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

Кафедра общественного здоровья и управления здравоохранением

МЕТОДИЧЕСКИЕ РАЗРАБОТКИ

ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

ДИСЦИПЛИНА:

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗДРАВООХРАНЕНИИ

Направление подготовки (код, специальность):	38.03.01 Экономика
Направленность (бакалаврская программа)	«Экономика и управление в здравоохранении»
Форма обучения:	очная
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.

Введение

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.

Самостоятельная работа обучающегося.

Виды самостоятельной работы: подготовка к занятиям, подготовка к тестированию, подготовка к текущему контролю

Виды СРО

Виды СР (АУДИТОРНАЯ РАБОТА)

№ п/п	№ семестра	Тема СР	Виды СР - выполнение аудиторной контрольной работы; - выполнение индивидуальных и групповых заданий преподавателя; - отработка практических навыков, - решение практических заданий; - разбор ситуаций; - изучение нормативных и иных материалов; - использование справочной литературы; - чтение и анализ текстов (нормативных актов, учебной литературы и т.п.) - написании истории родов, истории болезни; - иные формы, предусмотренные рабочей программой дисциплины	Всего часов
1	2	3	4	5
1	1	Правовые и организационные вопросы регулирования отношений в сфере обработки персональных данных	- изучение нормативных и иных материалов - решение практических заданий - разбор ситуаций	2
2	1	Организация защиты персональных данных и конфиденциальной информации	- изучение нормативных и иных материалов - решение практических заданий	2

		в медицинских организациях		
ИТОГО часов в семестре:				**4**

Виды СР (ВНЕАУДИТОРНАЯ РАБОТА)

№ п/п	№ семестра	Тема СР	**Виды СР** - подготовка к практическим занятиям; - подготовка к лекциям; - выполнение практических заданий (решение задач, разбор ситуации) - выполнение внеаудиторной контрольной работы; - конспектирование источников; - аннотирование, рецензирование текста; - работа с электронными ресурсами; - чтение учебной литературы, текстов лекций; - подготовка ко всем видам промежуточной аттестации (зачетам, экзаменам, в том числе итоговым аттестационным испытаниям); - подготовка отчетов о прохождении практик; - подготовка и написание рефератов, курсовых работ, выпускной квалификационной работы; - подготовка к участию в научно-практических конференциях; - оформление мультимедийных презентаций учебных разделов; - иные формы.	Всего часов
1	2	3	4	5
1	1	Категории и источники персональных данных	- подготовка к лекциям, - подготовка к практическим занятиям, - изучение учебной литературы, законодательных, нормативных и правовых документов, текстов лекций, - работа с электронными ресурсами, - подготовка к текущему контролю	12
2	1	Медицинская организация как оператор персональных данных.	- подготовка к практическим занятиям, - изучение учебной литературы, законодательных, нормативных и правовых документов, текстов лекций, - работа с электронными ресурсами, - выполнение практических заданий (решение задач, разбор ситуаций, нормативно-правовой документации, составление локальных актов медицинских организаций), - подготовка к текущему контролю	12
3	1	Организация защиты конфиденциальной информации в медицинских организациях. Персональные данные пациента и врачебная тайна. Защита персональных данных медицинского работника.	- подготовка к практическим занятиям, - изучение учебной литературы, законодательных, нормативных и правовых документов, текстов лекций, - выполнение практических заданий (решение задач, разбор ситуаций, нормативно-правовой документации), - подготовка к текущему контролю	12

4	1	Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства	- подготовка к практическим занятиям, - работа с электронными ресурсами, - выполнение практических заданий (решение задач, разбор ситуаций, нормативно-правовой документации), - подготовка к текущему контролю - подготовка к промежуточному контролю	12
ИТОГО часов в семестре:				**48**

При изучении учебной дисциплины «Защита персональных данных в здравоохранении» необходимо использовать нормативные правовые акты в области персональных данных и освоить практические умения с использованием Интернет-ресурсов.

Практические занятия проводятся в виде опроса, использования наглядных пособий, решения ситуационных задач, ответов на тестовые задания.

Удельный вес занятий, проводимых в интерактивных формах, составляет не менее 70% от аудиторных занятий.

Самостоятельная работа обучающихся подразумевает подготовку к опросу, тестированию. Работа с учебной литературой рассматривается как вид учебной работы по дисциплине «Защита персональных данных в здравоохранении» и выполняется в пределах часов, отводимых на её изучение (в разделе СРО).

Каждый обучающийся обеспечен доступом к библиотечным фондам университета и кафедры.

По каждому разделу учебной дисциплины разработаны методические указания для обучающихся «Защита персональных данных в здравоохранении» и методические рекомендации для преподавателей «Защита персональных данных в здравоохранении».

Исходный уровень знаний, обучающихся определяется тестированием, текущий контроль усвоения предмета определяется устным опросом в ходе занятий, при решении типовых ситуационных задач и ответах на тестовые задания.

В конце изучения учебной дисциплины «Защита персональных данных в здравоохранении» проводится промежуточный контроль знаний с использованием тестового контроля, с проверкой практических умений и решением ситуационных задач.

Вопросы по учебной дисциплине «Защита персональных данных в здравоохранении» включены в Итоговую государственную аттестацию выпускников.

Лист актуализации заполняется ежегодно при наличии изменений в названии учреждения, кафедры, пересмотра учебного плана, обновлений в списке литературы и др.

Тема 1. «Правовые и организационные вопросы регулирования отношений в сфере обработки персональных данных»

Тема: «Правовые и организационные вопросы регулирования отношений в сфере обработки персональных данных».

Цель изучения темы: ознакомиться с нормативно-правовым регулированием медицинской деятельности в Российской Федерации в рамках подготовки к практическому занятию по соответствующей теме.

Задачи:

– рассмотреть основные нормативные правовые акты в сфере медицинской деятельности в Российской Федерации.

Обучающийся должен знать:

1. До изучения темы (базисные знания):

– методы и приемы устного и письменного изложения предметного материала, основы проведения анализа литературных источников;
– проведение критического анализа научной и публицистической литературы.
2. После изучения темы:
– основные нормативные правовые акты в сфере медицинской деятельности в Российской Федерации.

должен владеть:

– навыками использования нормативных правовых актов в сфере медицинской деятельности в Российской Федерации.

должен уметь:

– использовать нормативные правовые акты в сфере медицинской деятельности в Российской Федерации.

должен сформировать компетенции (частично):

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

Задания для самостоятельной контактной работы обучающихся по указанной теме

Перечень контрольных вопросов по теме

1. Основные нормативные правовые документы, содержащие положения защиты информации в сфере здравоохранения.
2. Дайте определение персональных данных (далее – ПД). Что входит в понятие «обработка ПД».
3. Назовите принципы обработки ПД. Укажите условия обработки ПД.
4. Что относится к общедоступным источникам ПД. Приведите примеры.
5. Перечислите сведения, относящиеся к специальным категориям ПД. В каких случаях допускается обработка специальных категорий ПД без согласия субъекта ПД. Дайте характеристику биометрическим персональным данным.
6. Перечислите ИСПД в зависимости от категории и типа субъекта ПД.
7. Что понимается под актуальными угрозами безопасности. Назовите типы угроз.

Тестовый контроль знаний:

Выберите один правильный ответ

1. К ОБЩЕДОСТУПНОМУ ИСТОЧНИКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТНОСИТСЯ

1. телефонный справочник
2. адресная книга
3. библиографический энциклопедический справочник
4. список пациентов, представленный в приемном покое медицинской организации

2. ЦЕЛЬ ФЕДЕРАЛЬНОГО ЗАКОНА ОТ 27.07.2006 № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

1. упорядочение сбора, систематизации, использования, накопления, хранения и иных действий (операций) с персональными данными
2. обеспечение защиты прав и свобод человека и гражданина при обработке его ПД, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну
3. обеспечение защиты прав и свобод человека и гражданина при его обращении в федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, иные государственные органы, органы местного самоуправления
4. упорядочение автоматизированной обработки ПД

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ - ЭТО

1) временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачу
2) действия, результатом которых возникает невозможность хранения и иные действия (операции) с персональными данными

3) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

4) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе или в результате которых уничтожаются материальные носители персональных данных

Ознакомление обучающихся с содержанием занятия

Понятие конфиденциальной информации и закрепление его в законодательстве

Информация приобретает все большее значение, важность и коммерческую ценность, а значит и необходимость защиты от посторонних посягательств. В соответствии со ст. 2 Федерального закона от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Рассматривая соотношение понятий

- конфиденциальная информация,
- служебная тайна,
- врачебная тайна необходимо обратиться, прежде всего, к содержанию самих понятий.

Конфиденциальность информации. Данное понятие упоминается в тексте ст. 727 ГК РФ. Под ним понимается обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Указ Президента РФ "Об утверждении перечня сведений конфиденциального характера" утвердил шесть категорий таких сведений.

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные).

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна). Служебная тайна - служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами, информация, представляющая собой объект гражданских прав в случае, если она имеет действительную или потенциальную коммерческую ценность, обусловленную ее неизвестностью третьим лицам в силу отсутствия к ней доступа на законном основании и принятия обладателем информации, мер к охране ее конфиденциальности (ГК РФ, ст. 139). Режим охраны информации, составляющей служебную тайну, законодательством четко не определен.

4. Сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.). Врачебная тайна - сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (ст. 13 Федерального закона № 323-ФЗ).

5. Сведения, связанные с коммерческой деятельностью (коммерческая тайна). Коммерческая тайна. В соответствии с Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (ст. 3) коммерческая тайна - это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. В законе О коммерческой тайне, в том числе, приводится перечень сведений, в отношении

которых режим КТ не может быть установлен лицами, осуществляющими предпринимательскую деятельность (например, учредительные документы; документы, дающие право на осуществление предпринимательской деятельности; о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест; и пр.)

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Цели, принципы и условия обработки персональных данных

Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из ФЗ-152 «О персональных данных» и других определяющих случаи и особенности обработки ПД федеральных законов.

Согласно данному Закону *персональные данные* - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Именно эти данные накапливаются в информационных системах медицинских организаций.

Под обработкой ПД подразумевают: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПД.

Принципы обработки персональных данных:

1. Обработка ПД должна осуществляться на законной и справедливой основе.

2. Обработка ПД должна ограничиваться достижением конкретных, заранее определенных и законных целей.

3. Не допускается объединение баз данных, содержащих ПД, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только ПД, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых ПД должны соответствовать заявленным целям обработки.

6. При обработке ПД должны быть обеспечены точность ПД, их достаточность, а также актуальность по отношению к целям обработки ПД.

7. Хранение ПД должно осуществляться в форме, позволяющей определить субъекта ПД, не дольше, чем этого требуют цели обработки ПД, если срок хранения ПД не установлен Законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД.

Условия обработки персональных данных. Обработка ПД допускается в следующих случаях:

1) обработка ПД осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка ПД необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) если обработка ПД необходима:

- для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги,

для регистрации субъекта ПД на едином портале государственных и муниципальных услуг;

- для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПД, а также для заключения договора по инициативе субъекта ПД или договора, по которому субъект ПД будет являться выгодоприобретателем или поручителем;

- для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД, если получение согласия субъекта ПД невозможно;

- необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПД;

- необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПД;

4) обработка ПД осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Закона, при условии обязательного обезличивания ПД;

5) осуществляется обработка ПД, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Оператор вправе поручить обработку ПД другому лицу с согласия субъекта ПД, если иное не предусмотрено Законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта.

Лицо, осуществляющее обработку ПД по поручению оператора, обязано соблюдать принципы и правила обработки ПД, предусмотренные Законом. В поручении оператора должны быть определены перечень действий (операций) с ПД, которые будут совершаться лицом, осуществляющим обработку ПД, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПД и обеспечивать безопасность ПД при их обработке.

Лицо, осуществляющее обработку ПД по поручению оператора, не обязано получать согласие субъекта ПД на обработку его ПД.

В случае, если оператор поручает обработку ПД другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку ПД по поручению оператора, несет ответственность перед оператором.

Операторы и иные лица, получившие доступ к ПД, обязаны не раскрывать третьим лицам и не распространять ПД без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Источники и категории персональных данных

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. Общедоступные ПД относятся к 4-й категории персональных данных, конфиденциальность для которых обеспечивать не требуется.

В целях информационного обеспечения могут создаваться *общедоступные источники персональных данных* (в том числе справочники, адресные книги). В общедоступные источники ПД с письменного согласия субъекта ПД могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом ПД.

Сведения о субъекте ПД должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта ПД либо по решению суда или иных уполномоченных государственных органов.

Обработка *специальных категорий персональных данных*, касающихся расовой,

национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается. Обработка указанных специальных категорий ПД допускается в случаях, если субъект ПД дал согласие в письменной форме на обработку своих ПД или, если ПД сделаны общедоступными субъектом ПД.

Законом определяется, что обработка специальных категорий ПД, без согласия субъекта ПД допускается в случае, если:

- обработка ПД необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- обработка ПД осуществляется в соответствии с Федеральным законом от 25 января 2002 года № 8-ФЗ «О Всероссийской переписи населения»;
- обработка ПД осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
- обработка ПД необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПД невозможно;
- обработка ПД осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка ПД осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка ПД членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПД не будут распространяться без согласия в письменной форме субъектов ПД;
- обработка ПД необходима для установления или осуществления прав субъекта ПД или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка ПД осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка ПД осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- обработка ПД осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.

Обработка ПД о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Биометрические персональные данные содержат сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность. При использовании оператором биометрических ПД их обработка в целях установления личности субъекта ПД допускается только при наличии согласия в письменной форме субъекта ПД.

Обработка биометрических ПД может осуществляться без согласия субъекта ПД в

связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

Определение класса защищенности информационной системы персональных данных (ИСПД)

До 11 марта 2013 г. все организации, в том числе государственные и муниципальные органы, которые осуществляют обработку персональных данных, обязаны были проводить классификацию информационных систем, а также определять цели и содержание такой обработки.

Классификация ИСПД осуществлялась согласно Приказу ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 18.02.2009 г. «Об утверждении порядка проведения классификации информационных систем персональных данных».

Классификация проводилась с целью определения способов и методов, которые необходимо было применять для защиты персональных данных. Классификация проводилась как на стадии создания информационной системы, так и на стадии ее модернизации.

В настоящее время процедура классификации проводится только для Государственных информационных систем (Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»).

Для обычных ИСПДн проводится определение уровня защищенности.

Уровень защищенности зависит от:

- категорий данных;
- актуальных угроз;
- числа людей, обработка ПД которых осуществляется;
- контингента граждан – субъектов этих данных

Для определения класса защищенности ИСПД необходимо определить категорию обрабатываемых персональных данных:

- категория 1: ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

- категория 2: ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1;

- категория 3: ПД, позволяющие идентифицировать субъекта ПД;

- категория 4: обезличенные и (или) общедоступные ПД.

Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

- высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;
- средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;
- низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Класс защищенности информационной системы определяется в соответствии с таблицей:

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

Трансграничная передача персональных данных

Трансграничная передача ПД на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПД, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов ПД, осуществляется в соответствии с Законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

Уполномоченный орган по защите прав субъектов ПД утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПД и обеспечивающих адекватную защиту прав субъектов ПД. Государство, не являющееся стороной данной Конвенции Совета Европы, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПД, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности ПД.

Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПД, обеспечивается адекватная защита прав субъектов ПД, до начала осуществления трансграничной передачи.

Трансграничная передача ПД на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПД, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта ПД на трансграничную передачу его ПД;
- предусмотренных международными договорами Российской Федерации;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект ПД;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта ПД или других лиц при невозможности получения согласия в письменной форме субъекта ПД.

Глоссарий. Основные понятия, используемые в области персональных данных

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не

всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией,

поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Персональные медицинские данные

Основными понятиямия, связанными с персональными данными медицинской организации являются:

Идентификатор пациента – уникальный символьный или цифровой код, применяемый для обозначения пациента и относящихся к нему данных в определенной учетной системе (системе учета).

Медицинские данные пациента – сведения о физиологических особенностях организма, перенесенных заболеваниях, состоянии здоровья и (или) оказанной пациенту медицинской помощи.

Персонифицированные данные – совокупность сведений, включающая персональные данные пациента, которые позволяют идентифицировать его личность.

Обезличивание данных (деперсонификация) – действия по удалению персональных данных пациента, в результате которого ни при каких условиях невозможно определить принадлежность медицинских данных конкретному физическому лицу и идентифицировать его личность. Обезличенные данные не являются конфиденциальными. Обезличивание данных используется в тех случаях, когда не требуется сопоставление медицинских данных с конкретным пациентом, например, для их статистической обработки, научных и учебных целей и т.д.

Анонимизация данных – использование для обозначения (пометки) медицинских данных (документов), относящихся к некоторому пациенту, его условного имени – криптонима (от греч. "kryptos" – тайный, скрытый и "onyma" – имя), раскрытие которого возможно только самим пациентом. Предполагается, что при использовании криптонима для идентификации пациента его персональные данные в учетной системе не хранятся. Ответственность за раскрытие своего криптонима несет только сам пациент. Анонимные данные не являются конфиденциальными, поэтому согласия пациента на их обработку не требуется. Анонимизация данных используется, в частности, в тех случаях, когда пациент сам организует сбор, накопление и передачу на хранение своих медицинских данных, например, на серверах в сети Интернет (проекты Google Helath и Microsoft HealthVault), а также при анонимном лечении.

Псевдонимизация данных – совокупность организационно-технических мероприятий, процедур и действий по присвоению пациенту специального псевдонима (от греч. «pseudo» – ложный и «onyma» – имя) для передачи, сбора, хранения и обработки его медицинских данных, исключающая возможность его несанкционированного сопоставления с конкретным физическим лицом и идентификацию его личности. Формирование псевдонима и его обратное сопоставление с персональными данными пациента осуществляется с помощью криптографических средств, использование которых жестко регламентировано. Псевдоним никогда не указывается на медицинских и иных документах, содержащих персональные данные пациента; не известен пациенту и поэтому не может быть им раскрыт или передан кому; может быть сопоставлен с персональными данными пациента (дешифрован) только с согласия пациента либо в иных случаях, предусмотренных законодательством;

персональный перечень должностных лиц, которым в этих случаях стала известна информация о соответствии псевдонима конкретному пациенту (его персональным данным) строго определен и также известен. Псевдонимизированные данные не содержат персональных данных пациентов и в этом смысле уже не являются конфиденциальными, что позволяет осуществлять их обработку без согласия пациентов (это положение законодательно определено, например, в Великобритании). Псевдонимизация персонифицированных сведений целесообразна при организации "сводных" медицинских баз данных (БД), когда: а) круг пользователей БД достаточно широк (например, органы управления здравоохранением, надзорно-контрольные органы, страховые организации и фонды ОМС, научно-исследовательские учреждения и т.д.); б) случаи, когда в процессе обработки и анализа данных пациента может возникнуть необходимость идентификации его личности или непосредственного контакта с ним, например, должностных лиц надзорно-контрольных органов. Примерами подобных псевдонимизированных БД могут являться специализированные медицинские регистры: доноров, онкологический, диабетический и т.д., которые ведутся в Великобритании, Германии и Австралии.

Отличие псевдонимизации от простого шифрования персональных данных пациента заключаются в жесткой регламентации и централизации процедур использования средств шифрования\дешифрования при присвоении псевдонима и его сопоставлении с персональными данными пациента, что в целом и обеспечивает возможность:

– сбора и интеграции медицинских данных пациента, помеченных его "единым" псевдонимом из многих независимых источников (учреждений);

– получения "открытого" доступа широкого круга пользователей к сводным медицинским базам данных пациентов без какого-либо риска нарушения их конфиденциальности.

Принципиально важным является то, что пользователям псевдонимизированных медицинских БД какие-либо критографические средства для обработки псевдонимов не нужны. При этом значительно снижаются требования к средствам защиты таких баз данных и существенно сокращаются совокупные расходы на их создание и эксплуатацию.

Полицевые данные – совокупность данных, относящихся к некоторому физическому лицу (пациенту). В зависимости от наличия в их составе персональных данных и используемых идентификаторов пациентов, полицевые данные могут быть: а) персонифицированными, б) псевдонимизированными, в) анонимными и г) обезличенными.

Деперсонифицированные данные – анонимные данные, а также данные, полученные в результате псевдонимизации или обезличивания.

Принято разделять "полицевые" медицинские данные, их потоки и хранилища (базы данных) на две категории:

1. *Первичные медицинские данные*, которые формируются и используются медицинскими работниками непосредственно в процессе оказания медицинской помощи пациенту и ведения электронной медицинской карты в медицинском учреждении. Доступ к персонифицированным "первичным" данным строго ограничен и жестко регламентирован законодательством.

2. *Вторичные данные* – интегрированные, агрегированные полицевые медицинские данные, формируемые на основе "первичных" данных, поступающих из множества лечебных учреждений. Обычно, такие данные накапливаются в течение продолжительного времени в виде различных "сводных" БД, используемых органами управления для анализа, планирования, выполнения надзорно-контрольных функций, ведения "листов ожидания", а также экспертизы, оплаты (клиринга), эпидемиологических и иных научных исследований и т.д. Пользователи таких БД, как правило, непосредственно не оказывают медицинскую помощь пациентам. Формирование и ведение "сводных" БД в общем случае осуществляется вне медицинских учреждений в специальных центрах сбора и обработки данных. В последнее время наблюдается тенденция ведения "вторичных" баз данных в псевдонимизированном или обезличенном виде. Примерами таких сводных

псевдонимизированных БД являются канцер-регистры в Великобритании, Германии и Австралии (см. выше).

Разделение медицинских данных на указанные категории прежде всего обусловлено требованиями законодательства по защите персональных данных. Кроме того, это позволяет существенно снизить риски нарушения конфиденциальности данных пациентов и значительно сократить совокупные расходы на администрирование и эксплуатацию всей системы в целом.

Формы контроля освоения заданий по самостоятельной аудиторной/внеаудиторной работе по данной теме (контрольные вопросы).

Ответьте на следующие вопросы:

1. Определение понятия «персональные данные». Что входит в понятие «обработка ПД»?
2. Что относится к общедоступным персональным данным. Приведите примеры?
3. Основные нормативные правовые документы, содержащие положения защиты информации в сфере здравоохранения.
4. Дайте определение персональных данных (далее – ПД). Что входит в понятие «обработка ПД».
5. Назовите принципы обработки ПД.
6. Укажите условия обработки ПД.
7. Что относится к общедоступным источникам ПД. Приведите примеры.
8. Перечислите сведения, относящиеся к специальным категориям ПД. В каких случаях допускается обработка специальных категорий ПД без согласия субъекта ПД.
9. Дайте характеристику биометрическим персональным данным.
10. Перечислите классы защищенности ИСПД.
11. Что понимается под актуальными угрозами безопасности. Назовите типы угроз.
12. Дайте характеристику информационным системам медицинских организаций, в которых обрабатываются ПД о состоянии здоровья.
13. Приведите алгоритм трансграничной передачи ПД.
14. Дайте определение конфиденциальной информации. Какими нормативными документами регулируется режим конфиденциальности информации. Перечислите категории сведений конфиденциального характера.
15. Дайте характеристику операторам ПД. Каков порядок регистрации в качестве оператора ПД медицинских организаций.
16. Какой государственный орган является уполномоченным по ведению реестра операторов ПД. В каких случаях не требуется уведомление регистрирующего органа.
17. Какие данные пациента в системе персонифицированного учета медицинской организации относятся к ПД.
18. Дайте характеристику врачебной тайны. Каким нормативным документом охраняется врачебная тайна.

Ситуационные задачи.

Ситуационная задача 1. 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 жалобы 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.

Обоснована ли жалоба родственников пациента?

Ситуационная задача 2. Больной М. проживает в сельской местности и наблюдается в центральной районной больнице. После перенесенного ожога у больного М. сохранились язвы и гранулирующие раны на груди, правом плече, верхней трети спины. Показано оперативное лечение. Подобные операции проводятся в нескольких центральных клиниках. Для решения вопроса об оперативном лечении заведующий отделением принимает решение о проведении дистанционной (телемедицинской) консультации.

Необходимо ли в этом случае письменное согласие пациента?

Ситуационная задача 3. Пациент Д. предъявил претензии медицинской организации, указав, что после проведенного лечения по поводу устранения деформаций челюстно-лицевой области в информационной системе медицинской организации остались его фотографии. Письменного согласия на хранение фотографии пациент не давал.

Обоснована ли жалоба пациента? Каким образом можно исправить ситуацию?

Ситуационная задача 4. Согласно п. 7 ст. 21 и п. 7 ст. 79 Закона № 323-ФЗ при выборе врача и медицинской организации гражданин имеет право на получение информации в доступной для него форме, в т. ч. размещенной в информационно-телекоммуникационной сети Интернет. Медицинские организации предоставляют информацию о медицинской организации, об осуществляемой ею медицинской деятельности, о врачах, об уровне их образования и квалификации.

Какую информацию о врачах в информационно-телекоммуникационной сети Интернет можно размещать только с письменного согласия работника?

Разбор ситуационных задач

Ситуационная задача 1. Нет, не обоснована.

Согласие пациента на обработку ПД не требуется в следующих случаях:

- медицинская помощь оказывается по программе обязательного медицинского страхования (ОМС), и персональные данные передаются только в территориальный фонд ОМС и страховую организацию (ст. 38, 39, 43, 44 и 48 Федерального закона № 326-ФЗ);
- персональные данные пациента о состоянии его здоровья передаются третьим лицам (ч. 4 ст. 13 Закона № 323-ФЗ):
- если пациент в результате своего состояния не способен выразить свою волю, но ему необходимо лечение;
- при угрозе распространения инфекционных заболеваний, массовых отравлений;
- по запросу органов дознания и следствия, суда, органа уголовно-исполнительной системы;
- в случае оказания медицинской помощи несовершеннолетнему;
- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются основания полагать, что вред его здоровью причинен в результате противоправных действий;
- в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов;
- в целях расследования несчастного случая на производстве и профессионального заболевания;
- при обмене информацией медицинскими организациями, в т. ч. размещенной в информационных системах, в целях оказания медицинской помощи;
- в целях осуществления учета и контроля в системе обязательного социального страхования;
- в целях осуществления контроля качества и безопасности медицинской помощи.

Ситуационная задача 2. Да, необходимо.

Письменное согласие пациента на передачу (предоставление) его персональных данных, составляющих врачебную тайну, требуется в случаях, когда:

- медицинская помощь оказывается пациенту на платной основе, вне программы государственных гарантий, и сведения передаются третьим лицам (организациям), не являющимся медицинскими организациями, например в страховую компанию и (или) страхователю по дополнительному медицинскому страхованию (в случае, если им не является сам пациент или его законный представитель);

- информация о состоянии здоровья пациента передается лицам, указанным самим пациентом или его законным представителем (ч. 5 ст. 19 Закона № 323-ФЗ); в согласии должны быть указаны фамилия, имя, отчество и контактные данные этих лиц (при этом можно считать, что пациент является представителем этих лиц, в связи с чем их специальное письменное согласие на обработку (хранение) указанных персональных данных в медицинском учреждении не требуется (ч. 1 и 8 ст. 9 Закона «О персональных данных»);

- передача персональных данных (документов) пациента осуществляется по открытым каналам связи (сети Интернет, электронной почте), например, при проведении дистанционных (телемедицинских) консультаций;

- осуществляется трансграничная передача персональных данных пациента, например, при осуществлении телемедицинских консультаций с участием врачей, находящихся в странах, не являющихся сторонами Конвенции Совета Европы по защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. ETS № 108 или не включенных в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, утверждаемый Роскомнадзором (ст. 12 Закона «О персональных данных»).

В настоящее время данную Конвенцию подписали и ратифицировали Австрия, Бельгия, Болгария, Дания, Великобритания, Венгрия, Германия, Греция, Ирландия, Испания, Италия, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Финляндия, Франция, Чехия, Швеция, Эстония.

К странам, обеспечивающим адекватную защиту персональных данных, имеющим общенациональные нормативные правовые акты в области защиты персональных данных и уполномоченный надзорный орган по защите прав субъектов персональных данных, относятся Андорра, Аргентина, Израиль, Исландия, Канада, Лихтенштейн, Норвегия, Сербия, Хорватия, Черногория, Швейцария, Южная Корея, Япония.

Ситуационная задача 3. Да, жалоба обоснована.

В случаях, когда в информационной системе медицинской организации хранятся и обрабатываются биометрические данные пациента (данные геометрии контура кисти руки, изображения отпечатка пальца, сосудистого русла, изображение радужной оболочки глаза, изображение (фотография) лица, данные ДНК и др.), на это необходимо его специальное письменное согласие (ст. 11 Закона «О персональных данных»).

Фотографии необходимо сделать обезличенными таким образом, чтобы по ним нельзя было идентифицировать субъекта персональных данных.

Ситуационная задача 4. Фотографию, так как фотография содержит биометрические данные субъекта персональных данных.

Место проведения самоподготовки:

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

Рекомендуемая литература

Основная литература

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.	Неограниченный доступ

- Электрон. текстовые дан. - М. : Гэотар Медиа, 2015. -on-line. - Режим доступа: ЭБС «Консультант студента» http://www.studmedlib.ru/ru/book/ISBN9785970432914.html	

Дополнительная литература

Нагаев, Р. Я. 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
Нагаев, Р. Я. 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» http://library.bashgmu.ru/elibdoc/elib582.pdf	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.
- Конституция Российской Федерации. Принята на всенародном голосовании 12 декабря 1993г.
- Кодекс Российской Федерации об административных правонарушениях № 195-ФЗ от 30.12. 2001 г. (ред. от 26.07.2019) (с изм. и доп., вступ. в силу с 29.07.2019).
- Трудовой кодекс Российской Федерации от 30.12.2001г. № 197-ФЗ - Глава 14 «Защита персональных данных работника»)
- Уголовный кодекс Российской Федерации № 63-ФЗ от 13.06.1996 г.
- Федеральный закон от 21.07.2014 г. № 242-ФЗ «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 «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 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»
- Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»
- Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»
- Федеральный закон от 27.07.2006г. № 149-ФЗ «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»
- Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» (ред. от 18.04.2018г.)
- Указ Президента Российской Федерации от 17.03.2008 г. № 351 «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 «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 «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 «О лицензировании деятельности по технической защите конфиденциальной информации»
- Постановление Правительства Российской Федерации от 21.03.2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
- Постановление Правительства Российской Федерации от 16.04. 2012 г. №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
- 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 РФ от 04.03.2010г. № 125 "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию"
- Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «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»
- Постановление Правительства Российской Федерации от 03.11.1994г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использования атомной энергии и уполномоченном органе по космической деятельности»
- Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14.11. 2011г. № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых

коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»

- 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 ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
- Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»
- Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст) http://standartgost.ru/.
- Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3.02. 2012 г. № 79.

Интернет-ресурсы по защите персональных данных

База данных «Электронная учебная библиотека»	Свидетельство №2009620253 от 08.05.2009 http://library.bashgmu.ru
Электронно-библиотечная система eLIBRARY. Коллекция российских научных журналов по медицине и здравоохранению	ООО РУНЭБ, Договор №750 от 18.12.2018 http:// elibrary.ru
База данных Scopus	ФГБУ ГПНТБ России, Сублицензионный договор № SCOPUS/50 от 09.10.2019 https://www.scopus.com
Базаданных Web of Science Core Collection	ФГБУ ГПНТБ России, Сублицензионный договор № Wos/50 от 05.09.2019 http://apps.webofknowledge.com
База данных Russian Science Citation Index	НП НЭИКОН, Сублицензионный договор № 0301100049619000695000 1 от 06.12.2019 http://apps.webofknowledge.com
База данныхMEDLINE	НП НЭИКОН, Сублицензионный договор № 0301100049619000695000 1 от 06.12.2019 http://apps.webofknowledge.com
Консультант Плюс: справочно-правовая система	ООО Компания Права «Респект» Договор о сотрудничестве от 21.03.2012 локальный доступ

Тема 2. «Организация защиты персональных данных и конфиденциальной информации в медицинских организациях»

Тема: «Организация защиты персональных данных и конфиденциальной информации в медицинских организациях».

Цель изучения темы: ознакомиться с организацией защиты персональных данных и конфиденциальной информации в медицинских организациях в рамках подготовки к практическому занятию по соответствующей теме.

Задачи:

– рассмотреть основы организации защиты персональных данных и конфиденциальной информации в медицинских организациях.

Обучающийся должен знать:

1. До изучения темы (базисные знания):

– методы и приемы устного и письменного изложения предметного материала, основы проведения анализа литературных источников;

– проведение критического анализа научной и публицистической литературы.

2. После изучения темы:

– основы организации защиты персональных данных и конфиденциальной информации в медицинских организациях.

должен владеть:

– принимать управленческие решения, направленные на обеспечение защиты ПД о пациентах и ПД медицинских работников в медицинских организациях.

должен уметь:

– осуществлять комплекс организационно-правовых мероприятий по организации защиты ПД и защиты конфиденциальной информации в медицинских организациях.

должен сформировать компетенции (частично):

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

Задания для самостоятельной контактной работы обучающихся по указанной теме

Перечень контрольных вопросов по теме

1) Дайте характеристику информационным системам медицинских организаций, в которых обрабатываются ПД о состоянии здоровья.
2) Дайте характеристику операторам ПД. Каков порядок регистрации в качестве оператора ПД медицинских организаций.
3) Какие данные пациента в системе персонифицированного учета медицинской организации относятся к ПД.
4) Дайте характеристику врачебной тайны. Каким нормативным документом охраняется врачебная тайна.
5) Что должно быть включено в согласие пациента на обработку ПД.

Тестовый контроль знаний:

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. МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ, КАК ОПЕРАТОРЫ, ОБЯЗАНЫ ПОДАВАТЬ УВЕДОМЛЕНИЕ В РОСКОМНАДЗОР ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, КРОМЕ 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

3. 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

Ознакомление обучающихся с содержанием занятия

Медицинская организация как оператор персональных данных

Абсолютное большинство информационных ресурсов медицинских организаций содержат те или иные сведения конфиденциального характера (служебная, коммерческая, врачебная тайна).

В соответствии со ст. 727 Гражданского кодекса Российской Федерации под *конфиденциальностью информации* понимается обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» определяет, что к таковым, в частности относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);
- сведения, составляющие тайну следствия и судопроизводства, а также сведения о государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства;
- служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна);
- сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.). В частности, врачебная тайна - сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении;
- сведения, связанные с коммерческой деятельностью (коммерческая тайна);
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Примеры обработки общих и специальных персональных данных приведены в таблице.

В соответствии с частью 4 ст. 9 Закона «Об информации, информационных технологиях и о защите информации» доступ к конфиденциальной информации должен быть ограничен. Соответственно, любая медицинская организация, фонд обязательного медицинского страхования, страховая медицинская организация, являются операторами ПД. Виды конфиденциальной информации, обрабатываемые в медицинских информационных системах, представлены на схеме 1.

Схема 1. Виды конфиденциальной информации, обрабатываемых в медицинских информационных системах

Таблица

Обработка общих и специальных персональных данных в медицинской организации

Общие персональные данные	**Конкретизация данных**	**Примеры обработки**
	Фамилия, имя, отчество, дата и место рождения, адрес, профессия	Обработка персональных данных сотрудников в деятельности кадровых служб ЛПУ
		Обработка персональных данных пациентов в связи с их обращениями в ЛПУ (в рамках обязательного медицинского страхования, добровольного медицинского страхования, для оказания платной медицинской услуги)
	Сведения о доходах лица	Обработка персональных данных сотрудников бухгалтерией ЛПУ
Специальные персональные данные	Сведения о состоянии здоровья, интимной жизни субъекта персональных данных	Обработка персональных данных пациентов в связи с их обращениями в ЛПУ в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну
	Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные)	

Оператором ПД является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

В общем случае оператор ПД должен:

- зарегистрироваться в качестве оператора ПД. Для этого оператор ПД должен подготовить и направить уведомление в территориальный орган Роскомнадзора, который Приказом № 346 определён в качестве уполномоченного органа по ведению реестра операторов, осуществляющих обработку персональных данных. Вышеуказанным приказом определены процедуры по внесению сведений об Операторе в Реестр; изменению сведений об Операторе, исключению сведений об Операторе из Реестра, а также по предоставлению выписки из Реестра;

- получить письменные согласия пациентов (субъектов ПД) на обработку, в том числе передачу их персональных данных, а также на передачу кому-либо сведений, содержащих врачебную тайну;

- обеспечить информирование пациентов по их запросам о целях, способах и сроках обработки, хранения их ПД, а также о лицах, имеющих к ним доступ. Для этого в информационной системе учреждения должны быть реализованы функции разграничения полномочий, аутентификации, регистрации (учёта) и контроля доступа пользователей к ПД, автоматического ведения журналов доступа;

- для определения необходимых мер и выбора средств защиты ПД провести классификацию своей ИС в зависимости от характера (состава) и объема обрабатываемых

ПД и угроз безопасности жизненно важным интересам личности в случае нарушения их конфиденциальности (утечки) и оформить соответствующий документ (все ИС ПД, в которых обрабатываются сведения о состоянии здоровья, в соответствии с требованиями Приказа № 55/86/20 являются системами 1-го класса - К1);

- организовать и поддерживать систему защиты конфиденциальной информации от несанкционированного доступа в соответствии с установленным классом ИС с использованием средств защиты, сертифицированных в установленном порядке; для подтверждения соответствия ИС требованиям защиты конфиденциальной информации и ПД необходимо провести аттестацию системы.

Регистрация медицинской организации в качестве оператора ПД

Регистрация оператора осуществляется в соответствии со ст. 22 Закона. Для регистрации оператор ПД должен подготовить и направить уведомление в территориальный орган Роскомнадзора, который Приказом № 346 определён в качестве уполномоченного органа по ведению реестра операторов, осуществляющих обработку персональных данных. Вышеуказанным приказом определены процедуры по внесению сведений об Операторе в Реестр; изменению сведений об Операторе, исключению сведений об Операторе из Реестра, а также по предоставлению выписки из Реестра.

Типовая форма уведомления утверждена Приказом № 706.

Уведомление должно содержать следующие сведения:

- наименование (фамилия, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

Уведомление должно быть направлено в виде документа на бумажном носителе или в формате электронного документа, подписанное уполномоченным лицом.

Применительно к сфере здравоохранения можно дать следующие комментарии по заполнению некоторых пунктов уведомления территориального органа Роскомнадзора для медицинских организаций.

В пункте формы уведомления «Правовое основание обработки ПД» указать «обработка персональных данных необходима для защиты жизни, ПД и получение согласия субъекта персональных данных невозможно» либо «обработка персональных данных осуществляется в медико-профилактических целях (в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг)». Здесь же можно сослаться на статьи Закона, а в случае обработки ПД работника медицинской организации – на главу 4 ТК РФ.

В пункте «Цель обработки» необходимо указать: «в медико-профилактических целях», либо «в целях установления медицинского диагноза», либо «в целях оказания медицинских и медико-социальных услуг», а также перечислить цели деятельности организации согласно уставу.

В пункте «Категории персональных данных»:

- для пациентов: Ф.И.О., пол, дата рождения, адрес места жительства, реквизиты документа, удостоверяющего личность, реквизиты полиса медицинского страхования, сведения о наличии льгот, СНИЛС (страховой номер индивидуального лицевого счета гражданина в системе персонифицированного учета Пенсионного фонда России), сведения о случаях обращения за медицинской помощью, данные о состоянии здоровья;

- для работников медицинской организации: Ф.И.О., пол, дата и место рождения, адрес места жительства, реквизиты документа, удостоверяющего личность, реквизиты полиса медицинского страхования, СНИЛС, ИНН, сведения о наличии льгот, данные кадрового учёта (образование, квалификация, должность и т. д.), сведения о заработной плате.

Если в ИС хранятся и обрабатываются фотографии пациентов и (или) работников учреждения, то помимо перечисленного в этом поле необходимо также указать (привести) биометрические персональные данные (фотографии) (соответственно работников или пациентов). Для хранения в ИС фотографии пациента или работника в электронном виде обязательно получение его письменного согласия (ст. 11 Закона № 152-ФЗ).

В пункте «Категории субъектов, персональные данные которых обрабатываются» необходимо указать: «работники организации», для пациентов - гражданство («гражданин РФ», «иностранный гражданин», «лицо без гражданства»).

В пункте «Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных» указать: «Смешанная обработка - ввод, сбор, систематизация, накопление, хранение, изменение, удаление, использование, передача по внутренней сети».

Если в медицинской организации формируются массивы персонифицированных данных для передачи во внешние организации (страховые медицинские организации, фонды ОМС, медицинские информационно-аналитические центры и т. п.), необходимо указать способы передачи (на машинных носителях, по защищенным каналам связи и т. п.), привести реквизиты распорядительных документов (приказов и т. п.), на основании которых эти данные передаются.

В соответствии с Постановлением № 687 персональные данные, обрабатываемые на бумажных носителях, должны обособляться от иной информации «путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков)», то есть, путём их представления на отдельных листах, в специальных разделах или в полях форм (бланков) документов. Из этого следует, что подавляющее большинство персонифицированных форм учётно-отчётных документов, которые сегодня используются в здравоохранении, подлежит переработке.

В ряде случаев медицинская организация может обрабатывать персональные данные, не посылая уведомление в адрес уполномоченного органа по ведению реестра операторов, осуществляющих обработку ПД. В соответствии с Законом, уведомление не требуется в следующих случаях:

- если ПД обрабатываются в соответствии с трудовым законодательством (отделы кадров);

- при получении и использовании ПД в связи с заключением договора, стороной которого является субъект персональных данных;

- обработка ПД общественным объединением или религиозной организацией как информации о членах организации;

- обработка ПД, содержащих только Ф.И.О.;

- обработка ПД в целях однократного пропуска субъекта на охраняемую территорию;

- в специальных случаях, предусмотренных законодательством Российской Федерации в целях защиты безопасности государства и общественного порядка (например, при противодействии правонарушениям и терроризму);

- в случаях обработки ПД для обеспечения транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Общий срок внесения сведений об Операторе в Реестр - 15 дней с момента регистрации уведомления. Общий срок внесения изменений в сведения об Операторе в Реестр - 15 дней с момента регистрации информационного письма. Общий срок исключения сведений об Операторе из Реестра - 15 дней с момента регистрации заявления. Срок размещения общедоступных сведений, содержащихся в Реестре, на официальном сайте Роскомнадзора - не позднее 3 дней с даты подписания приказа о внесении сведений об Операторе в Реестр (внесении изменений и исключении сведений об Операторе из Реестра).

Цикл работ по обеспечению информационной безопасности в медицинских организациях

Обработка персональных данных требует создание специального режима, в котором четко определены технология их обработки, порядок и условия существования ПД на каждом этапе их жизненного цикла. Это предусматривает разработку и внедрение процедур их сбора, приема, учета, регистрации, хранения, использования, уничтожения и т.п. Большое значение при этом имеет срок хранения ПД, а также наличие системы контроля обработки ПД на всех этапах их жизненного цикла.

- Этап 1. Аудит и оценка защищённости. На этом этапе оценивается текущее состояние защиты информации, а так же её соответствие обязательным требованиям (зависят от особенностей деятельности организации).
- Этап 2. Составление плана работ по приведению в приемлемое состояние или улучшению системы защиты информации (выбор решения).
- Этап 3. Внедрение новых процессов работы с
- информацией и её защиты и/или средств защиты информации на основе оценки защищенности и выбранного решения. Разработка необходимой организационно-распорядительной документации.
- Этап 4. Сопровождение и поддержание в рабочем состоянии готовой системы защиты информации (это касается, в первую очередь, технических средств). Сопровождение (устранение сбоев в работе, обслуживание, оптимизация работы со средствами защиты информации (СЗИ), плановые и внеплановые проверки состояния СЗИ).
- После проведения проверки состояния системы происходи возврат на этап 1. По результатам контроля, возникает необходимость в доработке системы и снова осуществить весь цикл работ.

Организация защиты конфиденциальной информации в медицинских организациях

Конкретные требования к обеспечению безопасности ПД при их обработке в информационных системах указаны в «Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденном Постановлением Правительства Российской Федерации № 781 от 17 ноября 2007 г.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к ПД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий.

Пример простейшей медицинской информационной системы приведен на схеме 2.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты ПД, включающей:

- организационные меры;
- средства защиты информации (в том числе шифровальные (криптографические) средства;
- средства предотвращения несанкционированного доступа;
- средства предотвращения утечки информации по техническим каналам;
- средства предотвращения программно-технических воздействий на технические средства обработки персональных данных);
- используемые в информационной системе информационные технологии.

Перечисленные выше меры и средства защиты ПД должны использоваться в комплексе и в рамках оператора, работающего с ПД, должны формировать систему защиты ПД. Выпадение из этой системы любого образующего ее звена недопустимо, т.к. ведет к ее уязвимости и разрушению.

В первую очередь, медицинской организации целесообразно составить график мероприятий по организации обработки и защиты персональных данных.

Необходимо издать разработать и издать следующие документы:

1. Приказ «О назначении структурного подразделения или должностного лица, ответственного за организацию обработки персональных данных в медицинской организации».

Приказом должны быть утверждены положение об этом подразделении, должностные инструкции ответственного лица и администраторов безопасности информации, в которых должны быть перечислены их функции, права и обязанности, определены их подчиненность, подотчетность, и особые полномочия. В обязанности ответственного входит:

- осуществление контроля над соблюдением оператором и сотрудниками медицинской организации законодательства о персональных данных и требований к их защите;

- доведение до сведения работников медицинской организации положений законодательства и иных актов (например, локальных актов учреждения), регламентирующих процессы обработки персональных данных, и требований к их защите;

- организация приема и обработки обращений и запросов субъектов персональных данных (работников медицинской организации и пациентов) и осуществление контроля над их приемом и обработкой.

Ответственный за организацию обработки персональных данных подотчетен непосредственно руководителю медицинской организации.

2. Приказ «О допуске сотрудников медицинской организации к обработке ПД».

Приказом утверждается список сотрудников с указанием полномочий их доступа к различным категориям информации, в том числе персональным данным пациентов и работников учреждения. Внесение изменений в список также должно проводиться приказом. Соответствующие изменения вносятся в должностные инструкции указанных в приказе сотрудников.

3. Приказ «О закреплении компьютеров, предназначенных для обработки персональных данных с учетом их работы в составе различных подразделений медицинской организации (например, отдел кадров, бухгалтерия, регистратура), а значит разных ИС ПД».

4. Приказ «О назначении комиссии для проведения обследования и классификации информационной системы обработки персональных данных в медицинской организации».

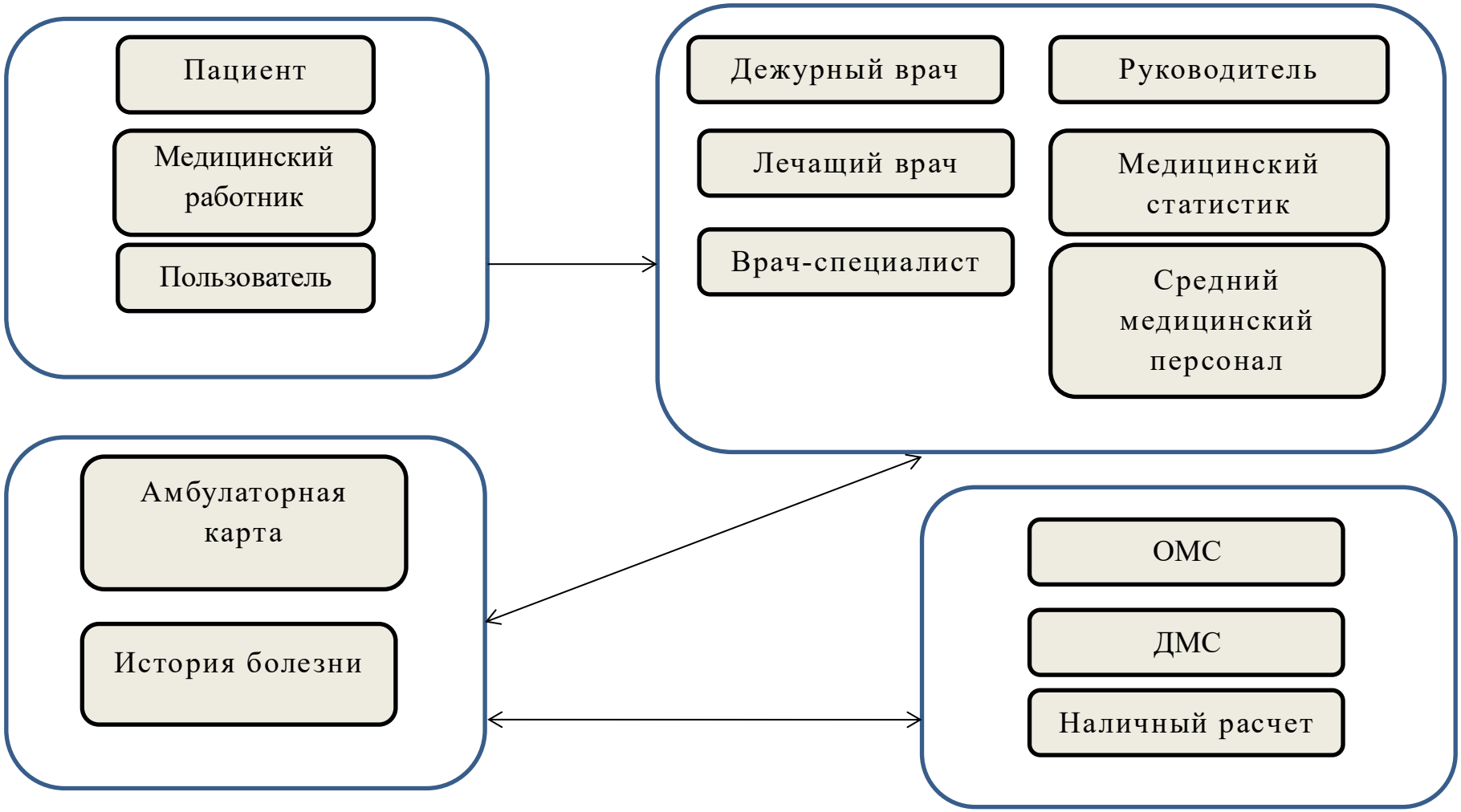

Схема 2. Пример простейшей медицинской информационной системы

Приказом утверждается состав комиссии, цели, задачи и сроки проведения обследования. Основными задачами комиссии являются:

- инвентаризация всех информационных ресурсов в учреждении, обрабатываемых с помощью компьютеров, их категорирование - отнесение к открытой или конфиденциальной информации, в том числе к различным категориям ПД,
- выделение всех отдельных ИС ПД,
- определение класса ИС ПД и оформление акта классификации.

5. Приказ «О проведении обследования информационной системы медицинской организации».

Обследование информационной системы осуществляется с целью систематизации сведений об организации и обрабатываемых данных, выделения систем обработки персональных данных и их классификации в соответствии со ст. 19 Закона № 152-ФЗ, нормативными и методическими документами.

По результатам обследования составляется отчет о результатах обследования информационной системы медицинской организации, который включает перечень и основные характеристики всех ИС, в которых обрабатываются ПД разных категорий.

Отчет должен содержать также:

а) перечень сведений конфиденциального характера, обрабатываемых в учреждении;

б) общее, краткое описание потоков данных как внутри учреждения, так и передаваемых и получаемых внешних ИС с указанием их источников, носителей, периодичностью передачи/получения информации.

Кроме того комиссией составляется Акт классификации ИС ПД медицинской организации, который утверждается руководителем медицинской организации.

Классификация ИС, в которых обрабатываются персональные данные, должна отвечать требованиям документа «Порядок проведения классификации информационных систем персональных данных», утвержденного Приказом № 55/86/20.

Согласно указанному документу классификация осуществляется на основе следующих критериев:

- категория обрабатываемых данных;
- объем обрабатываемых данных (количество субъектов персональных данных;
- характеристика безопасности ПД;
- структура ИС:

– автономные ИС - не подключенные к иным информационным системам;

– комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа - локальные информационные системы;

– на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа - распределенные информационные системы;

- наличие подключения информационной системы к сетям общего пользования или международного информационного обмена (Интернет);
- режим обработки ПД (однопользовательские ИС и многопользовательские);
- режим разграничения прав доступа пользователей информационной системы (системы без разграничения прав доступа и системы с разграничением прав доступа);
- местонахождение технических средств ИМС (системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации).

Присвоение класса ИС осуществляется самим оператором ПД (медицинским учреждением), класс должен быть оформлен документально; заметим, что в соответствии с п. 8 Порядка медицинские ИС относятся к специальным системам, поскольку в них обрабатываются данные о состоянии здоровья пациентов. Как указано в п. 16 Порядка, класс специальных ИС

определяется на основе анализа данных и модели угроз безопасности ПД в соответствии с методическими документами ФСТЭК и ФСБ.

В соответствии с перечисленными выше документами медицинской организации, эксплуатирующие информационные системы классов, обязаны:

а) получить лицензию ФСТЭК на техническую защиту информации (срок действия — пять лет);

б) выполнить все необходимые мероприятия по обеспечению защиты информации для указанных классов информационных систем;

в) провести аттестационные испытания ИС по требованиям ФСТЭК.

При наличии в медицинской организации нескольких ИС ПД, обрабатывающих данные разной категории, ИС ПД в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

После присвоения класса и частной модели угроз безопасности ПД разрабатываются Требования по обеспечению безопасности ПД. Документ должен включать перечень организационных мер и требования к программным, и техническим средствам защиты информации, на основе которых определяется состав и осуществляется выбор средств защиты и(или) разрабатывается техническое задание на создание (модернизацию) системы защиты информации в медицинской организации.

6. Приказ «Об утверждении перечня сведений конфиденциального характера, обрабатываемых в медицинской организации».

Документ разрабатывается по результатам инвентаризации и категорирования информационных ресурсов медицинской организации, которые проводятся в рамках обследования ИС медицинской организации. Включает перечень персональных данных сотрудников и пациентов медицинской организации, подлежащих защите от несанкционированного доступа. Утверждается руководителем.

7. Приказ «Об утверждении Плана мероприятий по обеспечению безопасности ПД медицинской организации».

План мероприятий разрабатывается по результатам обследования ИС в части выполнения установленных требований к безопасности информации. План должен быть комплексным и включать как однократно выполняемые мероприятия, так и постоянно и периодически выполняемые мероприятия.

В Плане необходимо предусмотреть обеспечение мероприятий необходимыми ресурсами, в том числе выделение соответствующих финансовых средств.

Должно быть определено должностное лицо, на которое возлагается контроль за выполнением плана, например, заместитель главного врача.

8. Приказ «О проведении приемочных испытаний системы защиты информации в медицинской организации».

Приказом должна быть назначена комиссия для проведения испытаний, определены сроки испытаний. В приказе должно быть указано, что испытания проводятся в соответствии с утвержденной руководителем учреждения программой и методикой испытаний системы защиты информации.

По результатам испытаний оформляется протокол, содержащий заключение о готовности средств защиты информации к использованию. При положительных результатах испытаний является основанием для:

а) издания приказа о вводе системы защиты информации учреждения в эксплуатацию;

б) оформления декларации подтверждения соответствия информационной системы учреждения требованиям по безопасности информации для систем класса К3.

9. Приказ «О вводе в эксплуатацию системы защиты информации в учреждении».

Издается по результатам приемочных испытаний системы, на основе протокола испытаний. В приказе должны быть назначены ответственные за организацию технической эксплуатации системы и предусмотрено выделение необходимых ресурсов и финансовых средств. Необходимо обратить внимание на необходимость документального подтверждения сертифицированности

средства защиты информации, о чём составляется Акт установки сертифицированных средств защиты информации в медицинской организации.

10. Положение о работе с персональными данными, в котором формулируются общие требования, принципы организации и подходы к обеспечению безопасности информации, порядок доступа различных категорий пользователей к конфиденциальным данным и ресурсам информационной системы в учреждении с учетом специфики его деятельности, меры ответственности за нарушение установленного режима обеспечения безопасности информации и т.д. В положении должно быть определено, когда, как и кем проводится инструктаж и доведение до сотрудников требований и документов по соблюдению установленных требований к защите информации, проведение контроля и т.п. Документ должен содержать перечень всех организационно-методических и учетных документов (инструкций, положений, журналов, ведомостей и др.), определяющих требования к защите информации и регламентирующих процессы обработки конфиденциальных данных в учреждении. Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите ПД.

11. Форму Акта об уничтожении персональных данных, который оформляется в случае отзыва пациентом согласия на обработку его ПД в медицинской организации.

12. Инструкцию пользователю информационной системы по защите ПД – разрабатывается для каждой отдельной ИС ПД в медицинской организации. Инструкция должна содержать: требования к компетенции, права, обязанности и правила работы пользователя ИС в части обеспечения безопасности ПД; меры ответственности пользователя за несоблюдение установленных требований безопасности; перечень всех применяемых мер и средств защиты.

13. Порядок информирования пациентов об обработке их ПД в медицинской организации.

Информирование пациентов об обработке их ПД - цели, способы и сроки обработки, список лиц, имеющих доступ к их ПД. Информирование осуществляется по запросу пациента. В документе должны быть определены порядок учета обращений и информирования пациентов, и ответственные за подготовку и предоставление указанных сведений пациентам.

14. Порядок оформления, учета и хранения письменного согласия пациента на обработку его ПД в медицинской организации.

Порядок должен содержать описание процедур получения (оформления), учета и порядка хранения письменного согласия пациента, образец оформления согласия пациента, а также порядок отзыва этого. Необходимо вести журнал по учету пациентов, давших и отозвавших согласие на обработку их ПД, а также регистрация фактов уничтожения ПД по требованию пациента.

15. Инструкцию по использованию электронной почты общего пользования и Интернета в медицинской организации.

Для упрощения и удешевления системы защиты информации доступ в Интернет рекомендуется осуществлять только со специально выделенных компьютеров.

В инструкции должно быть указано, что использовать открытую (обычную) электронную почту для передачи ПД без применения сертифицированных ФСБ средств криптографической защиты информации категорически запрещается.

В медицинской организации в целях защиты ПД ведутся следующие журналы:

- Журнал учета запросов пользователей ИС медицинской организации для допуска к персональным данным.

- Журнал учета мероприятий по обеспечению безопасности ПД в медицинской организации. В журнале учитываются как плановые, так и ситуационно выполненные мероприятия, учет которых не предусмотрен в других журналах, в частности, контрольные проверки.

- Журнал учета инструктажа сотрудников учреждения по обеспечению режима защиты ПД. В начале журнала заполняется ведомость ознакомления сотрудников учреждения с документами по защите информации - под подпись.

В должностные инструкции всех сотрудников медицинской организации должны быть включены требования по обеспечению конфиденциальности информации, в том числе, возможно, со ссылками на документы по защите ПД в медицинской организации.

Формы контроля освоения заданий по самостоятельной аудиторной/внеаудиторной работе по данной теме (контрольные вопросы).

Ответьте письменно на следующие вопросы:

1. Какие данные пациента в системе персонифицированного учета медицинской организации относятся к ПД.
2. Каким нормативным документом охраняется врачебная тайна.
3. Каков порядок регистрации в качестве оператора ПД медицинских организаций.

Ситуационные задачи

Для конкретной медицинской организации составить:

- *Образец приказа руководителя о назначении ответственного за работу с персональными данными и обеспечении их защиты*
- *Образец приказа, содержащий перечень персональных данных, которые используются в деятельности медицинской организации.*
- *Образец приказа об утверждении списка лиц, допущенных к работе с персональными данными.*
- *Примерный образец Положения о работе с персональными данными.*
- *Примерный образец Согласия сотрудника медицинской организации на обработку персональных данных.*
- *Примерный образец Согласия пациента медицинской организации на обработку персональных данных.*

Разбор ситуационных задач

Образец приказа руководителя о назначении ответственного за работу с персональными данными и обеспечении их защиты

Общество с ограниченной ответственностью «Х»

ПРИКАЗ

г. Уфа «___» _____ 20___ года

О назначении ответственного
за работу с персональными данными
и обеспечение их защиты

В целях обеспечения выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за реализацию мер, предусмотренных законодательными и иными нормативными правовыми актами по защите персональных данных, специалиста Отдела кадров Иванову Марию Ивановну.
2. Внести дополнения в должностную инструкцию специалиста Отдела кадров, в связи с обязанностями по обработке персональных данных.
3. Контроль выполнением данного приказа возложить на начальника отдела кадров Иванову Марию Ивановну.

Директор Петров П.П. Петров

Образец приказа, содержащий перечень персональных данных, которые используются в деятельности медицинской организации.

Общество с ограниченной ответственностью «Х»

ПРИКАЗ

г. Уфа «___» _____ 20___ года

Об утверждении перечня персональных данных,
обрабатываемых Обществом
с ограниченной ответственностью «Х»

В целях обеспечения выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:
1. Утвердить перечень персональных данных, обрабатываемых Обществом с ограниченной ответственностью «Х», согласно приложению.
2. Контроль над исполнением данного приказа возложить на начальника отдела кадров Иванову Марию Ивановну.

Директор Петров П.П. Петров

Приложение ХХ
к приказу _____

Перечень
персональных данных, обрабатываемых ООО «Х»

Перечень персональных данных субъектов ПД

Персональные данные субъектов ПД (пациентов) включают:
ФИО;
Дата рождения;
Контактный телефон;
Адрес прописки;
Адрес фактического проживания;
Паспортные данные;
Данные о состоянии здоровья (история болезни).

Перечень персональных данных сотрудников Учреждения

Персональные данные сотрудников Учреждения включают:
Фамилия, имя, отчество;
Место, год и дата рождения;
Адрес по прописке;
Паспортные данные (серия, номер паспорта, кем и когда выдан);
Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
Информация о трудовой деятельности до приема на работу;
Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
Адрес проживания (реальный);

Телефонный номер (домашний, рабочий, мобильный);

Семейное положение и состав семьи (муж/жена, дети);

Информация о знании иностранных языков;

Форма допуска;

Оклад;

Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

ИНН;

Данные об аттестации работников;

Данные о повышении квалификации;

Данные о наградах, медалях, поощрениях, почетных званиях;

Информация о приеме на работу, перемещении по должности, увольнении;

Информация об отпусках;

Информация о командировках;

Информация о болезнях;

Информация о негосударственном пенсионном обеспечении.

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 ПД, их составе и структуре, принципах и технических решениях защиты;

информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, 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.

Программно-технические средства обработки

Программно-технические средства включают в себя:

общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);

резервные копии общесистемного программного обеспечения;

инструментальные средства и утилиты систем управления ресурсами ИСПД;

аппаратные средства обработки ПД;

сетевое оборудование.

Средства защиты ПД

Средства защиты ПД состоят из аппаратно-программных средств, 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 межсетевого экранирования;
средства анализа защищенности;
средства обнаружения вторжений;
средства криптографической защиты ПД, при их передачи по каналам связи сетей общего и (или) международного обмена.

Каналы информационного обмена и телекоммуникации

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

Объекты и помещения, в которых размещены компоненты ИСПД

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

Образец приказа об утверждении списка лиц, допущенных к работе с персональными данными.

Общество с ограниченной ответственностью «Х»

ПРИКАЗ

г. Уфа «___» _____ 20___ года

Об утверждении списка лиц,
допущенных к работе
с персональными данными

В целях обеспечения выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить список лиц, допущенных к работе с персональными данными в Обществе с ограниченной ответственностью «Х», согласно приложению.
2. Контроль над исполнением данного приказа возложить на начальника отдела кадров Иванову Марию Ивановну.

Директор Петров П.П. Петров

Приложение:
к приказу ХХ

Список
лиц, допущенных к работе с персональными данными в ООО «Х»

1. Директор;
2. Руководитель Отдела кадров
3. Ведущий специалист Отдела кадров
4. Специалист Отдела кадров
5. Главный бухгалтер
6. Бухгалтер
7. Начальник отдела экономической безопасности;
8. Секретарь;
9. Начальник отдела внутреннего контроля;
10. Руководители структурных подразделений.

Примерный образец Положения о работе с персональными данными.

Утверждено приказом по ООО «Х»
от «___» _____ 20___ г. № _____

ПОЛОЖЕНИЕ
о работе с персональными данными

1. Общие положения

1.1. Настоящим Положением определяется порядок обращения с персональными данными работников ООО «Х» (далее - Работодатель).

1.2. Персональными данными работника является любая информация, относящаяся к работнику и необходимая Работодателю в связи с трудовыми отношениями. Конкретный перечень персональных данных, обрабатываемых Работодателем, утверждается Работодателем.

1.3. Защита персональных данных работника от неправомерного их использования, утраты обеспечивается Работодателем в порядке, установленном законодательством.

1.4. Сведения о персональных данных работников относятся к категории конфиденциальных.

2. Сбор и обработка персональных данных

2.1. Информацию обо всех персональных данных работника Работодатель может получать непосредственно от работника.

2.2. Если персональные данные можно получить только у третьей стороны, то для получения подобной информации Работодатель должен получить предварительное письменное согласие работника по форме, утвержденной Работодателем.

2.3. Обработка персональных данных работников Работодателем возможна только с их письменного предварительного согласия по форме утвержденной Работодателем.

2.4. Без письменного предварительного согласия персональные данные могут обрабатываться Работодателем в следующих случаях:

- персональные данные являются общедоступными;
- обработка данных осуществляется на основании Трудового кодекса РФ или иного федерального закона;
- обработка данных производится в целях исполнения трудового договора;
- обработка данных осуществляется для статистических целей при условии обязательного обезличивания;
- данные предоставляются по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.
- персональные данные относятся к состоянию здоровья работника, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия работника невозможно;

3. Доступ к персональным данным

3.1. Право доступа к персональным данным работников имеют лица, указанные в списке, утверждаемом Работодателем.

3.2. Работники и их представители должны быть ознакомлены под расписку с документами, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.3. Работник имеет право на доступ к своим персональным данным, ознакомление с ними, в том числе на получение безвозмездно одной копии любой записи, содержащей его персональные данные.

3.4. Копирование персональных данных работника возможно исключительно в служебных целях с письменного разрешения начальника отдела кадров.

3.5. Передача персональных данных другим лицам, не указанным в настоящем Положении, а также доступ этих лиц к сведениям, составляющим персональные данные, возможна исключительно с письменного предварительного согласия работника.

4. Порядок обработки и передачи данных

4.1. Передача персональных данных третьим лицам осуществляется только при наличии письменного предварительного согласия работника, за исключением случаев, перечисленных в п. 4.2 настоящего Положения.

4.2. Без согласия работника персональные данные могут предоставляться:

а) при несчастном случае с работником на основании ст. 228 Трудового кодекса РФ – органам, указанным в ст. 228.1 Трудового кодекса РФ, а при тяжелом несчастном случае или смерти также родственникам работника.

б) государственным инспекторам труда при осуществлении ими надзорной и контрольной деятельности на основании статьи 357 Трудового кодекса РФ.

в) в органы Пенсионного фонда на основании статей 9 и 11 Федерального закона от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»

г) в иных случаях, предусмотренных Федеральными законами.

4.3. Во всех случаях, предусмотренных настоящим Положением, в том числе и при подготовке данных к передаче в случаях, указанных в п. 4.2. настоящего Положения, обработка персональных данных производится только лицами, указанными в разделе 3 настоящего Положения.

5. Ответственность за нарушение правил работы с персональными данными

5.1. Сотрудники Работодателя, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную и уголовную ответственность в соответствии с федеральными законами.

6.2. Работодатель за нарушение порядка обращения с персональными данными несет административную ответственность.

6.3. Работодатель возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом работнике.

Примерный образец Согласия сотрудника медицинской организации на обработку персональных данных.

Директору ООО «Х»
Петрову П.П.
Иванова Ивана Ивановича,
паспорт серии … № ….
выдан …,
зарегистрированного по месту жительства
по адресу: …

СОГЛАСИЕ
на обработку персональных данных

Настоящим я, Иванов Иван Иванович, в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» даю согласие Обществу с ограниченной ответственностью «Х» (ИНН … , КПП …) на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных.

Мне известно, что под обработкой моих персональных данных подразумевается совершение действий, предусмотренных пунктом 3 части 1 статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», со сведениями о фактах, событиях и обстоятельствах моей жизни, которые я предоставил ООО «Х» как в рамках трудовых отношений, так и вне таковых.

Мне разъяснено, что я имею право отозвать настоящее согласие в любой момент, сообщив об этом директору ООО «Х» в письменной форме.

Иванов /Иванов И.И./
Дата

Примерный образец Согласия пациента медицинской организации на обработку персональных данных.

СОГЛАСИЕ
на обработку персональных данных

Я, нижеподписавшийся Иванов Иван Иванович, проживающий по адресу <_по месту регистрации, паспорт <_серия и номер_>, выдан <_дата и название выдавшего органа_>, в соответствии с требованиями статьи 9 Федерального закона "О персональных данных" от 27.07.2006 № 152-ФЗ, подтверждаю свое согласие на обработку в ООО «Х» (далее - Оператор) моих персональных данных, включающих: фамилию, имя, отчество, пол, дату рождения, адрес места жительства, контактные телефоны, реквизиты паспорта (документа удостоверения личности), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью - в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну. В процессе оказания Оператором мне медицинской помощи я предоставляю право медицинским работникам передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими порядок ведения и состав данных в учетно-отчетной медицинской документации, а также договором на оказание медицинской помощи между Оператором и страховой медицинской компанией <_название и адрес компании, № и дата договора_>.

Оператор имеет право во исполнение своих обязательств по указанному выше договору на обмен (прием и передачу) моими персональными данными со страховой медицинской компанией <_полное название_> с использованием машинных носителей информации, по каналам связи и(или) в виде бумажных документов, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, без специального уведомления меня об этом, при условии, что их прием и обработка осуществляются лицом, обязанным сохранять профессиональную (служебную) тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов (медицинской карты) и составляет двадцать пять лет.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной <_дата_> и действует бессрочно.

Контактный телефон(ы) <...> и почтовый адрес <...>

< подпись субъекта персональных данных >

Место проведения самоподготовки:
читальный зал, учебная комната для самостоятельной работы обучающихся, компьютерный класс.

Рекомендуемая литература

Основная литература

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» http://www.studmedlib.ru/ru/book/ISBN9785970432914.html	Неограниченный доступ

Дополнительная литература

Нагаев, Р. Я. 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
Нагаев, Р. Я. 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» http://library.bashgmu.ru/elibdoc/elib582.pdf	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..
- Конституция Российской Федерации. Принята на всенародном голосовании 12 декабря 1993г.
- Кодекс Российской Федерации об административных правонарушениях № 195-ФЗ от 30.12. 2001 г..
- Трудовой кодекс Российской Федерации от 30.12.2001г. № 197-ФЗ - Глава 14 «Защита персональных данных работника»
- Уголовный кодекс Российской Федерации № 63-ФЗ от 13.06.1996 г.
- Федеральный закон от 21.07.2014 г. № 242-ФЗ «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 «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 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

- Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»
- Федеральный закон от 27.07.2006г. № 152-ФЗ) «О персональных данных»
- Федеральный закон от 27.07.2006г. № 149-ФЗ) «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»
- Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне»
- Указ Президента Российской Федерации от 17.03.2008 г. № 351 «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) «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 «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 «О лицензировании деятельности по технической защите конфиденциальной информации»
- Постановление Правительства Российской Федерации от 21.03.2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
- Постановление Правительства Российской Федерации от 16.04. 2012 г. №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
- 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 РФ от 04.03.2010г. № 125 "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию"
- Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «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»

- Постановление Правительства Российской Федерации от 03.11.1994г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использования атомной энергии и уполномоченном органе по космической деятельности»
- Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14.11. 2011г. № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»
- 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 ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
- Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»
- Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст) http://standartgost.ru/.
- Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3.02. 2012 г. № 79

Интернет-ресурсы по защите персональных данных

База данных «Электронная учебная библиотека»	Свидетельство №2009620253 от 08.05.2009 http://library.bashgmu.ru
Электронно-библиотечная система eLIBRARY. Коллекция российских научных журналов по медицине и здравоохранению	ООО РУНЭБ, Договор №750 от 18.12.2018 http:// elibrary.ru
База данных Scopus	ФГБУ ГПНТБ России, Сублицензионный договор № SCOPUS/50 от 09.10.2019 https://www.scopus.com
Базаданных Web of Science Core Collection	ФГБУ ГПНТБ России, Сублицензионный договор № Wos/50 от 05.09.2019 http://apps.webofknowledge.com
База данных Russian Science Citation Index	НП НЭИКОН, Сублицензионный договор № 0301100049619000695000l от 06.12.2019 http://apps.webofknowledge.com
База данныхMEDLINE	НП НЭИКОН, Сублицензионный договор №

	0301100049619000695000l от 06.12.2019 http://apps.webofknowledge.com
Консультант Плюс: справочно-правовая система	ООО Компания Права «Респект» Договор о сотрудничестве от 21.03.2012 локальный доступ

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

Тема: Обеспечение контроля и надзора за соответствием обработки персональных данных требованиям законодательства

Цель изучения темы: ознакомиться с основами обеспечения контроля и надзора за соответствием обработки персональных данных требованиям законодательства в рамках подготовки к практическому занятию по соответствующей теме.

Задачи:

– рассмотреть основы обеспечения контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

Обучающийся должен знать:

1. До изучения темы (базисные знания):

– методы и приемы устного и письменного изложения предметного материала, основы проведения анализа литературных источников;

– проведение критического анализа научной и публицистической литературы.

2. После изучения темы:

– основы обеспечения контроля и надзора за соответствием обработки персональных данных требованиям законодательства

должен владеть:

– навыками обеспечения контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

должен уметь:

– использовать основы обеспечения контроля и надзора за соответствием обработки персональных данных требованиям законодательства.

должен сформировать компетенции (частично):

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

Задания для самостоятельной контактной работы обучающихся по указанной теме:

Перечень контрольных вопросов

1. Ознакомиться с теоретическим материалом по теме занятия с использованием конспектов лекций, рекомендуемой учебной литературы.

2. Ответить на вопросы для самоконтроля:

1) Какие государственные органы, помимо уполномоченного органа, осуществляют контроль над системами защиты ПД.
2) Перечислите полномочия ФСТЭК по обеспечению системы защиты ПД.
3) Какую ответственность несут лица, виновные в нарушении требований законодательства о ПД.
4) Какая ответственность может наступить за неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина.
5) Какая ответственность может наступить за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

6) Какая ответственность может наступить за разглашение конфиденциальной информации, лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.
7) Какая ответственность может наступить за осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии), если такое разрешение (лицензия) обязательно.
8) Какие меры дисциплинарного взыскания и в каком порядке можно применить к работнику за разглашение ПД.
9) К каким видам ответственности могут быть привлечены виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работника.

3. Проверить свои знания с использованием тестового контроля:

Тестовый контроль знаний

Выберите один правильный ответ

В СООТВЕТСТВИИ С ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27.07.2006 № 152- ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ» ОПЕРАТОРОМ ЯВЛЯЕТСЯ

1) муниципальный или государственный орган, физическое или юридическое лицо, определяющие цели и содержание обработки персональных данных, а также организующие и (или) осуществляющие их обработку
2) только физическое лицо, осуществляющее сбор, систематизацию, накопление, использование, хранение и иные действия (операции) с персональными данными
3) специально уполномоченная организация по обработке персональных данных
4) физическое лицо, ответственное за обработку персональных данных с использованием средств автоматизации или без использования таких средств

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 рабочих дней с даты этого выявления
4) в срок, не превышающий трех рабочих дней с даты этого выявления

В ОБЕЗЛИЧЕННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ НИКОГДА НЕ УКАЗЫВАЮТСЯ

1) фамилия, имя, отчество пациента
2) возраст пациента
3) место проживания пациента
4) номер полиса обязательного медицинского страхования

Ознакомление обучающихся с содержанием занятия

Защита данных о пациенте. Врачебная тайна

Конституция Российской Федерации, как основной закон страны, в статье 23 определяет, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Врачебная тайна – это сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении.

Федеральным законом № 323-ФЗ в статье 19, посвященной правам пациента, закреплено право пациента на защиту сведений, составляющих врачебную тайну.

Данным законом впервые определено, что соблюдение врачебной тайны входит в девять основных принципов охраны здоровья человека. Статья 13 закона устанавливает, что предоставление третьим лицам сведений, составляющих врачебную тайну, теперь допускается только с письменного согласия гражданина или его законного представителя. Кроме того, устанавливается прямой запрет на разглашение сведений, составляющих врачебную тайну, даже после смерти человека.

В статье 13 Федеральным законом № 323-ФЗ предусмотрен исчерпывающий перечень случаев, при которых допускается предоставление третьим лицам сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя. Одним из таких случаев является предоставление информации в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю. При этом, допуская возможность передачи информации, законодательство не определяет, когда именно и кому можно ее передавать. Поэтому представляется допустимым решать этот вопрос в каждом конкретном случае.

Закон делает ссылку на п. 1 ч. 9 ст. 20 указанного закона, которая гласит, что медицинское вмешательство без согласия гражданина, одного из родителей или иного законного представителя допускается, если оно необходимо по экстренным показаниям для устранения угрозы жизни человека и если его состояние не позволяет выразить свою волю или отсутствуют законные представители в отношении следующих категорий:

- в отношении несовершеннолетнего, не достигшего возраста 15 лет (а в отношении несовершеннолетнего, больного наркоманией - в возрасте старше шестнадцати лет);

- несовершеннолетнего больного наркоманией при оказании ему наркологической помощи или при медицинском освидетельствовании несовершеннолетнего в целях установления состояния наркотического либо иного токсического опьянения.

Кроме того, предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

- в случае оказания медицинской помощи несовершеннолетнему, больному наркоманией при оказании ему наркологической помощи или при медицинском освидетельствовании несовершеннолетнего в целях установления состояния наркотического либо иного токсического опьянения (за исключением установленных законодательством Российской Федерации случаев приобретения несовершеннолетними полной дееспособности до достижения ими восемнадцатилетнего возраста);

- в случае оказания медицинской помощи несовершеннолетнему в возрасте старше шестнадцати лет и иным несовершеннолетним в возрасте старше пятнадцати лет для информирования одного из его родителей или иного законного представителя;

- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий в соответствии с приказом Минздравсоцразвития России от 17 мая 2012 г. № 565н «Об утверждении Порядка информирования медицинскими организациями органов внутренних дел о поступлении пациентов, в отношении которых имеются достаточные основания полагать, что вред их здоровью причинен в результате противоправных действий»;

- в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

- в целях расследования несчастного случая на производстве и профессионального заболевания;

- при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

- в целях осуществления учета и контроля в системе обязательного социального страхования;

- в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом.

Обладателем информации, содержащей сведения о ПД, является пациент (субъект ПД) или его законный представитель. В данном случае, в соответствии с законодательством, должно быть получено согласие пациента на передачу сведений, содержащих врачебную тайну, кому-либо, в том числе должностным лицам в интересах его обследования и лечения.

Согласие пациента на обработку своих ПД должно быть оформлено письменно и включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва.

В поликлинике письменное согласие можно оформлять при первом обращении пациента и оформлении амбулаторной карты, в стационаре - при каждом случае госпитализации в виде вкладыша в историю болезни.

При организации работы рекомендуется максимально ограничить круг сотрудников, которым предоставлен доступ к ПД пациентов.

Согласно ст. 20 Закона, медицинская организация обязана предоставить безвозмездно пациенту возможность ознакомления с его персональными данными. В срок, не превышающий 7 рабочих дней со дня предоставления пациентом сведений, подтверждающих, что персональные данные были получены незаконно или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные.

Защита персональных данных медицинского работника

Работа отдела кадров медицинской организации связана с подбором персонала, приёмом на работу работников, а также с накоплением, обработкой, хранением и использованием сведений о работниках. Защита ПД работника, порядок доступа к ним, процедура предоставления информации третьим лицам регулируется трудовым законодательством Российской Федерации (глава 14, статьи 85-90 ТК РФ).

Кодекс устанавливает, что «*Персональные данные работника* - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника». *Обработка персональных данных* работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Обязанность защиты персональных данных работника от неправомерного их использования или утраты возложена на работодателя, который обеспечивает это за счет собственных средств в порядке, установленном ТК РФ и иными федеральными законами (п. 7 ст. 86 ТК РФ).

Принятая в 1981 году в Страсбурге Конвенция о защите физических лиц при автоматизированной обработке ПД устанавливает, что «*данные личного характера*» - любая

информация, относящаяся к физическому лицу, либо идентифицированному, либо которое может быть идентифицировано.

Персональные данные работника содержатся в основном документе персонального учета работников - личном деле работника, которое включает следующие документы: кадровая справка; заявление работника о приеме на работу; анкета; автобиография; характеристика-рекомендация; результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей; копия приказа о приеме на работу; расписка работника об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также о его правах и обязанностях в этой области; расписка работника об ознакомлении его с лекальными нормативными актами организации; дополнение к личному делу; карточка поощрений и взысканий; внутренняя опись.

Все документы личного дела подшиваются в обложку образца, установленного в организации; на обложке должны быть фамилия, имя, отчество работника.

Личные дела, в которых хранятся ПД работников, являются документами «Для внутреннего пользования» и находятся в отделе кадров в специально отведенном шкафу, обеспечивающем защиту от несанкционированного доступа.

ПД работников могут также храниться в электронном виде в локальной компьютерной сети. Доступ к ПД работника, как правило, имеют руководитель медицинской организации, заместитель руководителя медицинской организации, главный врач, главный бухгалтер, а к тем данным, которые необходимы для выполнения конкретных функций, - также непосредственный руководитель работника, специалисты отдела кадров и бухгалтерии.

Доступ специалистов других отделов к ПД должен осуществляться на основании письменного разрешения руководителя медицинской организации или его заместителя.

Делать копии и выписки ПД работника допускается исключительно в служебных целях с письменного разрешения руководителя медицинской организации. ПД работника используются только для целей, связанных с выполнением работником трудовых функций.

Работодатель не вправе предоставлять ПД работника третьей стороне без письменного согласия работника. Если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение ПД работника либо отсутствует письменное согласие работника на предоставление его персональных сведений, работодатель обязан отказать в предоставлении ПД.

В соответствии с совместными разъяснениями Минкомсвязи России и Роскомнадзора «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве» работодатель вправе без соответствующего согласия осуществлять обработку ПД работника в случаях, предусмотренных коллективным договором, в том числе правилами внутреннего трудового распорядка, являющимися, как правило, приложением к коллективному договору, соглашением, а также локальными актами работодателя, принятыми в порядке, установленном ст. 372 ТК РФ.

Кроме того, получение работодателем согласия на обработку ПД не требуется в следующих случаях:

1. Обязанность по обработке, в том числе опубликованию и размещению ПД работников в сети Интернет, предусмотрена законодательством Российской Федерации.

2. Обработка ПД близких родственников работника в объеме, предусмотренном унифицированной формой № Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат).

3. Обработка специальных категорий ПД работника, в том числе, сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения работником трудовой функции на основании положений п. 2.3 ч. 2 ст. 10 Закона в рамках трудового законодательства.

4. При передаче ПД работника третьим лицам в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных

ТК РФ или иными федеральными законами.

Передача ПД работников в Фонд социального страхования Российской Федерации, Пенсионный фонд Российской Федерации осуществляется без их согласия.

Согласие работника, государственного служащего не требуется при передаче его ПД в случаях, связанных с выполнением им должностных обязанностей, в том числе, при его командировании.

Под исключения, связанные с отсутствием необходимости получения согласия, подпадают случаи передачи работодателем ПД работников, государственных служащих в налоговые органы, военные комиссариаты, профсоюзные органы, предусмотренные действующим законодательством Российской Федерации.

Согласие работника не требуется при получении, в рамках установленных полномочий, мотивированных запросов от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

5. Обработка ПД работника при осуществлении пропускного режима на территорию служебных зданий и помещений работодателя, при условии, что организация пропускного режима осуществляется работодателем самостоятельно либо если указанная обработка соответствует порядку, предусмотренному коллективным договором, локальными актами работодателя, принятыми в соответствии со ст. 372 ТК РФ.

Согласие работника может быть оформлено как в виде отдельного документа, так и закреплено в тексте трудового договора и отвечать требованиям, предъявляемым к содержанию согласия, согласно ч. 4 ст. 9 Закона.

Контроль и надзор за обработкой персональных данных. Уполномоченный орган по защите прав субъектов персональных данных

Уполномоченным органом по защите прав субъектов ПД, на который возлагается обеспечение контроля и надзора за соответствием обработки ПД требованиям законодательства, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи. В соответствии с Приказом № 312 эти функции осуществляет Роскомнадзор.

Уполномоченный орган по защите прав субъектов ПД рассматривает обращения субъекта ПД о соответствии содержания ПД и способов их обработки целям их обработки и принимает соответствующее решение.

Уполномоченный орган по защите прав субъектов ПД имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки ПД, осуществляемой с нарушением требований Закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов ПД и представлять интересы субъектов персональных данных в суде;

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу ПД третьим лицам без согласия в письменной форме субъекта ПД;

7) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПД, в соответствии с подведомственностью;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов ПД;

9) привлекать к административной ответственности лиц, виновных в нарушении Федерального закона.

В отношении ПД, ставших известными уполномоченному органу по защите прав субъектов ПД в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

При контрольных мероприятиях Росомнадзора подотчётному лицу необходимо предъявить следующие документы:

- учредительные документы;
- выписка из ЕГРЮЛ на момент проведения проверки;
- копия уведомления об обработке персональных данных;
- копия документа, подтверждающего полномочия оператора на взаимодействие с сотрудниками Роскомнадзора в период проведения проверки (приказ, доверенность);
- типовые формы документов, предполагающие или допускающие содержание ПД;
- журналы, реестры, книги, содержащие ПД, необходимые для однократного пропуска субъекта ПД на территорию, на которой находится Оператор;
- приказы об утверждении мест хранения материальных носителей ПД;
- письменное согласие субъектов ПД на обработку их персональных данных;
- положение о порядке обработки персональных данных;
- приказ о назначении ответственных лиц по работе с ПД;
- договоры с субъектами ПД, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных;
- распечатки электронных шаблонов полей, содержащих ПД;
- справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка ПД;
- заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности ПД при их обработке (при наличии);
- должностные регламенты лиц, имеющих доступ и (или) осуществляющих обработку персональных данных;
- журналы (книги) учета обращений граждан (субъектов ПД);
- акты об уничтожении персональных данных субъекта (-ов) персональных данных (в случае достижения цели обработки);
- положение о подразделении, осуществляющем функции по организации защиты персональных данных;
- план мероприятий по защите персональных данных;
- план внутренних проверок состояния защиты ПД;
- документы о присвоении информационной системе соответствующего класса (Акт о присвоении класса);
- журнал учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля;
- документы организации охраны, режима обеспечения безопасности (приказы, распоряжения);
- документ, определяющий политику в отношении обработки ПД.

Порядок работы Роскомнадзора с обращениями граждан в сфере работы с персональными данными приведен на схеме.

Контроль над порядком обработки ПД работников медицинской организации могут осуществлять органы Федеральной службы по труду и занятости (Роструда) в ходе плановых

проверок соблюдения трудового законодательства, а также по обращению субъекта ПД - работника медицинской организации, в том числе о нарушении его прав в рамках трудовых отношений.

Кроме того, контроль систем защиты ПД также осуществляют ФСТЭК или ФСБ в ходе контроля систем защиты конфиденциальных данных или использования криптосредств.

ФСТЭК осуществляет:

- надзор за деятельностью лицензиата ФСТЭК;
- проверки по обращению Роскомнадзора;
- внеплановые проверки по контролю нарушений обязательных требований.

ФСБ осуществляет:

- контроль за соблюдением правил использования средств криптографической защиты информации;
- надзор за деятельностью лицензиата ФСБ;
- внеплановые проверки по контролю нарушений обязательных требований;
- проверки по обращению Роскомнадзора.

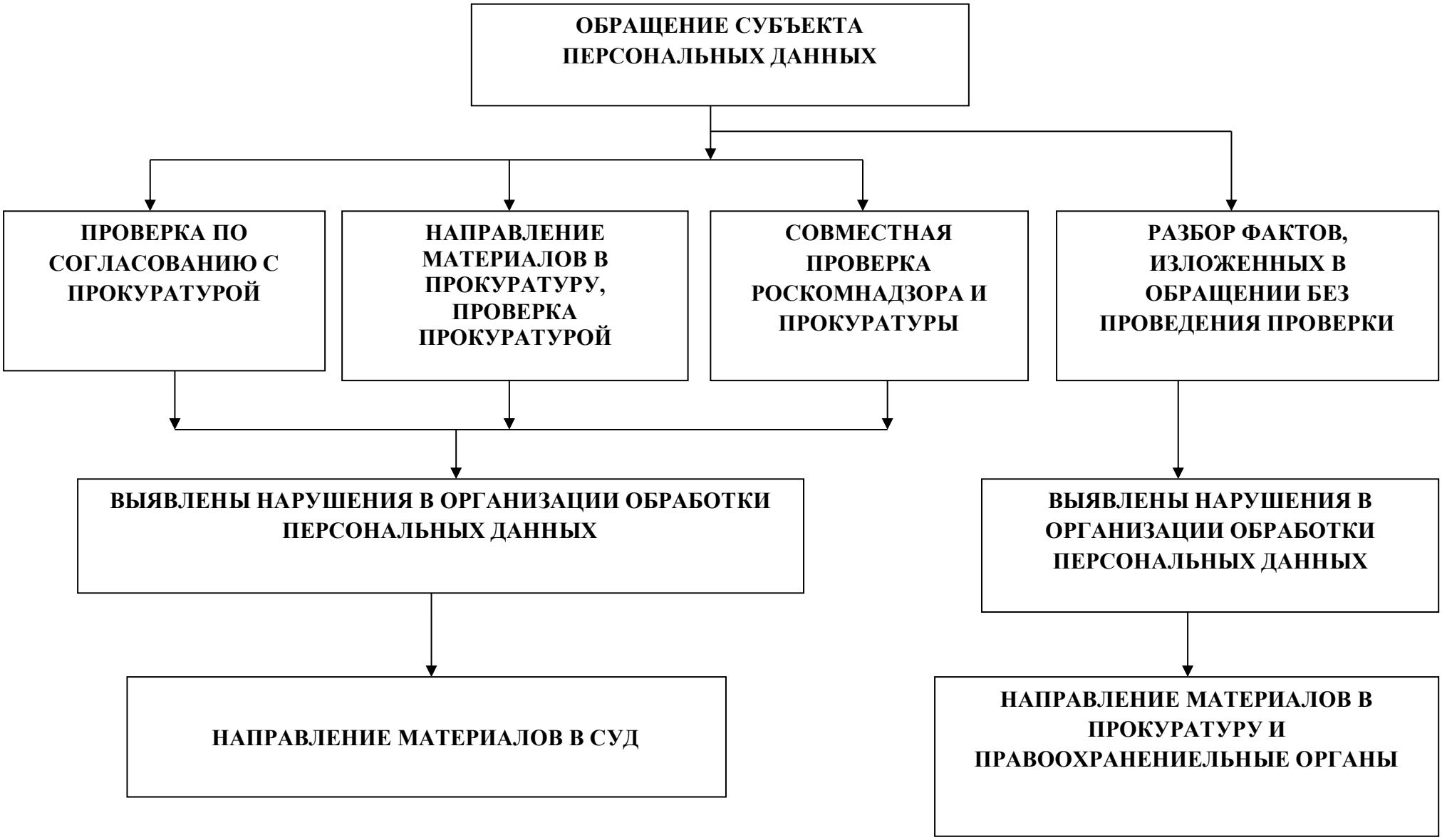

Схема. Порядок работы Роскомнадзора с обращениями граждан

Ответственность, предусмотренная за правонарушения в сфере защиты информации

В соответствии со статьей 24 Закона лица, виновные в нарушении требований безопасности ПД, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Уголовная ответственность

К уголовной ответственности могут быть привлечены исключительно физические лица, совершившие преступление, посягающее на интересы личности, общества и государства.

Статья 137. Нарушение неприкосновенности частной жизни

Часть 1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующим произведении или средствах массовой информации

- наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Часть 2. Те же деяния, совершенные лицом с использованием своего служебного положения,

- наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Статья 272. Неправомерный доступ к компьютерной информации

Часть 1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации,

- наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Часть 2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности,

- наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

Часть 3. Деяния, предусмотренные частями первой или второй, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения,

- наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной

платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей, если они повлекли тяжкие последствия или создали угрозу их наступления,

- наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Часть 1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб,

- наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Часть 2. Деяние, предусмотренное частью первой, если оно повлекло тяжкие последствия или создало угрозу их наступления,

- наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Административная ответственность

Перечень нарушений, предусматривающих ответственность за нарушение требований законодательства в сфере персональных данных КоАП РФ, более широк. И в соответствии с нормами административного законодательства субъектом правонарушения может быть юридическое лицо, лицо, осуществляющее предпринимательскую деятельность без образования юридического лица, а также должностное лицо, а также граждане.

Административная ответственность установлена:

1) за нарушение правил обработки персональных данных;
2) неисполнение обязанностей при взаимодействии с гражданином - субъектом персональных данных;
3) невыполнение требований по защите персональных данных;
4) неисполнение обязанностей при взаимодействии с Роскомнадзором;
5) нарушение требований к размещению и обработке биометрических персональных данных в ЕБС (других информсистемах, обеспечивающих аутентификацию на основе таких данных).

Если в ходе проверки будет выявлено два и более нарушения, ответственность за которые предусмотрена одной и той же статьей (частью статьи) разд. II КоАП РФ, вас накажут как за одно. Если же ответственность за выявленные нарушения предусмотрена двумя и более статьями (их частями), грозить будет одно - наиболее строгое - наказание. В последнем случае могут назначить и дополнительные санкции (ч. 2 - 6 ст. 4.4 КоАП РФ).

Обратите внимание, что к ответственности за нарушение могут одновременно привлечь и организацию, и виновное физическое лицо, за исключением ряда случаев. Например, юрлицо не привлекут к ответственности, если привлекли его должностное лицо (работника). Избежать наказания сможет то юрлицо, которое приняло все предусмотренные законодательством меры для соблюдения соответствующих правил и норм (ч. 3 - 4 ст. 2.1 КоАП РФ).

Основной вид административного наказания за нарушение законодательства о персональных данных - штраф. Его размер зависит от конкретного нарушения. Например,

максимальный штраф для организации за обработку персональных данных без письменного согласия гражданина, когда согласие требуется, или за отсутствие в нем всех необходимых сведений составляет 700 000 руб., за повторное правонарушение - 1 500 000 руб. (ч. 2, 2.1 ст. 13.11 КоАП РФ).

Дисциплинарная ответственность

В соответствии с ТК РФ разглашение персональных данных, а также нарушение норм, регулирующих получение, обработку и защиту персональных данных работников, может грозить работнику организации увольнением. В частности ТК РФ предусматривает, что трудовой договор может быть расторгнут в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей (п. «в» ч. 6 ст. 81, глава 14 ТК РФ).

Уволить за разглашение персональных данных можно только тех работников, которым такие сведения стали известны в связи с исполнением ими трудовых обязанностей. К таким сотрудникам относятся работники кадровых служб, бухгалтерии, военно-учетного подразделения, службы охраны труда, а также руководитель медицинской организации или лицо, его заменяющее. Однако если работник узнал персональные данные случайно (например, из-за халатности сотрудника, ответственного за сохранность информации) и в его должностные обязанности не входит работа с личными сведениями, увольнение будет являться незаконным.

Увольнение за разглашение персональных данных является увольнением по инициативе работодателя, поэтому незаконным будет прекращение трудового договора по данному основанию в период временной нетрудоспособности работника и в период его пребывания в отпуске (ч. 6 ст. 81 ТК РФ). Также в силу прямого указания статьи 192 ТК РФ рассматриваемое увольнение является дисциплинарным взысканием, а, следовательно, оно должно осуществляться по правилам статьи 193 ТК РФ

Необходимо отметить, что увольнение работника за разглашение ПД затруднительно для работодателя по причине того, что сложно установить и доказать сам факт разглашения конкретным работником. Важно учесть и то, что для увольнения работника за разглашение ПД не важно, был ли проступок совершен умышленно или по неосторожности, руководствовался ли нарушитель какими-либо корыстными мотивами или нет.

Согласно статье 90 ТК РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Формы контроля освоения заданий по самостоятельной аудиторной/внеаудиторной работе по данной теме (контрольные вопросы).

Ответьте письменно на следующие вопросы:

1. Какие меры дисциплинарного взыскания и в каком порядке можно применить к работнику за разглашение ПД.
2. К каким видам ответственности могут быть привлечены виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работника.

Ситуационные задачи

Ситуационная задача 1. Вправе ли должностное лицо, в производстве которого находится дело об административном правонарушении, запрашивать у руководства медицинской организации персональные данные их работников?

Ситуационная задача 2. В медицинской организации сотрудница отдела бухгалтерского учета и отчетности передала другой фирме документы, касающиеся оплаты труда и премирования, не скрыв Ф.И.О. нескольких работников. При этом имело место разглашение персональных данных. Руководитель медицинской организации хочет уволить провинившуюся сотрудницу. Однако работники, чьи персональные данные были

разглашены, ее простили и подписали обращение к руководству, что претензий к ней не имеют. Можно ли в данной ситуации уволить работника?

Ситуационная задача 3. В медицинскую организацию поступил телефонный звонок от сотрудника банка с целью проверки, работает ли в организации гражданин И. Сотрудником отдела кадров была предоставлена исчерпывающая информация о работнике И. с указанием паспортных данных, ИНН и пр. Является ли это нарушением законодательства о защите ПД работника? Может ли медицинская организация отказать звонящему в предоставлении сведений о работнике?

Ситуационная задача 4. В помещении отдела кадров медицинской организации перегорела лампа дневного освещения. Был вызван штатный электрик. Он быстро справился с поставленной задачей. Но, уходя, прочитал приказы о премировании работников административно-хозяйственного отдела, забытые на столе кадровиком. При этом он заметил, что из всех сотрудников АХО ему была выплачена самая маленькая премия. Электрик был очень обижен и поспешил поделиться об этом со всеми, кто был готов его выслушать. История быстро дошла до руководителя медицинской организации, который хотел даже его уволить за разглашение персональных данных. Однако при выяснении обстоятельств выяснил, что приказы были оставлены на столе специалистом отдела кадров.

Как следует поступить руководителю в данной ситуации?

Ситуационная задача 5. В приемном покое медицинской организации на стенде представлен список пациентов, находящихся на стационарном лечении с указанием отделения, Ф.И.О., номера палаты. Кроме того, представлен список пациентов реанимационного отделения с дополнительным указанием тяжести состояния. Нарушены ли права пациентов, находящихся на стационарном лечении в медицинской организации?

Ситуационная задача 6. Гражданин Г. работает охранником в ГБУЗ Кожно-венерологический диспансер. Находясь на дежурстве в приемном покое, он случайно встретил своего соседа по дому гражданина П. В беседе П. пояснил, что проходит медицинский осмотр. Охранник, придя домой со смены, сообщил супруге о встрече. Спустя месяц гр. П. подал в суд на гр. Г. о защите своих конституционных прав на неприкосновенность частной жизни, защиту чести и доброго имени. Правомерен ли судебный иск?

Разбор ситуационных задач

Ситуационная задача 1. В соответствии со статьей 28.3 КоАП РФ протоколы об административных правонарушениях составляются должностными лицами органов, уполномоченных рассматривать дела об административных правонарушениях в пределах компетенции соответствующего органа.

Требования к содержанию протокола об административном правонарушении установлены статьей 28.2 КоАП РФ. В частности, в протоколе об административном правонарушении указываются сведения о лице, в отношении которого возбуждено дело об административном правонарушении.

Кроме того, статьей 26.10 КоАП РФ предусмотрено, что орган, должностное лицо, в производстве которых находится дело об административном правонарушении, вправе вынести определение об истребовании сведений, необходимых для разрешения дела. Истребуемые сведения должны быть направлены в трехдневный срок со дня получения определения в порядке, предусмотренном ст.26.10 КоАП РФ. При невозможности представления указанных сведений организация обязана в трехдневный срок уведомить об этом в письменной форме судью, орган, должностное лицо, вынесших определение.

Пунктом 1 части 2 статьи 6 Закона «О персональных данных» предусмотрена обработка персональных данных на основании Федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора без согласия субъекта персональных данных.

Таким образом, должностное лицо органа, уполномоченного составлять и рассматривать протоколы об административном правонарушении вправе в рамках производства по делу об административном правонарушении запрашивать у организаций персональные данные их работников, в отношении которых возбуждено дело об административном правонарушении.

Ситуационная задача 2. Да, можно. Трудовой кодекс не делает оговорку, что увольнение является незаконным в случае примирения с работником, чьи персональные данные были разглашены (подп. «в» п. 6 ч. 1 ст. 81 ТК РФ). Более того, прекращение трудового договора происходит в рамках двусторонних трудовых отношений работодателя и работника. Зависимость таких отношений от третьих лиц законодательством исключается.

Ситуационная задача 3. Да, является. Нормами ст. 88 ТК РФ установлено, что работодатель не вправе сообщать ПД третьей стороне без письменного согласия их субъекта. В случае отсутствия письменного согласия работника работодатель обязан отказать в их предоставлении.

Ситуационная задача 4. В соответствии с подпунктом «в» пункта 6 части первой статьи 81 ТК РФ трудовой договор может быть расторгнут работодателем в случае разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника. Сохранение личных сведений о сотрудниках не входит в трудовые обязанности электрика. Персональные данные стали известны ему случайно вследствие халатности сотрудника кадровой службы, в должностные обязанности которого входит сохранность указанной информации. Следовательно, увольнение электрика было бы незаконным. Руководителю следует привлечь к дисциплинарной ответственности специалиста по кадрам за несоблюдение установленного порядка работы с документами, содержащими персональные данные.

Ситуационная задача 5. Да, нарушены. В соответствии со ст. 13 Федерального закона № 323-ФЗ врачебная тайна - сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении.

Ситуационная задача 6. Да, правомерен. В соответствии с частью 2 **с**татьи 13 Федерального закона № 323-ФЗ не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при исполнении трудовых, должностных, служебных обязанностей. В данном случае гражданин Г., работающий охранником и находящийся на службе, не имея злого умысла, по неосторожности, допустил разглашение конфиденциальной информации. При этом законодательство не делает оговорку, совершен ли проступок умышленно или по неосторожности.

Место проведения самоподготовки:

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

Рекомендуемая литература

Основная литература

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» http://www.studmedlib.ru/ru/book/ISBN9785970432914.html	Неограниченный доступ

Дополнительная литература

Нагаев, Р. Я. 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
Нагаев, Р. Я. 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» http://library.bashgmu.ru/elibdoc/elib582.pdf	Неограниченный доступ

Нормативные правовые акты в области защиты персональных данных

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28.01.1981
- 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..
- Конституция Российской Федерации. Принята на всенародном голосовании 12 декабря 1993г.
- Кодекс Российской Федерации об административных правонарушениях № 195-ФЗ от 30.12. 2001 г. .
- Трудовой кодекс Российской Федерации от 30.12.2001г. № 197-ФЗ - Глава 14 «Защита персональных данных работника»
- Уголовный кодекс Российской Федерации № 63-ФЗ от 13.06.1996 г.
- Федеральный закон от 21.07.2014 г. № 242-ФЗ «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 «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 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» (в ред. от 17.06.2019г.)
- Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»
- Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных»
- Федеральный закон от 27.07.2006г. № 149-ФЗ «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»
- Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне»
- Указ Президента Российской Федерации от 17.03.2008 г. № 351 «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 «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 «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. № «О лицензировании деятельности по технической защите конфиденциальной информации»
- Постановление Правительства Российской Федерации от 21.03.2012г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
- Постановление Правительства Российской Федерации от 16.04. 2012 г. № «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
- 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 РФ от 04.03.2010г. № 125 "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию"
- Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «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»
- Постановление Правительства Российской Федерации от 03.11.1994г. «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использования атомной энергии и уполномоченном органе по космической деятельности»
- Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14.11. 2011г. № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»
- 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 ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
- Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»
- Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст) http://standartgost.ru/.
- Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3.02. 2012 г. № 79

Интернет-ресурсы по защите персональных данных

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