Сведения
о реализуемых требованиях к защите персональных данных

Для защиты персональных данных, обрабатываемых в КГБУЗ «Уссурийская ЦГБ» приняты правовые, организационные и технические меры:

I. Правовые меры:

1. Разработаны локальные акты по вопросам обработки и защиты персональных данных:

политика в отношении обработки персональных данных;

положение об обработке и защите персональных данных;

модель угроз безопасности информационной системы персональных данных;

перечень персональных данных, подлежащих защите в информационных системах персональных данных;

положение о разграничении прав доступа к обрабатываемым персональным данным;

правила работы с обезличенными персональными данными;

правила обработки персональных данных без использования средств автоматизации;

разрешительная система доступа к персональным данным, обрабатываемым в информационных системах персональных данных;

порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных.

2. Отказ от любых способов обработки персональных данных, не соответствующих требованиям законодательства Российской Федерации о персональных данных.

II. Организационные меры:

Приказом КГБУЗ «Уссурийская ЦГБ» назначены:

ответственный за организацию обработки персональных данных в;

администраторы информационных систем персональных данных;

Разработаны:

инструкции пользователям по защите персональных данных, антивирусной защите, действиям в кризисных ситуациях.

план мероприятий по защите персональных данных.

Комиссией организации установлены уровни защищенности персональных данных при их обработке в информационных системах персональных данных с оформлением актов.

Организован:

прием и обработка обращений и запросов субъектов персональных данных или их представителей;

контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

Обработка персональных данных работников КГБУЗ «Уссурийская ЦГБ» осуществляется с их письменного согласия.

Определены:

угрозы безопасности персональных данных, актуальных для информационных систем персональных данных;

перечни лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

работники, допущенные к работе со сведениями персонифицированного учета медицинской помощи, оказанной застрахованным лицам;

подразделение, ответственное за обеспечение безопасности персональных данных в информационных системах;

места хранения персональных данных (материальных носителей).

Установлены:

правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных;

порядок хранения и использования персональных данных работников КГБУЗ «Уссурийская ЦГБ» с соблюдением требований Трудового Кодекса и иных федеральных законов.

Организован учет:

лиц, допущенных к работе с персональными данными в информационных системах персональных данных;

машинных носителей персональных данных (с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

Организовано ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, требованиями к защите персональных данных, локальными актами по вопросам обработки и защиты персональных данных, ответственностью за нарушение норм, регулирующих обработку и защиту персональных данных.

III. Технические меры:

Приняты меры по защите от несанкционированного доступа к персональным данным (идентификация и проверка подлинности пользователя при входе в информационную систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов).

Для выявления вредоносного программного обеспечения в информационных системах применяется антивирусное программное обеспечение.

Производится резервное копирование баз данных, содержащих персональные данные, для возможности их восстановления при модификации или уничтожения вследствие несанкционированного доступа к ним.

Обмен данными с медицинскими и страховыми медицинскими организациями, территориальным и Федеральным фондом в целях ведения персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам, осуществляется в электронном виде по каналам связи с применением средств криптографической защиты информации.

Здания и помещения объектов информатизации оборудованы системами безопасности (пожарной и охранной сигнализации, средствами пожаротушения, видеонаблюдения).

Начальник отдела информационных
технологий и связи А.Г.Губков