	данных с использованием средств автоматизации		
3.	Документальное регламентирование	При необходимости	Разработка локальных нормативных актов по защите персональных данных ли внесение

БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
РЕСПУБЛИКИ КАЛМЫКИЯ
«КАЛМЫЦКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ ИМ. Т. ХАХЛЫНОВОЙ»

Утверждаю
Директор БПОУ РК
«Калмыцкий медицинский
колледж им.Т. Хахлыновой»
_____ В.Азыдов
«_13_» _01_ 2018г.

ПЛАН
мероприятий по защите персональных данных
в БПОУ РК «Калмыцкий медицинский колледж им. Т. Хахлыновой»

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
1.	Оформление правового основания обработки персональных данных	При вводе информационной системы персональных данных (ИСПДн) в эксплуатацию	При создании ИСПДн необходимо оформить приказ о вводе ее в эксплуатацию. Приказ оформляется руководителем образовательной организации.
2.	Направление в уполномоченный орган (Роскомнадзор) уведомления о своем намерении осуществлять обработку персональных данных с использованием средств автоматизации	При необходимости	Уведомление направляется при вводе в эксплуатацию новых информационных систем персональных данных, либо при внесении изменений в существующие
3.	Документальное регламентирование работы с ПД	При необходимости	Разработка локальных нормативных актов по защите персональных данных ли внесение изменений в существующие локальные нормативные акты
4.	Получение письменного согласия субъектов ПД (физических лиц) на обработку ПД в случаях, когда этого требует законодательство	Постоянно	Письменное согласие получается при передаче ПД субъектами для обработки в ИСПДн, либо для обработки без использования средств автоматизации. Форма согласия приведена в Положении об обработке ПД.
5.	Ограничение доступа работников к ПД	При необходимости (при создании ИСПДн)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона необходимо разграничить доступ к ПД сотрудников организации согласно

6.	Повышение квалификации сотрудников в области защиты персональных данных	Постоянно	Ответственных за выполнение работ – не менее раз в два года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за защиту персональных данных)
7.	Инвентаризация информационных ресурсов	Раз в год	Проводится с целью выявления присутствия и обработки в них ПД
8.	Классификация информационных систем персональных данных (ИСПД)	При необходимости	Классификация проводится при создании ИСПДн, при выявлении в информационных системах ПД, при изменении состава, структуры самой ИСПДн или технических особенностей ее построения (изменилось ПО, топология и прочее)
9.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
10.	Эксплуатация ИСПД и контроль безопасности ПД	Постоянно	
11.	Понижение требований по защите персональных данных путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона.
12.	Внедрение антивирусной защиты (Касперский)	При необходимости	
13.	Ограничение доступа работников к ПД	Постоянно	
14.	Ограничение доступа к административным компьютерам	Постоянно	Установление паролей