧРЕЖДЕНИЯ
ОТ «14» АВГУСТА 2017Г. № 275
ПРИЛОЖЕНИЕ № 17

Модель нарушителя безопасности и Модель угроз безопасности в ГБУЗ «ЦРБ» Майского муниципального района

Под нарушителем в ГБУЗ «ЦРБ» Майского муниципального района понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Нарушители подразделяются по признаку принадлежности к ИСПДн.

Все нарушители делятся на две группы:

1 - ***внешние нарушители*** – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

2 - ***внутренние нарушители*** – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн в ГБУЗ «ЦРБ» Майского муниципального района можно выделить следующие угрозы:

1) Угрозы от утечки по техническим каналам:

а) Угрозы утечки акустической информации.

б) Угрозы утечки видовой информации.

в) Угрозы утечки информации по каналам ПЭМИН.

2) Угрозы несанкционированного доступа к информации:

а) Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн:

- *Кража ПЭВМ;*
- *Кража носителей информации;*
- *Кража ключей и атрибутов доступа;*
- *Кражи, модификации, уничтожения информации;*
- *Вывод из строя узлов ПЭВМ, каналов связи;*
- *Несанкционированное отключение средств защиты.*

б) Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):

- *Действия вредоносных программ (вирусов);*
- *Недекларированные возможности системного ПО и ПО для обработки персональных данных;*
- *Установка ПО не связанного с исполнением служебных обязанностей.*

в) Угрозы не преднамеренных действий пользователей и наруше-ний безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении,

а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:

- Утрата ключей и атрибутов доступа;

-Непреднамеренная модификация (уничтожение) информации сотрудниками;

- Непреднамеренное отключение средств защиты;

- Выход из строя аппаратно-программных средств;

- Сбой системы электроснабжения;

- Стихийное бедствие.

г) Угрозы преднамеренных действий внутренних нарушителей:

- Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;

- Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

д) Угрозы несанкционированного доступа по каналам связи:

1) Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

- Перехват за пределами с контролируемой зоны;

- Перехват в пределах контролируемой зоны внешними нарушителями;

- Перехват в пределах контролируемой зоны внутренними нарушителями.

2) Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

3) Угрозы выявления паролей по сети.

4) Угрозы навязывание ложного маршрута сети.

5) Угрозы подмены доверенного объекта в сети.

6) Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

7) Угрозы типа «Отказ в обслуживании».

8) Угрозы удаленного запуска приложений.

9) Угрозы внедрения по сети вредоносных программ.