



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
«Б1.В.ДВ.01.02 РАЗРАБОТКА РЕГЛАМЕНТА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ
ДАННЫХ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Старший преподаватель кафедры
Информационно-измерительных систем Бельшева Ю. В.

Старший преподаватель кафедры
Информационно-измерительных систем Нахаева А. С.

Преподаватель кафедры Информационно-измерительных систем
Рыжиков К. С.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями
ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность,
утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

ПК-2 Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах

ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах

Знать:

ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах

Уметь:

ПК-2.1/Ум3 Идентифицировать и классифицировать актуальные угрозы безопасности персональных данных применительно к конкретному автоматизированному рабочему месту или информационной системе

Владеть:

ПК-2.1/Нв3 Навыками к обоснованному выбору организационных и технических мер защиты, адекватных выявленной модели угроз и профилю нарушителя, для включения в текст регламента

ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности

Знать:

ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных

Уметь:

ПК-2.2/Ум4 Классифицировать выявленные угрозы безопасности персональных данных по заданным признакам

Владеть:

ПК-2.2/Нв3 Методикой классификации угроз информационной безопасности применительно к информационным системам персональных данных

ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации

Знать:

ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных

Уметь:

ПК-2.3/Ум4 Проектировать организационную структуру системы защиты персональных данных и распределять зоны ответственности между сотрудниками

Владеть:

ПК-2.3/Нв3 Методикой разработки «Политики информационной безопасности» и «Положения о защите персональных данных» в части, касающейся прав и обязанностей персонала

ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах

Знать:

ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах

Уметь:

ПК-2.4/Ум4 Разрабатывать планы и программы контрольных мероприятий соблюдения персоналом требований регламента защиты персональных данных

Владеть:

ПК-2.4/Нв2 Методикой проведения внутреннего аудита системы защиты персональных данных на соответствие требованиям законодательства и локальным регламентам

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ПК-2 Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах	Повышенный	ИДК ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах Знать: ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах Уметь: ПК-2.1/Ум3 Идентифицировать и классифицировать актуальные угрозы безопасности персональных данных применительно к конкретному автоматизированному рабочему месту или информационной системе Владеть: ПК-2.1/Нв3 Навыками к обоснованному выбору организационных и технических мер защиты, адекватных выявленной модели угроз и профилю нарушителя, для включения в текст регламента ИДК ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности Знать: ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных Уметь: ПК-2.2/Ум4 Классифицировать выявленные угрозы безопасности персональных данных по заданным признакам Владеть: ПК-2.2/Нв3 Методикой классификации угроз информационной безопасности применительно к информационным системам персональных данных

	ИДК ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации Знать: ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных Уметь: ПК-2.3/Ум4 Проектировать организационную структуру системы защиты персональных данных и распределять зоны ответственности между сотрудниками Владеть: ПК-2.3/Нв3 Методикой разработки «Политики информационной безопасности» и «Положения о защите персональных данных» в части, касающейся прав и обязанностей персонала ИДК ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах Знать: ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах Уметь: ПК-2.4/Ум4 Разрабатывать планы и программы контрольных мероприятий соблюдения персоналом требований регламента защиты персональных данных Владеть: ПК-2.4/Нв2 Методикой проведения внутреннего аудита системы защиты персональных данных на соответствие требованиям законодательства и локальным регламентам
Базовый	ИДК ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах Знать: ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах Уметь: ПК-2.1/Ум3 Идентифицировать и классифицировать актуальные угрозы безопасности персональных данных применительно к конкретному автоматизированному рабочему месту или информационной системе

		ИДК ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности Знать: ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных Уметь: ПК-2.2/Ум4 Классифицировать выявленные угрозы безопасности персональных данных по заданным признакам ИДК ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации Знать: ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных Уметь: ПК-2.3/Ум4 Проектировать организационную структуру системы защиты персональных данных и распределять зоны ответственности между сотрудниками ИДК ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах Знать: ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах Уметь: ПК-2.4/Ум4 Разрабатывать планы и программы контрольных мероприятий соблюдения персоналом требований регламента защиты персональных данных
	Пороговый	ИДК ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах Знать: ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах

		ИДК ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности Знать: ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных ИДК ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации Знать: ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных ИДК ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах Знать: ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах
--	--	---

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах ПК-2.1/Ум3 Идентифицировать и классифицировать актуальные угрозы безопасности персональных данных применительно к конкретному автоматизированному рабочему месту или информационной системе ПК-2.1/Нв3 Навыками к обоснованному выбору организационных и технических мер защиты, адекватных выявленной модели угроз и профилю нарушителя, для включения в текст регламента ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных ПК-2.2/Ум4 Классифицировать выявленные угрозы безопасности персональных данных по заданным признакам ПК-2.2/Нв3 Методикой классификации угроз информационной безопасности применительно к информационным системам персональных данных

	ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных ПК-2.3/Ум4 Проектировать организационную структуру системы защиты персональных данных и распределять зоны ответственности между сотрудниками ПК-2.3/Нв3 Методикой разработки «Политики информационной безопасности» и «Положения о защите персональных данных» в части, касающейся прав и обязанностей персонала ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах ПК-2.4/Ум4 Разрабатывать планы и программы контрольных мероприятий соблюдения персоналом требований регламента защиты персональных данных ПК-2.4/Нв2 Методикой проведения внутреннего аудита системы защиты персональных данных на соответствие требованиям законодательства и локальным регламентам
Хорошо	ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах ПК-2.1/Ум3 Идентифицировать и классифицировать актуальные угрозы безопасности персональных данных применительно к конкретному автоматизированному рабочему месту или информационной системе ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных ПК-2.2/Ум4 Классифицировать выявленные угрозы безопасности персональных данных по заданным признакам ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных ПК-2.3/Ум4 Проектировать организационную структуру системы защиты персональных данных и распределять зоны ответственности между сотрудниками

	ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах ПК-2.4/Ум4 Разрабатывать планы и программы контрольных мероприятий соблюдения персоналом требований регламента защиты персональных данных
Удовлетворительно	ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах
Неудовлетворительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Практическая работа Тестирование
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Анализ объекта защиты и идентификация персональных данных	ПК-2.1	Практическая работа Тестирование	Экзамен
2	Оценка угроз и рисков безопасности персональных данных	ПК-2.1 ПК-2.2	Практическая работа Тестирование	Экзамен
3	Проектирование организационных и технических мер защиты	ПК-2.3 ПК-2.4	Практическая работа Тестирование	Экзамен

4	Регламентация процедур обработки и жизненный цикл документа	ПК-2.3 ПК-2.4	Практическая работа Тестирование	Экзамен
---	---	---------------	-------------------------------------	---------

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 7 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

6. Оценочные материалы текущего контроля

Раздел 1. Анализ объекта защиты и идентификация персональных данных

Контролируемые ИДК: ПК-2.1

Тема 1.1. Введение в разработку регламентов защиты ПДн

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Идентификация персональных данных и субъектов в организации

Определите гипотетическую организацию, для которой будет разрабатываться регламент. Определите перечень обрабатываемых категорий ПДн. Определите категории субъектов ПДн

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое регламент защиты персональных данных?

2. Какие основные нормативные правовые акты регулируют обработку персональных данных в РФ?

3. Какие сведения необходимо определить при выборе гипотетической организации для разработки регламента?

Тема 1.2. Инвентаризация персональных данных и субъектов

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Назовите категории персональных данных по 152-ФЗ.
2. Приведите примеры специальных категорий персональных данных.
3. Какие категории субъектов персональных данных можно выделить в типичной организации?

Тема 1.3. Картирование потоков персональных данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Моделирование потоков персональных данных и определение мер защиты
- Построение DFD-диаграммы для вашей организации. Определение перечня организационных и технических мер по обеспечению информационной безопасности. Детализация списка ПДн.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое карта (схема) потоков персональных данных?
2. Какие элементы обязательно отражаются на DFD-диаграмме потоков ПДн?
3. С какой целью строится карта потоков персональных данных?

Раздел 2. Оценка угроз и рисков безопасности персональных данных

Контролируемые ИДК: ПК-2.1 ПК-2.2

Тема 2.1. Моделирование угроз безопасности ПДн

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что понимается под угрозой безопасности персональных данных?
2. Назовите основные источники угроз для персональных данных.
3. Какие классификации угроз используются при моделировании?
4. Где можно получить актуальный перечень угроз безопасности ПДн?

Тема 2.2. Оценка рисков и их документирование

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Оценка уровня защищенности и регламентация прав субъектов персональных данных

Определение уровня защищенности ПДн. Описание прав субъекта ПДн.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое риск информационной безопасности при обработке ПДн?
2. Какие методы оценки рисков существуют?
3. Что включает в себя реестр рисков?

Раздел 3. Проектирование организационных и технических мер защиты

Контролируемые ИДК: ПК-2.3 ПК-2.4

Тема 3.1. Организационные и технические меры защиты ПДн

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Формирование раздела мер и условий обеспечения безопасности персональных данных

Описание мер и условий защиты и обеспечения безопасности персональных данных.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие группы мер защиты персональных данных предусмотрены нормативными документами?
2. Приведите примеры организационных мер защиты ПДн.
3. Что относится к техническим мерам защиты ПДн?
4. Какие требования предъявляются к помещениям, где обрабатываются ПДн?

Тема 3.2. Распределение ответственности и регламентация действий персонала

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Разработка раздела о правах и обязанностях оператора и согласия на обработку ПДн
- Описание прав и обязанностей оператора ПДн. Составление согласия на обработку ПДн клиента или сотрудника.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие должностные лица обычно назначаются ответственными за обеспечение безопасности ПДн в организации?
2. Какие обязанности включаются в должностные инструкции сотрудников, работающих с ПДн?
3. Что должно быть указано в разделе регламента «Права и обязанности оператора»?
4. Какие обязанности у оператора при сборе персональных данных через интернет-сайт?

Раздел 4. Регламентация процедур обработки и жизненный цикл документа

Контролируемые ИДК: ПК-2.3 ПК-2.4

Тема 4.1. Взаимодействие с субъектами персональных данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Регламентация порядка и условий обработки персональных данных
- Описание порядка и условий обработки ПДн.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие права имеет субъект персональных данных согласно 152-ФЗ?
2. Какие обязательные элементы должно содержать согласие на обработку персональных данных?
3. В течение какого срока оператор обязан предоставить субъекту информацию о наличии его персональных данных?

Тема 4.2. Управление инцидентами и изменениями

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Определение порядка уничтожения, блокирования, исправления, актуализации ПДн и обстоятельств изменения регламента

Описание порядка уничтожения, блокирования, исправления и актуализации ПДн. Описание обстоятельств изменения регламента.

2. Разработка порядка реагирования на инциденты и описание ответственности за нарушения

Разработка порядка реагирования на инциденты, связанные с ПДн. Описание ответственности за нарушение норм обработки и защиты ПДн.

3. Компонировка и оформление итогового регламента по защите персональных данных
Формирование регламента по защите ПДн (на основе предыдущих практических работ).

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Каков порядок уничтожения персональных данных по требованию субъекта или по истечении срока обработки?

2. Что должно быть предусмотрено в порядке реагирования на инциденты, связанные с ПДн?

3. Какие обстоятельства могут служить основанием для изменения регламента защиты ПДн?

7. Оценочные материалы промежуточной аттестации

7 семестр, Экзамен

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4

Вопросы/Задания:

1. Юридическая и техническая природа регламента защиты персональных данных: соотношение понятий, место в системе локальных нормативных актов оператора.

2. Специфика идентификации и документирования специальных и биометрических персональных данных при разработке регламента.

3. Категории субъектов персональных данных и особенности правового режима обработки данных разных категорий

4. Соотношение понятий «угроза», «уязвимость» и «риск» применительно к разработке раздела регламента об оценке угроз

5. Методика определения актуальных угроз безопасности персональных данных с использованием Банка данных угроз ФСТЭК России

6. Соотношение требований Приказа ФСТЭК № 21 и других нормативных документов при формировании перечня мер защиты в регламенте

7. Особенности регламентации защиты персональных данных в зависимости от уровня защищенности информационной системы

8. Проблема обеспечения достаточности и избыточности мер защиты при разработке регламента

9. Требования к помещениям, в которых осуществляется обработка персональных данных

10. Распределение ответственности за обеспечение безопасности персональных данных между различными категориями персонала
11. Права и обязанности оператора персональных данных
12. Юридически значимые элементы согласия на обработку персональных данных и последствия их отсутствия
13. Основания и порядок отзыва согласия на обработку персональных данных
14. Процедуры уничтожения, блокирования, исправления и актуализации персональных данных
15. Порядок реагирования на инциденты информационной безопасности, связанные с персональными данными
16. Виды ответственности за нарушение норм обработки и защиты персональных данных
17. Основания и процедура пересмотра регламента защиты персональных данных в условиях изменяющейся нормативной среды
18. Система законодательства РФ в области персональных данных
19. Сравнительный анализ понятий «оператор», «обработка», «распространение», «предоставление» и «трансграничная передача» персональных данных
20. Критерии отнесения персональных данных к специальным, биометрическим и общедоступным категориям
21. Взаимосвязь уровня защищенности персональных данных и выбранных мер защиты: как результаты оценки рисков трансформируются в требования регламента?
22. Права субъекта персональных данных
23. Правовое регулирование обработки персональных данных работников
24. Правовое регулирование обработки персональных данных клиентов
25. Порядок действий оператора при получении требования субъекта о прекращении обработки или отзыве согласия
26. Понятие инцидента информационной безопасности, связанного с персональными данными
27. Особенности разработки регламента для оператора, осуществляющего трансграничную передачу персональных данных
28. Обработка персональных данных без использования средств автоматизации

29. Методика проведения внутреннего аудита соблюдения требований регламента защиты персональных данных

30. Проблемные аспекты локализации баз данных персональных данных на территории РФ