Утверждено Приказом

Главного врача

Республиканского Центра СПИД

_____ **/ Санчы И.Д./**

«10» января 2023г. №____

Перечень защищаемых данных в информационной системе «Региональная медицинская информационно-аналитическая система 17» в ГБУЗ Республики Тыва «Республиканский Центр по профилактике и борьбе со СПИД и инфекционными заболеваниями» (Республиканский Центр СПИД)

Кызыл – 2023г.

Защищаемыми информационными ресурсами в информационной системе «Региональная медицинская информационно-аналитическая система 17» в Республиканском Центре СПИД являются:

1. Обрабатываемая информация

1.1. Данные, содержащиеся в ИС «Региональная медицинская информационно-аналитическая система 17» в Республиканском Центре СПИД, в том числе информация:

- анкетные и биографические данные гражданина, включая адрес места жительства и проживания;
- паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи);
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (включая серию, номер, дату выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дату начала и завершения обучения);
- сведения о трудовой деятельности, занимаемой должности;
- сведения о состоянии здоровья и наличии заболеваний;
- сведения из страховых полисов обязательного (добровольного) медицинского страхования;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

1.2. В ИС «Региональная медицинская информационно-аналитическая система 17» в Республиканском Центре СПИД могут включаться иные сведения, за исключением сведений, являющихся персональными данными или отнесенных к государственной тайне.

2. Технологическая информация

Технологическая информация, подлежащая защите, включает:

- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о системе защиты ИС, ее составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации;
- информация о программно-технических средствах обработки;
- информация о средствах защиты информации;
- информация о каналах информационного обмена и телекоммуникации;
- информация об объектах и помещениях, в которых размещены компоненты ИС.

3. Программно-технические средства обработки

Программно-технические средства включают в себя:

- общесистемное и специальное программное обеспечение (операционные системы, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИС;
- аппаратные средства обработки защищаемой информации (АРМ);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

4. Средства защиты информации

Средства защиты информации состоят из программных средств и включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства анализа защищенности;
- средства межсетевого экранирования;
- средства криптографической защиты данных, при их передачи по каналам связи сетей общего и (или) международного обмена.

5. Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

6. Объекты и помещения, в которых размещены компоненты ИС

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

Разработал
Администратор
информационной безопасности _____ Сандаков З.Н.

"09" января 2023 г.