

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»  
МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Кафедра общественного здоровья и управления здравоохранением**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ**

**к практическому занятию на тему:**

**ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В  
ЗДРАВООХРАНЕНИИ**

Направление подготовки (код, специальность):	38.03.01 Экономика
Направленность (бакалаврская программа)	«Экономика и управление в здравоохранении»
Курс:	I
Семестр:	I

Уфа 2025

Рецензенты:

1. Проректор по учебно-методической работе ФГБОУ ВО «Уфимский государственный нефтяной технический университет», кандидат экономических наук, доцент Карачурина Р.Ф.
2. И.о. заведующего кафедрой экономики предпринимательства ФГБОУ ВО «Уфимский университет науки и технологий», кандидат экономических наук, доцент Давлетшина С.М.

Авторы:

1. Профессор кафедры общественного здоровья и управления здравоохранением, д.м.н., профессор С.Г. Ахмерова
2. Профессор кафедры общественного здоровья и управления здравоохранением, д.м.н., доцент З.М. Султанаева

Утверждена на заседании кафедры общественного здоровья и управления здравоохранением №2 от 01 октября 2025 г.

Учебная дисциплина «Защита персональных данных в здравоохранении» разработана на основании ФГОС ВО по направлению подготовки 38.03.01 Экономика (уровень бакалавриата), утвержденный приказом Министерством науки и высшего образования Российской Федерации от «12» августа 2020 г № 954.

Программа дисциплины «Защита персональных данных в здравоохранении» по направлению подготовки 38.03.01 - Экономика (профиль – «Экономика и управление в здравоохранении») формирует компетенции специалиста в соответствии с требованиями ФГОС ВО 3, обязательные при реализации основных профессиональных образовательных программ высшего образования – программ подготовки кадров высшей квалификации в магистратуре и обеспечивающих решение профессиональных задач защиты персональных данных здравоохранения в процессе осуществления всех видов профессиональной деятельности.

**Процесс изучения дисциплины направлен на формирование следующих компетенций:**  
универсальной компетенции УК-1.

**Цель и задачи освоения дисциплины (модуля).**

**Цель** освоения учебной дисциплины «Защита персональных данных в здравоохранении» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой персональных данных (ПДн), обучением принципам и методам защиты информации в информационных системах персональных данных (ИСПДн).

**Задачи дисциплины:**

- изучение типовых угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- овладение навыками разработки внутренних нормативных документов, обеспечивающих защиту ПД в информационных системах медицинской организации;
- приобретение навыков обеспечения безопасности персональных данных при их обработке в медицинских информационных системах персональных данных.

**Место учебной дисциплины (модуля) в структуре ООП специальности**

Дисциплина «Защита персональных данных в здравоохранении» относится к обязательной части профессионального цикла. Изучение её базируется на следующих дисциплинах: «Основы медицинского законодательства и права», «Компьютерные технологии в биологии», «Санитарно-эпидемиологические требования при работе с компьютерами».

**Учебная дисциплина** «Защита персональных данных в здравоохранении» относится к обязательной части основной образовательной программы (ОПП) высшего образования по направлению подготовки 38.03.01 - Экономика (уровень бакалавриата).

Для формирования профессиональных компетенций обучающиеся должны **знать:**

- - нормативное правовое регулирование защиты ПД в Российской Федерации и за рубежом;
- основные понятия, используемые в законодательных правовых документах, регламентирующих защиту ПД и конфиденциальной информации в медицинских организациях;
- характеристику медицинской организации как оператора ПД;
- виды конфиденциальной информации, обрабатываемые в медицинских информационных системах;
- основные требования к обеспечению защиты данных о пациенте, врачебной тайны;
- основные требования к защите ПД медицинского работника;
- механизмы контроля и организации надзора за обработкой ПД;
- ответственность, предусмотренную за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций обучающиеся должны **уметь:**

- осуществлять комплекс организационно-правовых мероприятий по организации защиты ПД

- и защиты конфиденциальной информации в медицинских организациях;
- организовывать деятельность медицинской организации как оператора ПД;
  - принимать управленческие решения, направленные на обеспечение защиты ПД о пациентах и ПД медицинских работников в медицинских организациях;
  - выявлять и предотвращать нарушения законодательства в сфере защиты конфиденциальной информации;
  - использовать существующее законодательство в сфере защиты ПД при решении конкретных задач по управлению в сфере здравоохранения.

Для формирования *опыта практической деятельности* обучающиеся должны обладать:

- навыками организации комплексной системы защиты ПД и конфиденциальной информации медицинских организаций;
- навыками управления по обеспечению организационно-правовых и технических мер, определяемых с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в информационных системах.
- навыками определения типа угроз безопасности ПД, актуальных для информационной системы медицинской организации;
- навыками разработки внутренних нормативных документов, обеспечивающих защиту ПД в информационных системах медицинской организации.

**Требования к результатам освоения учебной дисциплины «Защита персональных данных в здравоохранении»**

**Типы профессиональной деятельности, которые лежат в основе преподавания данной дисциплины:**

1. организационно-управленческий;
2. научно-исследовательский.

**Название тем практических занятий и количество часов по семестрам изучения учебной дисциплины «Защита персональных данных в здравоохранении»**

№ п/п	Название тем практических занятий учебной дисциплины	Семестры
		3
1	2	3
1	Категории и источники персональных данных. Тип угроз для ИС ПД и уровень защищенности персональных данных. Трансграничная передача персональных данных	3
2	Медицинская организация как оператор персональных данных. Обеспечение безопасности персональных данных в медицинских информационных системах.	3
3	Организация защиты конфиденциальной информации в медицинских организациях. Персональные данные пациента и врачебная тайна. Защита персональных данных медицинского работника.	3
4	Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства	3
	<b>Итого</b>	<b>12</b>

**Занятие 1. «Категории и источники персональных данных. Тип угроз для ИС ПД и уровень защищенности персональных данных. Трансграничная передача персональных данных»**

**1. Тема и ее актуальность.** «Категории и источники персональных данных. Классификация информационных систем персональных данных (ИС ПД). Тип угроз для ИС ПД и уровень защищенности персональных данных. Трансграничная передача персональных данных».

Для практической деятельности специалиста в области сестринского дела необходимы знания в области категорий и источников персональных данных. Классификация информационных систем персональных данных (ИС ПД). Тип угроз для ИС ПД и уровень защищенности персональных данных. Трансграничная передача персональных данных.

**2. Учебные цели:** освоение учебной дисциплины «Защита персональных данных в здравоохранении» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой персональных данных (ПДн), обучением принципам и методам защиты информации в информационных системах персональных данных (ИСПДн).

Для формирования профессиональных компетенций обучающийся должен **знать:**

- нормативное правовое регулирование защиты ПД в Российской Федерации и за рубежом;
- основные понятия, используемые в законодательных правовых документах, регламентирующих защиту ПД и конфиденциальной информации в медицинских организациях;
- характеристику медицинской организации как оператора ПД;
- виды конфиденциальной информации, обрабатываемые в медицинских информационных системах;
- основные требования к обеспечению защиты данных о пациенте, врачебной тайны;
- основные требования к защите ПД медицинского работника;
- механизмы контроля и организации надзора за обработкой ПД;
- ответственность, предусмотренную за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций обучающийся должен **владеть и уметь,** и овладеть следующими **компетенциями** (частично):

УК-1. способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Перечисленные компетенции направлены на частичное формирование следующих трудовых функций:

Е/01.8 – Проектирование и организация процессов деятельности медицинской организации. Правовые и организационные вопросы регулирования отношений в сфере обработки персональных данных.

1. Правовые основы института персональных данных. Принципы и условия обработки персональных данных.

Классификация угроз для медицинских информационных систем, основные организационные меры, технические и программные средства защиты информации при организации обработки ПД.

1.1. Категории и источники персональных данных.

1.2. Классификация информационных систем персональных данных (ИС ПД).

1.3. Тип угроз для ИС ПД и уровень защищенности персональных данных.

1.4 Трансграничная передача персональных данных;

Е/02.8– Управление ресурсами по обеспечению процессов деятельности медицинской организации. Организация защиты персональных данных и конфиденциальной информации в медицинских организациях.

2. Обеспечение безопасности персональных данных в медицинских информационных системах

2.1. Медицинская организация как оператор персональных данных. Персональные данные пациента и врачебная тайна.

2.2 . Защита персональных данных медицинского работника. Организация защиты конфиденциальной информации в медицинских организациях;

Е/03.8 – Менеджмент качества и безопасности медицинской деятельности в медицинской организации. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

3. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства

3.1. Уполномоченный орган по защите прав субъектов персональных данных.  
3.2. Ответственность, предусмотренная за правонарушения в сфере защиты информации.  
Для формирования профессиональных компетенций студент должен **уметь**:

- осуществлять комплекс организационно-правовых мероприятий по организации защиты ПД и защиты конфиденциальной информации в медицинских организациях;
- организовывать деятельность медицинской организации как оператора ПД;
- принимать управленческие решения, направленные на обеспечение защиты ПД о пациентах и ПД медицинских работников в медицинских организациях;
- выявлять и предотвращать нарушения законодательства в сфере защиты конфиденциальной информации;
- использовать существующее законодательство в сфере защиты ПД при решении конкретных задач по управлению в сфере здравоохранения.

### **3. Необходимые базисные знания и умения:**

- навыками организации комплексной системы защиты ПД и конфиденциальной информации медицинских организаций;
- навыками управления по обеспечению организационно-правовых и технических мер, определяемых с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в информационных системах.
- навыками определения типа угроз безопасности ПД, актуальных для информационной системы медицинской организации;
- навыками разработки внутренних нормативных документов, обеспечивающих защиту ПД в информационных системах медицинской организации.

**4. Вид занятия:** практическое занятие.

**5. Продолжительность занятия:** 3 часа.

### **6. Оснащение:**

- 6.1. Дидактический материал (ситуационные задачи, тестовые задания по изучаемым темам).  
6.2 Компьютерный класс, объединенный в локальную вычислительную сеть. На компьютерах установлены серверные версии операционной системы Windows, доступ в глобальную вычислительную сеть Интернет. В целях сохранения результатов работы наличие у обучающихся при себе носителей информации (flash-накопители).

### **7. Содержание занятия:**

7.1. Контроль исходного уровня знаний и умений.

Задания для самоконтроля: решение обучающимися индивидуальных наборов тестов по теме  
Выберите один правильный ответ

**1. В случае отказа в предоставлении информации о наличии персональных данных субъекту персональных данных или его представителю при их обращении оператор обязан дать в письменной форме мотивированный ответ, обосновывающий отказ**

- 1) в срок, не превышающий пяти дней со дня обращения субъекта персональных данных или его представителя
- 2) в срок, не превышающий десяти дней со дня обращения субъекта персональных данных или его представителя
- 3) в срок, не превышающий пятнадцати дней со дня обращения субъекта персональных данных или его представителя
- 4) в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя

**2. В случае представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки оператор обязан уничтожить эти персональные данные**

- 1) в срок, не превышающий трех рабочих дней со дня представления

- 2) в срок, не превышающий пяти рабочих дней со дня представления
- 3) в срок, не превышающий семи рабочих дней со дня представления
- 4) в срок, не превышающий десяти рабочих дней со дня представления

**3. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию**

- 1) в течение трех дней с даты получения такого запроса
- 2) в течение пяти дней с даты получения такого запроса
- 3) в течение пятнадцати дней с даты получения такого запроса
- 4) в течение тридцати дней с даты получения такого запроса

**7.3. Ознакомление обучающихся с содержанием занятия. Изложение узловых вопросов темы данного занятия. Демонстрация преподавателем методики практических приемов по данной теме. Теоретический разбор темы. Опрос.**

1. Какие данные пациента в системе персонифицированного учета медицинской организации относятся к ПД.
2. Приведите алгоритм трансграничной передачи ПД
3. Дайте характеристику информационным системам медицинских организаций, в которых обрабатываются ПД о состоянии здоровья
4. Перечислите сведения, относящиеся к специальным категориям ПД. В каких случаях допускается обработка специальных категорий ПД без согласия субъекта ПД
5. Дайте характеристику операторам ПД. Каков порядок регистрации в качестве оператора ПД медицинских организаций.

**7.4. Решение ситуационных задач**

Задание 1. Перечислите основные нормативные правовые документы, содержащие положения защиты информации в сфере здравоохранения

Задание 2. Дайте определение персональных данных (далее – ПД). Что входит в понятие «обработка ПД».

Задание 3. Перечислите сведения, относящиеся к специальным категориям ПД. В каких случаях допускается обработка специальных категорий ПД без согласия субъекта ПД.

**7.5. Контроль конечного уровня усвоения темы**

Подготовка к выполнению практических приемов по теме занятия.

Материалы для контроля уровня освоения темы: набор тестовых заданий, ситуационные задачи.

*Место проведения самоподготовки:*

читальный зал, учебная комната для самостоятельной работы обучающихся, компьютерный класс.

Учебно-исследовательская работа обучающихся по данной теме (проводится в учебное время): работа с основной и дополнительной литературой, решение ситуационных задач.

**Литература:**

*Основная:*

Общественное здоровье и здравоохранение: учебник / под ред.: В. А. Миняева, Н. И. Вишнякова. - 5-е изд., перераб. и доп. - М. : МЕДпресс-информ, 2009. - 655 с.	200
Лисицын, Ю.П. Общественное здоровье и здравоохранение [Электронный ресурс] : учебник / Ю. П. Лисицын. - 3-е изд., испр. и доп. - Электрон. текстовые дан. - М. : Гэотар Медиа, 2015. -on-line. - Режим доступа: ЭБС «Консультант студента» <a href="http://www.studmedlib.ru/ru/book/ISBN9785970432914.html">http://www.studmedlib.ru/ru/book/ISBN9785970432914.html</a>	Неограниченный доступ

*Дополнительная*

<p><b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Текст] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед. ун-т. - Уфа, 2014. - 107,[2] с.</p>	15
<p><b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Электронный ресурс] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед. ун-т. - Электрон. текстовые дан. - Уфа, 2014. - on-line. - Режим доступа: БД «Электронная учебная библиотека»  <a href="http://library.bashgmu.ru/elibdoc/elib582.pdf">http://library.bashgmu.ru/elibdoc/elib582.pdf</a></p>	Неограниченный доступ

*Нормативные правовые акты в области защиты персональных данных*

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28.01.1981 (с поправками от 15.06.1999)
- Директива № 2002/58/ЕС Европейского парламента и Совета Европейского Союза «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)», Брюссель, 12.07.2002 г. (с изм. и доп. от 25.11.2009).
- Федеральный закон от 21.07.2014 г. № 242-ФЗ (ред. от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»
- Федеральный закон от 21.11.2011 № 323-ФЗ (в ред. от 29.05.2019) «Об основах охраны здоровья граждан в Российской Федерации».
- Федеральный закон Российской Федерации от 25.07.2011г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»
- Федеральный закон от 27.07.2006г. № 152-ФЗ (ред. от 31.12.2017) «О персональных данных»
- Федеральный закон от 27.07.2006г. № 149-ФЗ (в ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 19.12.2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
- Указ Президента Российской Федерации от 17.03.2008 г. № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
- Указ Президента Российской Федерации от 30.05.2005 г. № 609 (ред. от 23.07.2019) «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»
- Указ Президента Российской Федерации от 06.03.1997г. № 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера»
- Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-РП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»
- Постановление Правительства Российской Федерации от 13.02.2019 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных»
- Постановление Правительства Российской Федерации от 03.02.2012 г. №79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации»
- Постановление Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных»

- Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Приказ Минздравсоцразвития России от 23.04.2012 № 390н «Об утверждении Перечня определенных видов медицинских вмешательств, на которые граждане дают информированное добровольное согласие при выборе врача и медицинской организации для получения первичной медико-санитарной помощи»
- Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
- Приказ Роскомнадзора от 30.05.2017 № 94 (ред. от 30.10.2018) «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»

#### *Интернет-ресурсы*

База данных «Электронная учебная библиотека»	Свидетельство №2009620253 от 08.05.2009 <a href="http://library.bashgmu.ru">http://library.bashgmu.ru</a>
Электронно-библиотечная система eLIBRARY. Коллекция российских научных журналов по медицине и здравоохранению	ООО РУНЭБ, Договор №750 от 18.12.2018 <a href="http://elibrary.ru">http://elibrary.ru</a>
База данных Scopus	ФГБУ ГПНТБ России, Сублицензионный договор № SCOPUS/50 от 09.10.2019 <a href="https://www.scopus.com">https://www.scopus.com</a>
База данных Web of Science Core Collection	ФГБУ ГПНТБ России, Сублицензионный договор № Wos/50 от 05.09.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
База данных Russian Science Citation Index	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
База данных MEDLINE	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
Консультант Плюс: справочно-правовая система	ООО Компания Права «Респект» Договор о сотрудничестве от 21.03.2012 локальный доступ

## **Занятие 2. «Медицинская организация как оператор персональных данных.**

### **Обеспечение безопасности персональных данных в медицинских информационных системах.»**

**1. Тема и ее актуальность.** «Медицинская организация как оператор персональных данных. Персональные данные пациента и врачебная тайна.»

Для практической деятельности специалиста в области сестринского дела необходимы знания в области медицинской организации как оператора персональных данных. Персональные данные пациента и врачебная тайна.

**2. Учебные цели:** освоение учебной дисциплины «Защита персональных данных в здравоохранении» является теоретическая и практическая подготовка специалистов к

деятельности, связанной с защитой персональных данных (ПДн), обучением принципам и методам защиты информации в информационных системах персональных данных (ИСПДн).

Для формирования профессиональных компетенций обучающийся должен **знать**:

- нормативное правовое регулирование защиты ПД в Российской Федерации и за рубежом;
- основные понятия, используемые в законодательных правовых документах, регламентирующих защиту ПД и конфиденциальной информации в медицинских организациях;
- характеристику медицинской организации как оператора ПД;
- виды конфиденциальной информации, обрабатываемые в медицинских информационных системах;
- основные требования к обеспечению защиты данных о пациенте, врачебной тайны;
- основные требования к защите ПД медицинского работника;
- механизмы контроля и организации надзора за обработкой ПД;
- ответственность, предусмотренную за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций обучающийся должен **владеть и уметь**, и овладеть следующими **компетенциями** (частично):

УК-1. способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Перечисленные компетенции направлены на частичное формирование следующих трудовых функций:

Е/01.8 – Проектирование и организация процессов деятельности медицинской организации. Правовые и организационные вопросы регулирования отношений в сфере обработки персональных данных.

1.Правовые основы института персональных данных. Принципы и условия обработки персональных данных.

Классификация угроз для медицинских информационных систем, основные организационные меры, технические и программные средства защиты информации при организации обработки ПД.

1.1. Категории и источники персональных данных.

1.2. Классификация информационных систем персональных данных (ИС ПД).

1.3. Тип угроз для ИС ПД и уровень защищенности персональных данных.

1.4 Трансграничная передача персональных данных;

Е/02.8– Управление ресурсами по обеспечению процессов деятельности медицинской организации. Организация защиты персональных данных и конфиденциальной информации в медицинских организациях.

2. Обеспечение безопасности персональных данных в медицинских информационных системах

2.1. Медицинская организация как оператор персональных данных. Персональные данные пациента и врачебная тайна.

2.2. Защита персональных данных медицинского работника. Организация защиты конфиденциальной информации в медицинских организациях;

Е/03.8 – Менеджмент качества и безопасности медицинской деятельности в медицинской организации. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

3. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства

3. 1. Уполномоченный орган по защите прав субъектов персональных данных.

3.2. Ответственность, предусмотренная за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций студент должен **уметь**:

- осуществлять комплекс организационно-правовых мероприятий по организации защиты ПД и защиты конфиденциальной информации в медицинских организациях;
- организовывать деятельность медицинской организации как оператора ПД;

- принимать управленческие решения, направленные на обеспечение защиты ПД о пациентах и ПД медицинских работников в медицинских организациях;
- выявлять и предотвращать нарушения законодательства в сфере защиты конфиденциальной информации;
- использовать существующее законодательство в сфере защиты ПД при решении конкретных задач по управлению в сфере здравоохранения.

### **3. Необходимые базисные знания и умения:**

- навыками организации комплексной системы защиты ПД и конфиденциальной информации медицинских организаций;
- навыками управления по обеспечению организационно-правовых и технических мер, определяемых с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в информационных системах.
- навыками определения типа угроз безопасности ПД, актуальных для информационной системы медицинской организации;
- навыками разработки внутренних нормативных документов, обеспечивающих защиту ПД в информационных системах медицинской организации.

**4. Вид занятия:** практическое занятие.

**5. Продолжительность занятия:** 3 часа.

### **6. Оснащение:**

- 6.1. Дидактический материал (ситуационные задачи, тестовые задания по изучаемым темам).
- 6.2 Компьютерный класс, объединенный в локальную вычислительную сеть. На компьютерах установлены серверные версии операционной системы Windows, доступ в глобальную вычислительную сеть Интернет. В целях сохранения результатов работы наличие у обучающихся при себе носителей информации (flash-накопители).

### **7. Содержание занятия:**

7.1. Контроль исходного уровня знаний и умений.

Задания для самоконтроля: решение обучающимися индивидуальных наборов тестов по теме Выберите один правильный ответ

**В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает**

- 1) орган государственной власти, независимо от того, является ли он законным представителем субъекта персональных данных или нет
- 2) опекун субъекта персональных данных
- 3) медицинская организация, в которой находится субъект персональных данных
- 4) любое лицо на основании доверенности субъекта персональных данных

**В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают**

- 1) опекун субъекта персональных данных
- 2) наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни
- 3) медицинская организация, в которой находится субъект персональных данных
- 4) любое лицо на основании доверенности субъекта персональных данных

**Медицинская организация обретает статус оператора обработки персональных данных относительно**

- 1) только своих сотрудников
- 2) только пациентов, которым медицинская помощь оказывается по программе ОМС
- 3) всех своих сотрудников и пациентов
- 4) статус оператора не обретает

**7.3. Ознакомление обучающихся с содержанием занятия. Изложение узловых вопросов темы данного занятия. Демонстрация преподавателем методики практических приемов по данной теме. Теоретический разбор темы. Опрос.**

1. Общая характеристика подтверждения факта обработки персональных данных оператором, а также цель данной обработки.
2. Общая характеристика способов обработки персональных данных, применяемые оператором;
3. Общая характеристика сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
4. Общая характеристика перечней обрабатываемых персональных данных и источник их получения
5. Общая характеристика сроков обработки персональных данных, в т. ч. сроки их хранения;

**7.4. Решение ситуационных задач**

Задание 1. Дайте определение конфиденциальной информации. Какими нормативными документами регулируется режим конфиденциальности информации. Перечислите категории сведений конфиденциального характера.

Задание 2. Дайте характеристику врачебной тайны. Каким нормативным документом охраняется врачебная тайна

Задание 3. Какой комплекс организационных и технических мероприятий необходимо провести в медицинских организациях для выполнения требований законодательства по персональным данным и устранения возможных угроз безопасности.

**7.5. Контроль конечного уровня усвоения темы**

Подготовка к выполнению практических приемов по теме занятия.

Материалы для контроля уровня освоения темы: набор тестовых заданий, ситуационные задачи.

*Место проведения самоподготовки:*

читальный зал, учебная комната для самостоятельной работы обучающихся, компьютерный класс.

Учебно-исследовательская работа обучающихся по данной теме (проводится в учебное время): работа с основной и дополнительной литературой, решение ситуационных задач.

**Литература:**

*Основная:*

Общественное здоровье и здравоохранение : учебник / под ред.: В. А. Миняева, Н. И. Вишнякова. - 5-е изд., перераб. и доп. - М. : МЕДпресс-информ, 2009. - 655 с.	200
Лисицын, Ю.П. Общественное здоровье и здравоохранение [Электронный ресурс] : учебник / Ю. П. Лисицын. - 3-е изд., испр. и доп. - Электрон. текстовые дан. - М. : Гэотар Медиа, 2015. -on-line. - Режим доступа: ЭБС «Консультант студента» <a href="http://www.studmedlib.ru/ru/book/ISBN9785970432914.html">http://www.studmedlib.ru/ru/book/ISBN9785970432914.html</a>	Неограниченный доступ

*Дополнительная*

<b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Текст] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед. ун-т. - Уфа, 2014. - 107,[2] с.	15
<b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Электронный ресурс] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед.	Неограниченный доступ

*Нормативные правовые акты в области защиты персональных данных*

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28.01.1981 (с поправками от 15.06.1999)
- Директива № 2002/58/ЕС Европейского парламента и Совета Европейского Союза «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)», Брюссель, 12.07.2002 г. (с изм. и доп. от 25.11.2009).
- Федеральный закон от 21.07.2014 г. № 242-ФЗ (ред. от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»
- Федеральный закон от 21.11.2011 № 323-ФЗ (в ред. от 29.05.2019) «Об основах охраны здоровья граждан в Российской Федерации».
- Федеральный закон Российской Федерации от 25.07.2011г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»
- Федеральный закон от 27.07.2006г. № 152-ФЗ (ред. от 31.12.2017) «О персональных данных»
- Федеральный закон от 27.07.2006г. № 149-ФЗ (в ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 19.12.2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
- Указ Президента Российской Федерации от 17.03.2008 г. № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
- Указ Президента Российской Федерации от 30.05.2005 г. № 609 (ред. от 23.07.2019) «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»
- Указ Президента Российской Федерации от 06.03.1997г. № 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера»
- Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-РП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»
- Постановление Правительства Российской Федерации от 13.02.2019 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных»
- Постановление Правительства Российской Федерации от 03.02.2012 г. №79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации»
- Постановление Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой

без использования средств автоматизации»

- Приказ Минздравсоцразвития России от 23.04.2012 № 390н «Об утверждении Перечня определенных видов медицинских вмешательств, на которые граждане дают информированное добровольное согласие при выборе врача и медицинской организации для получения первичной медико-санитарной помощи»
- Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
- Приказ Роскомнадзора от 30.05.2017 № 94 (ред. от 30.10.2018) «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»

#### *Интернет-ресурсы*

База данных «Электронная учебная библиотека»	Свидетельство №2009620253 от 08.05.2009 <a href="http://library.bashgmu.ru">http://library.bashgmu.ru</a>
Электронно-библиотечная система eLIBRARY. Коллекция российских научных журналов по медицине и здравоохранению	ООО РУНЭБ, Договор №750 от 18.12.2018 <a href="http://elibrary.ru">http://elibrary.ru</a>
База данных Scopus	ФГБУ ГПНТБ России, Сублицензионный договор № SCOPUS/50 от 09.10.2019 <a href="https://www.scopus.com">https://www.scopus.com</a>
База данных Web of Science Core Collection	ФГБУ ГПНТБ России, Сублицензионный договор № Wos/50 от 05.09.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
База данных Russian Science Citation Index	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
База данных MEDLINE	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
Консультант Плюс: справочно-правовая система	ООО Компания Права «Респект» Договор о сотрудничестве от 21.03.2012 локальный доступ

### **Занятие 3. «Организация защиты конфиденциальной информации в медицинских организациях. Персональные данные пациента и врачебная тайна. Защита персональных данных медицинского работника.»**

**1. Тема и ее актуальность.** «Защита персональных данных медицинского работника. Организация защиты конфиденциальной информации в медицинских организациях».

Для практической деятельности специалиста в области сестринского дела необходимы знания в области защиты персональных данных медицинского работника и организации защиты конфиденциальной информации в медицинских организациях

**2. Учебные цели:** освоения учебной дисциплины «Защита персональных данных в здравоохранении» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой персональных данных (ПДн), обучением принципам и методам защиты информации в информационных системах персональных данных (ИСПДн). Для формирования профессиональных компетенций обучающийся должен **знать:**

- нормативное правовое регулирование защиты ПД в Российской Федерации и за рубежом;
- основные понятия, используемые в законодательных правовых документах, регламентирующих защиту ПД и конфиденциальной информации в медицинских организациях;

- характеристику медицинской организации как оператора ПД;
- виды конфиденциальной информации, обрабатываемые в медицинских информационных системах;
- основные требования к обеспечению защиты данных о пациенте, врачебной тайны;
- основные требования к защите ПД медицинского работника;
- механизмы контроля и организации надзора за обработкой ПД;
- ответственность, предусмотренную за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций обучающийся должен **владеть и уметь**, и овладеть следующими **компетенциями** (частично):

УК-1. способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Перечисленные компетенции направлены на частичное формирование следующих трудовых функций:

Е/01.8 – Проектирование и организация процессов деятельности медицинской организации. Правовые и организационные вопросы регулирования отношений в сфере обработки персональных данных.

1. Правовые основы института персональных данных. Принципы и условия обработки персональных данных.

Классификация угроз для медицинских информационных систем, основные организационные меры, технические и программные средства защиты информации при организации обработки ПД.

1.1. Категории и источники персональных данных.

1.2. Классификация информационных систем персональных данных (ИС ПД).

1.3. Тип угроз для ИС ПД и уровень защищенности персональных данных.

1.4 Трансграничная передача персональных данных;

Е/02.8– Управление ресурсами по обеспечению процессов деятельности медицинской организации. Организация защиты персональных данных и конфиденциальной информации в медицинских организациях.

2. Обеспечение безопасности персональных данных в медицинских информационных системах

2.1. Медицинская организация как оператор персональных данных. Персональные данные пациента и врачебная тайна.

2.2. Защита персональных данных медицинского работника. Организация защиты конфиденциальной информации в медицинских организациях;

Е/03.8 – Менеджмент качества и безопасности медицинской деятельности в медицинской организации. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

3. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства

3.1. Уполномоченный орган по защите прав субъектов персональных данных.

3.2. Ответственность, предусмотренная за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций студент должен **уметь**:

- осуществлять комплекс организационно-правовых мероприятий по организации защиты ПД и защиты конфиденциальной информации в медицинских организациях;
- организовывать деятельность медицинской организации как оператора ПД;
- принимать управленческие решения, направленные на обеспечение защиты ПД о пациентах и ПД медицинских работников в медицинских организациях;
- выявлять и предотвращать нарушения законодательства в сфере защиты конфиденциальной информации;
- использовать существующее законодательство в сфере защиты ПД при решении конкретных задач по управлению в сфере здравоохранения.

**3. Необходимые базисные знания и умения:**

- навыками организации комплексной системы защиты ПД и конфиденциальной информации медицинских организаций;
- навыками управления по обеспечению организационно-правовых и технических мер, определяемых с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в информационных системах.
- навыками определения типа угроз безопасности ПД, актуальных для информационной системы медицинской организации;
- навыками разработки внутренних нормативных документов, обеспечивающих защиту ПД в информационных системах медицинской организации.

**4. Вид занятия:** практическое занятие.

**5. Продолжительность занятия:** 3 часа.

**6. Оснащение:**

- 6.1. Дидактический материал (ситуационные задачи, тестовые задания по изучаемым темам).
- 6.2 Компьютерный класс, объединенный в локальную вычислительную сеть. На компьютерах установлены серверные версии операционной системы Windows, доступ в глобальную вычислительную сеть Интернет. В целях сохранения результатов работы наличие у обучающихся при себе носителей информации (flash-накопители).

**7. Содержание занятия:**

**7.1. Контроль исходного уровня знаний и умений.**

**Задания для самоконтроля: решение обучающимися индивидуальных наборов тестов по теме**

Выберите один правильный ответ

**1. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, КАСАЮЩИХСЯ СОСТОЯНИЯ ЗДОРОВЬЯ, ДОПУСКАЕТСЯ В СЛУЧАЕ, ЕСЛИ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ**

- 1) осуществляется в медико-профилактических целях
- 2) осуществляется в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну
- 3) необходима для проведения медико-биологических исследований
- 4) необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных

**2. ОБРАБОТКА БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ МОЖЕТ ОСУЩЕСТВЛЯТЬСЯ БЕЗ СОГЛАСИЯ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

- 1) в случаях, предусмотренных законодательством Российской Федерации об обороне
- 2) если обработка данных осуществляется в медико-профилактических целях
- 3) в случаях, предусмотренных законодательством Российской Федерации о противодействии терроризму
- 4) в связи с осуществлением правосудия и исполнением судебных актов

**3. СУБЪЕКТ ПЕРСОНАЛЬНЫХ ДАННЫХ ВПРАВЕ ТРЕБОВАТЬ ОТ ОПЕРАТОРА УТОЧНЕНИЯ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ, ИХ БЛОКИРОВАНИЯ ИЛИ УНИЧТОЖЕНИЯ В СЛУЧАЕ, ЕСЛИ**

- 1) персональные данные являются неполными, устаревшими, неточными
- 2) персональные данные являются незаконно полученными
- 3) персональные данные касаются состояния здоровья субъекта и его семьи
- 4) персональные данные не являются необходимыми для заявленной цели обработки

**4. МЕДИЦИНСКАЯ ОРГАНИЗАЦИЯ ОБРЕТАЕТ СТАТУС ОПЕРАТОРА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТНОСИТЕЛЬНО**

- 1) только своих сотрудников
- 2) только пациентов, которым медицинская помощь оказывается по программе ОМС

3) всех своих сотрудников и пациентов

4) статус оператора не обретает

## 5. К ПРИНЦИПАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТНОСЯТСЯ

1) обработка персональных данных должна осуществляться на законной и справедливой основе

2) принцип гласности и открытости средств и методов защиты информационных систем, обрабатывающих персональные данные

3) принцип соответствия обработки персональных данных достижению конкретных, заранее определенных и законных целей

4) принцип централизации управления информационными системами, обрабатывающими персональные данные, в том числе объединение созданных для различных баз данных информационных систем баз персональных данных

### **7.2. Ознакомление обучающихся с содержанием занятия. Изложение узловых вопросов темы данного занятия. Демонстрация преподавателем методики практических приемов по данной теме. Теоретический разбор темы. Опрос.**

1. Охарактеризуйте понятие «безопасность ПД». Каким образом достигается безопасность ПД?

2. Какой комплекс организационных и технических мероприятий необходимо провести в медицинских организациях для выполнения требований законодательства по персональным данным и устранения возможных угроз безопасности?

3. Какой государственный орган в Российской Федерации является уполномоченным по защите прав субъектов ПД. Перечислите обязанности и основные права уполномоченного органа по защите прав субъектов ПД?

4. Какие государственные органы, помимо уполномоченного органа, осуществляют контроль над системами защиты ПД?

5. Перечислите полномочия ФСТЭК по обеспечению системы защиты ПД.

### **7.3. Решение ситуационных задач**

Ситуационная задача 1. В международном медицинском центре осуществляется передача данных о пациентах в Европейский центр.

Задание. Каким образом провести обезличивание персональных данных

Ситуационная задача 2. Родственники пациента М. обратились к главному врачу больницы с жалобой на нарушение прав пациента при обработке его персональных данных. В жалобе указывалось, что пациент М. при поступлении в больницу не давал письменного согласия на обработку персональных данных. При разборе выяснилось, что больной М. поступил в больницу по скорой помощи в состоянии сопора с открытой черепно-мозговой травмой и множественными переломами костей нижних конечностей. Больной госпитализирован в реанимационное отделение, перенёс несколько операций, находился в состоянии искусственной комы. Больной переведен в нейрохирургическое отделение.

Задание Определите обоснованность жалобы родственников пациента. Приведите дальнейшие действия главного врача

Задание. Используя нормативные правовые акты, предоставленные преподавателем, опишите этапы государственной регистрации биологически активных добавок.

### **7.4. Контроль конечного уровня усвоения темы**

Подготовка к выполнению практических приемов по теме занятия.

Материалы для контроля уровня освоения темы: набор тестовых заданий, ситуационные задачи.

*Место проведения самоподготовки:*

читальный зал, учебная комната для самостоятельной работы обучающихся, компьютерный класс.

Учебно-исследовательская работа обучающихся по данной теме (проводится в учебное время): работа с основной и дополнительной литературой, решение ситуационных задач.

**Литература:**

*Основная:*

Общественное здоровье и здравоохранение : учебник / под ред.: В. А. Миняева, Н. И. Вишнякова. - 5-е изд., перераб. и доп. - М. : МЕДпресс-информ, 2009. - 655 с.	200
Лисицын, Ю.П. Общественное здоровье и здравоохранение [Электронный ресурс] : учебник / Ю. П. Лисицын. - 3-е изд., испр. и доп. - Электрон. текстовые дан. - М. : Гэотар Медиа, 2015. -on-line. - Режим доступа: ЭБС «Консультант студента» <a href="http://www.studmedlib.ru/ru/book/ISBN9785970432914.html">http://www.studmedlib.ru/ru/book/ISBN9785970432914.html</a>	Неограниченный доступ

*Дополнительная*

<b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Текст] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед. ун-т. - Уфа, 2014. - 107,[2] с.	15
<b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Электронный ресурс] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед. ун-т. - Электрон. текстовые дан. - Уфа, 2014. - on-line. - Режим доступа: БД «Электронная учебная библиотека» <a href="http://library.bashgmu.ru/elibdoc/elib582.pdf">http://library.bashgmu.ru/elibdoc/elib582.pdf</a>	Неограниченный доступ

*Нормативные правовые акты в области защиты персональных данных*

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28.01.1981 (с поправками от 15.06.1999)
- Директива № 2002/58/ЕС Европейского парламента и Совета Европейского Союза «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)», Брюссель, 12.07.2002 г. (с изм. и доп. от 25.11.2009).
- Федеральный закон от 21.07.2014 г. № 242-ФЗ (ред. от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»
- Федеральный закон от 21.11.2011 № 323-ФЗ (в ред. от 29.05.2019) «Об основах охраны здоровья граждан в Российской Федерации».
- Федеральный закон Российской Федерации от 25.07.2011г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»
- Федеральный закон от 27.07.2006г. № 152-ФЗ (ред. от 31.12.2017) «О персональных данных»
- Федеральный закон от 27.07.2006г. № 149-ФЗ (в ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 19.12.2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»
- Указ Президента Российской Федерации от 17.03.2008 г. № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
- Указ Президента Российской Федерации от 30.05.2005 г. № 609 (ред. от 23.07.2019) «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»
- Указ Президента Российской Федерации от 06.03.1997г. № 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера»

- Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-РП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»
- Постановление Правительства Российской Федерации от 13.02.2019 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных»
- Постановление Правительства Российской Федерации от 03.02.2012 г. №79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации»
- Постановление Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Приказ Минздравсоцразвития России от 23.04.2012 № 390н «Об утверждении Перечня определенных видов медицинских вмешательств, на которые граждане дают информированное добровольное согласие при выборе врача и медицинской организации для получения первичной медико-санитарной помощи»
- Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
- Приказ Роскомнадзора от 30.05.2017 № 94 (ред. от 30.10.2018) «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»

*Интернет-ресурсы*

База данных «Электронная учебная библиотека»	Свидетельство №2009620253 от 08.05.2009 <a href="http://library.bashgmu.ru">http://library.bashgmu.ru</a>
Электронно-библиотечная система eLIBRARY. Коллекция российских научных журналов по медицине и здравоохранению	ООО РУНЭБ, Договор №750 от 18.12.2018 <a href="http://elibrary.ru">http://elibrary.ru</a>
База данных Scopus	ФГБУ ГПНТБ России, Сублицензионный договор № SCOPUS/50 от 09.10.2019 <a href="https://www.scopus.com">https://www.scopus.com</a>
База данных Web of Science Core Collection	ФГБУ ГПНТБ России, Сублицензионный договор № Wos/50 от 05.09.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
База данных Russian Science Citation Index	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
База данных MEDLINE	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
Консультант Плюс: справочно-правовая система	ООО Компания Права «Респект» Договор о сотрудничестве от 21.03.2012 локальный доступ

**Занятие 4. «Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства»**

**1. Тема и ее актуальность.** «Уполномоченный орган по защите прав субъектов персональных данных. Ответственность, предусмотренная за правонарушения в сфере защиты информации».

Для практической деятельности специалиста в области сестринского дела необходимы знания в области защиты прав субъектов персональных данных, ответственности, предусмотренной за правонарушения в сфере защиты информации

**2. Учебные цели:** овладение знаниями, умениями и навыками в области защите прав субъектов персональных данных

Для формирования профессиональных компетенций обучающийся должен **знать:**

- нормативное правовое регулирование защиты ПД в Российской Федерации и за рубежом;
- основные понятия, используемые в законодательных правовых документах, регламентирующих защиту ПД и конфиденциальной информации в медицинских организациях;
- характеристику медицинской организации как оператора ПД;
- виды конфиденциальной информации, обрабатываемые в медицинских информационных системах;
- основные требования к обеспечению защиты данных о пациенте, врачебной тайны;
- основные требования к защите ПД медицинского работника;
- механизмы контроля и организации надзора за обработкой ПД;
- ответственность, предусмотренную за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций обучающийся должен **владеть и уметь,** и овладеть следующими **компетенциями** (частично):

УК-1. способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Перечисленные компетенции направлены на частичное формирование следующих трудовых функций:

Е/01.8 – Проектирование и организация процессов деятельности медицинской организации. Правовые и организационные вопросы регулирования отношений в сфере обработки персональных данных.

1.Правовые основы института персональных данных. Принципы и условия обработки персональных данных.

Классификация угроз для медицинских информационных систем, основные организационные меры, технические и программные средства защиты информации при организации обработки ПД.

1.1. Категории и источники персональных данных.

1.2. Классификация информационных систем персональных данных (ИС ПД).

1.3. Тип угроз для ИС ПД и уровень защищенности персональных данных.

1.4 Трансграничная передача персональных данных;

Е/02.8 – Управление ресурсами по обеспечению процессов деятельности медицинской организации. Организация защиты персональных данных и конфиденциальной информации в медицинских организациях.

2. Обеспечение безопасности персональных данных в медицинских информационных системах

2.1. Медицинская организация как оператор персональных данных. Персональные данные пациента и врачебная тайна.

2.2. Защита персональных данных медицинского работника. Организация защиты конфиденциальной информации в медицинских организациях;

Е/03.8 – Менеджмент качества и безопасности медицинской деятельности в медицинской организации. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

3. Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства

3.1. Уполномоченный орган по защите прав субъектов персональных данных.

3.2. Ответственность, предусмотренная за правонарушения в сфере защиты информации.

Для формирования профессиональных компетенций студент должен **уметь**:

- осуществлять комплекс организационно-правовых мероприятий по организации защиты ПД и защиты конфиденциальной информации в медицинских организациях;
- организовывать деятельность медицинской организации как оператора ПД;
- принимать управленческие решения, направленные на обеспечение защиты ПД о пациентах и ПД медицинских работников в медицинских организациях;
- выявлять и предотвращать нарушения законодательства в сфере защиты конфиденциальной информации;
- использовать существующее законодательство в сфере защиты ПД при решении конкретных задач по управлению в сфере здравоохранения.

### **3. Необходимые базисные знания и умения:**

- навыками организации комплексной системы защиты ПД и конфиденциальной информации медицинских организаций;
- навыками управления по обеспечению организационно-правовых и технических мер, определяемых с учетом актуальных угроз безопасности ПД и информационных технологий, используемых в информационных системах.
- навыками определения типа угроз безопасности ПД, актуальных для информационной системы медицинской организации;
- навыками разработки внутренних нормативных документов, обеспечивающих защиту ПД в информационных системах медицинской организации.

**4. Вид занятия:** практическое занятие.

**5. Продолжительность занятия:** 3 часа.

### **6. Оснащение:**

6.1. Дидактический материал (ситуационные задачи, тестовые задания по изучаемым темам).

6.2 Компьютерный класс, объединенный в локальную вычислительную сеть. На компьютерах установлены серверные версии операционной системы Windows, доступ в глобальную вычислительную сеть Интернет. В целях сохранения результатов работы наличие у обучающихся при себе носителей информации (flash-накопители).

### **7. Содержание занятия:**

#### **7.1. Контроль исходного уровня знаний и умений.**

Задания для самоконтроля: решение обучающимися индивидуальных наборов тестов по теме  
Выберите один правильный ответ

1. РЕЕСТР МЕДИЦИНСКИХ ОРГАНИЗАЦИЙ, ЯВЛЯЮЩИХСЯ ОПЕРАТОРАМИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, СОСТАВЛЯЕТ

- 1) Федеральная служба безопасности Российской Федерации
- 2) управление информационных и аналитических технологий субъекта Российской Федерации
- 3) федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи
- 4) Министерство здравоохранения Российской Федерации

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ПРОДВИЖЕНИЯ МЕДИЦИНСКИХ УСЛУГ, ПРЕДОСТАВЛЯЕМЫХ МЕДИЦИНСКОЙ ОРГАНИЗАЦИЕЙ, РАСШИРЕНИЯ КЛИЕНТСКОЙ БАЗЫ, ПРИВЛЕЧЕНИЯ НОВЫХ ИНВЕСТОРОВ ДЛЯ ЗАКЛЮЧЕНИЯ ДОГОВОРОВ ДМС

- 1) допускается только при условии предварительного согласия субъекта персональных данных
- 2) допускается при использовании информации на бумажных носителях
- 3) допускается при автоматизированной обработке данных
- 4) допускается без согласия субъекта персональных данных

### 3. МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ, КАК ОПЕРАТОРЫ, НЕ ОБЯЗАНЫ ПОДАВАТЬ УВЕДОМЛЕНИЕ В РОСКОНАДЗОР ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

- 1) обрабатываемых в соответствии с Трудовым кодексом Российской Федерации
- 2) сделанных субъектом персональных данных общедоступными;
- 3) включающих только фамилии, имена и отчества субъектов персональных данных
- 4) включающих фамилии, имена и отчества, адреса и заключительные диагнозы пациентов

### 4. В СЛУЧАЕ ДОСТИЖЕНИЯ ЦЕЛЕЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОР ОБЯЗАН ПРЕКРАТИТЬ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ОБЕСПЕЧИТЬ ЕЕ ПРЕКРАЩЕНИЕ И УНИЧТОЖИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ИЛИ ОБЕСПЕЧИТЬ ИХ УНИЧТОЖЕНИЕ

- 1) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных
- 2) в срок, не превышающий шестидесяти дней с даты достижения цели обработки персональных данных
- 3) в срок, не превышающий месяца с даты достижения цели обработки персональных данных
- 4) в срок, не превышающий года с даты достижения цели обработки персональных данных

### 5. В СЛУЧАЕ ВЫЯВЛЕНИЯ НЕПРАВОМЕРНОЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ ОПЕРАТОРОМ ИЛИ ЛИЦОМ, ДЕЙСТВУЮЩИМ ПО ПОРУЧЕНИЮ ОПЕРАТОРА, ОПЕРАТОР ОБЯЗАН ПРЕКРАТИТЬ НЕПРАВОМЕРНУЮ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ОБЕСПЕЧИТЬ ЕЕ ПРЕКРАЩЕНИЕ ЛИЦОМ, ДЕЙСТВУЮЩИМ ПО ПОРУЧЕНИЮ ОПЕРАТОРА

- 1) в срок, не превышающий трех рабочих дней с даты этого выявления
- 2) в срок, не превышающий пяти рабочих дней с даты этого выявления
- 3) в срок, не превышающий трех календарных дней с даты этого выявления
- 4) в срок, не превышающий пяти календарных дней с даты этого выявления

### **7.2. Ознакомление обучающихся с содержанием занятия. Изложение узловых вопросов темы данного занятия. Демонстрация преподавателем методики практических приемов по данной теме.**

#### **7.3. Теоретический разбор темы. Опрос.**

1. К каким видам ответственности могут быть привлечены виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работника.
2. Какие меры дисциплинарного взыскания и в каком порядке можно применить к работнику за разглашение ПД.
3. Какая ответственность может наступить за осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии), если такое разрешение (лицензия) обязательно
4. Какую ответственность несут лица, виновные в нарушении требований законодательства о ПД.
5. Какие государственные органы, помимо уполномоченного органа, осуществляют контроль над системами защиты ПД.

#### **7.4. Решение ситуационных задач**

1. Какие государственные органы, помимо уполномоченного органа, осуществляют контроль над системами защиты ПД.
2. Что включено в понятие «ПД работника». Какие документы включает личное дело работника. Какими документами регламентируется защита ПД работника.
3. Приведите примеры оформления согласия работника на обработку ПД.

#### **7.5. Контроль конечного уровня усвоения темы**

Подготовка к выполнению практических приемов по теме занятия.

Материалы для контроля уровня освоения темы: набор тестовых заданий, ситуационные задачи.

*Место проведения самоподготовки:*

читальный зал, учебная комната для самостоятельной работы обучающихся, компьютерный класс.

Учебно-исследовательская работа обучающихся по данной теме (проводится в учебное время): работа с основной и дополнительной литературой, решение ситуационных задач.

## Литература:

*Основная:*

Общественное здоровье и здравоохранение : учебник / под ред.: В. А. Миняева, Н. И. Вишнякова. - 5-е изд., перераб. и доп. - М. : МЕДпресс-информ, 2009. - 655 с.	200
Лисицын, Ю.П. Общественное здоровье и здравоохранение [Электронный ресурс] : учебник / Ю. П. Лисицын. - 3-е изд., испр. и доп. - Электрон. текстовые дан. - М. : Гэотар Медиа, 2015. -on-line. - Режим доступа: ЭБС «Консультант студента» <a href="http://www.studmedlib.ru/ru/book/ISBN9785970432914.html">http://www.studmedlib.ru/ru/book/ISBN9785970432914.html</a>	Неограниченный доступ

*Дополнительная*

<b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Текст] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед. ун-т. - Уфа, 2014. - 107,[2] с.	15
<b>Нагаев, Р. Я.</b> Защита персональных данных в медицинских организациях: практические вопросы [Электронный ресурс] : учеб. пособие / Р. Я. Нагаев, С. Г. Ахмерова, С. Ф. Шамгулова ; Башк. гос. мед. ун-т. - Электрон. текстовые дан. - Уфа, 2014. - on-line. - Режим доступа: БД «Электронная учебная библиотека» <a href="http://library.bashgmu.ru/elibdoc/elib582.pdf">http://library.bashgmu.ru/elibdoc/elib582.pdf</a>	Неограниченный доступ

*Нормативные правовые акты в области защиты персональных данных*

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28.01.1981 (с поправками от 15.06.1999)
- Директива № 2002/58/ЕС Европейского парламента и Совета Европейского Союза «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи)», Брюссель, 12.07.2002 г. (с изм. и доп. от 25.11.2009).
- Федеральный закон от 21.07.2014 г. № 242-ФЗ (ред. от 31.12.2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»
- Федеральный закон от 21.11.2011 № 323-ФЗ (в ред. от 29.05.2019) «Об основах охраны здоровья граждан в Российской Федерации».
- Федеральный закон Российской Федерации от 25.07.2011г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»
- Федеральный закон от 27.07.2006г. № 152-ФЗ (ред. от 31.12.2017) «О персональных данных»
- Федеральный закон от 27.07.2006г. № 149-ФЗ (в ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации»
- Федеральный закон от 19.12.2005г. № 160-ФЗ «О ратификации Конвенции Совета

- Европы о защите физических лиц при автоматизированной обработке персональных данных»
- Указ Президента Российской Федерации от 17.03.2008 г. № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
  - Указ Президента Российской Федерации от 30.05.2005 г. № 609 (ред. от 23.07.2019) «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»
  - Указ Президента Российской Федерации от 06.03.1997г. № 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера»
  - Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-РП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»
  - Постановление Правительства Российской Федерации от 13.02.2019 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных»
  - Постановление Правительства Российской Федерации от 03.02.2012 г. №79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации»
  - Постановление Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
  - Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
  - Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
  - Приказ Минздравсоцразвития России от 23.04.2012 № 390н «Об утверждении Перечня определенных видов медицинских вмешательств, на которые граждане дают информированное добровольное согласие при выборе врача и медицинской организации для получения первичной медико-санитарной помощи»
  - Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
  - Приказ Роскомнадзора от 30.05.2017 № 94 (ред. от 30.10.2018) «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»

*Интернет-ресурсы*

База данных «Электронная учебная библиотека»	Свидетельство №2009620253 от 08.05.2009 <a href="http://library.bashgmu.ru">http://library.bashgmu.ru</a>
Электронно-библиотечная система eLIBRARY. Коллекция российских научных журналов по медицине и здравоохранению	ООО РУНЭБ, Договор №750 от 18.12.2018 <a href="http://elibrary.ru">http://elibrary.ru</a>
База данных Scopus	ФГБУ ГПНТБ России, Сублицензионный договор № SCOPUS/50 от 09.10.2019 <a href="https://www.scopus.com">https://www.scopus.com</a>
База данных Web of Science Core Collection	ФГБУ ГПНТБ России, Сублицензионный договор № Wos/50 от 05.09.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>

Баз данных Russian Science Citation Index	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
База данных MEDLINE	НП НЭИКОН, Сублицензионный договор № 03011000496190006950001 от 06.12.2019 <a href="http://apps.webofknowledge.com">http://apps.webofknowledge.com</a>
Консультант Плюс: справочно-правовая система	ООО Компания Права «Респект» Договор о сотрудничестве от 21.03.2012 локальный доступ