Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2023 12:38:19
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)»

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.В.03.10 «ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Направление подготовки:
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника: **бакалавр**

Тольятти 2023

Рабочая программа дисциплины «Организация защиты персональных данных» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

Составители:

старший преподаватель (ученая степень, ученое звание) Коновалова А.Д. (ФИО)

РПД обсуждена на заседании Высшей школы интеллектуальных систем и кибертехнологий

10.11.2023 г., протокол № 3

Директор ВШИСиКТ к.э.н., доцент (уч.степень, уч.звание) Филиппова О.А. (ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

- формирование способности организовывать защиту персональных данных в деятельности оператора на основе применимых нормативных правовых актов, нормативных и методических документов, обосновывать организационные и технические меры защиты и контролировать их выполнение.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине	Основание (ПС) *для профессиональных компетенций
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИОПК-6.1. Применяет технологии, методы и средства защиты информации ограниченного доступа. ИОПК-6.2. Знает и применяет положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа.	**Знает:** правовые основания и принципы обработки персональных данных; права субъектов и обязанности оператора; требования к организации защиты персональных данных при автоматизированной и неавтоматизированной обработке; порядок определения угроз и уровней защищенности, выбора организационных и технических мер защиты **Умеет:** обследовать процессы обработки персональных данных; определять состав защищаемых сведений и границы ИСПДн; обосновывать применимые требования, уровень защищенности и набор мер; разрабатывать локальные документы и правила доступа; проверять выполнение мер на учебном примере **Владеет:** навыками составления реестра процессов обработки, описания угроз и нарушителей, документирования мер защиты, планирования контроля, организации реагирования на инциденты и подготовки доказательств выполнения требований по защите персональных данных	-
ПК-1 Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ИПК-1.1. Устанавливает, настраивает и обслуживает программное обеспечение, программно-аппаратные и технические средства защиты информации с соблюдением требований по защите информации ИПК-1.2. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации		06.032 «Специалист по безопасности компьютерных систем и сетей»

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы (Б1.В.03 Профессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **3 з.е. (108 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**64/48**
занятия лекционного типа (лекции)	32/24
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	32/24
Лабораторные работы	0/0
Самостоятельная работа всего, в т.ч.:	**44/56**
Самоподготовка по темам (разделам) дисциплины	44/56
Контроль (часы на зачет)	**0/4**
Промежуточная аттестация	**Зачёт**

Примечание: -/- объем часов соответственно для очной, очно-заочной форм обучения.

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-6 ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 1. ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК ОБЪЕКТ ЗАЩИТЫ. НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ** Содержание лекции: Понятие персональных данных и идентифицируемости физического лица. Субъект, оператор и лицо, осуществляющее обработку по поручению оператора. Операции обработки, автоматизированная и неавтоматизированная обработка. Общие, специальные категории и биометрические персональные данные; особенности данных, разрешенных субъектом для распространения. Конфиденциальность, целостность и доступность в системе защиты прав субъектов. Федеральный закон № 152-ФЗ, его связь с законодательством об информации и трудовыми отношениями. Разграничение полномочий Роскомнадзора, ФСТЭК России и ФСБ России. Иерархия нормативных требований и локальных актов оператора. Проверка редакции и области применения документа. Различие правомерности обработки и безопасности информационной системы. Ответственность участников обработки и пределы полномочий специалиста по защите информации.	4/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 1. Идентификация персональных данных и составление карты нормативных требований.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	5/7	Самостоятельное изучение учебных материалов
ОПК-6 ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 2. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЕ ПРАВ СУБЪЕКТОВ** Содержание лекции: Законность и заранее определенные цели обработки. Соответствие состава и объема данных заявленным целям, недопустимость избыточности. Основания обработки: закон, договор, согласие и иные предусмотренные законом случаи. Требования к согласию, его доказуемость и отзыв; отдельное оформление согласия в предусмотренных законом случаях. Особые условия обработки специальных категорий, биометрических данных и данных, разрешенных для распространения. Предоставление информации субъекту, уточнение, блокирование, прекращение обработки и уничтожение. Уведомление уполномоченного органа об обработке и актуализация сведений. Поручение обработки: цели, операции, конфиденциальность, безопасность и распределение обязанностей. Локализация баз данных и трансграничная передача как самостоятельные требования. Сроки хранения и связь с обязанностями оператора.	4/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	Правовые последствия неправомерной обработки и порядок документирования решений.					
	Практическая работа 2. Обоснование обработки и подготовка документов для взаимодействия с субъектом.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	5/7	Самостоятельное изучение учебных материалов
ОПК-6 ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 3. ОБСЛЕДОВАНИЕ ПРОЦЕССОВ ОБРАБОТКИ И ОРГАНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ** Содержание лекции: Инвентаризация процессов, информационных систем, носителей и внешних взаимодействий. Границы ИСПДн, состав оборудования, программного обеспечения и пользователей. Жизненный цикл данных: сбор, использование, передача, хранение и уничтожение. Схемы потоков и выявление неучтенных копий. Реестр процессов обработки и перечень информационных ресурсов. Организационная структура защиты: руководитель оператора, ответственный за организацию обработки, ответственный за безопасность, владельцы процессов, администраторы и пользователи. Принцип разделения обязанностей. Политика обработки персональных данных и локальные акты: различия по назначению, содержанию и доступности. Порядок допуска персонала, обучение и обязательства по конфиденциальности. Управление документами: утверждение, версии, ознакомление, пересмотр. План создания и поддержания системы защиты с ответственными и проверяемыми результатами.	4/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 3. Обследование ИСПДн и разработка комплекта организационных документов.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	6/7	Самостоятельное изучение учебных материалов
ОПК-6 ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 4. МОДЕЛИРОВАНИЕ УГРОЗ И ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ИСПДН** Содержание лекции: Цель оценки угроз и исходные данные об объекте защиты. Защищаемые активы и негативные последствия для субъектов. Внешние и внутренние нарушители, их возможности и доступ. Источники угроз, уязвимости, способы реализации и условия возникновения угроз. Модель угроз как обоснование мер защиты, а не перечень всех записей банка угроз. Использование банка данных угроз ФСТЭК России и применимой методики оценки угроз. Документирование допущений и проверка их обоснованности. Угрозы, связанные с недекларированными	4/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	возможностями системного и прикладного программного обеспечения. Критерии постановления Правительства РФ № 1119: категории данных, категории и число субъектов, тип актуальных угроз. Порядок определения требуемого уровня защищенности и оформления решения. Различие уровня защищенности ИСПДн и уровня доверия к средству защиты. Пересмотр модели при изменении инфраструктуры или обработки.					
	Практическая работа 4. Разработка модели угроз и обоснование уровня защищенности.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	6/7	Самостоятельное изучение учебных материалов
ОПК-6 ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 5. ВЫБОР ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ** Содержание лекции: Переход от требований и модели угроз к проекту системы защиты. Базовый набор мер по приказу ФСТЭК России № 21, его адаптация, уточнение и дополнение. Обоснование компенсирующих мер в допустимых случаях. Идентификация и аутентификация; управление доступом и регистрация событий; защита носителей; антивирусная защита; обнаружение вторжений; анализ защищенности; обеспечение целостности и доступности; защита среды виртуализации и каналов связи. Требования к применяемым средствам защиты и проверке их документации. Условия применения криптографической защиты и нормативные документы ФСБ России, включая приказ № 378. Различие шифрования, обезличивания и уничтожения. Матрица «угроза - требование - мера - средство - доказательство». Проектирование ролей и минимальных привилегий. Оценка эффективности мер до ввода системы в эксплуатацию. Документирование ограничений и остаточных рисков.	4/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 5. Обоснование набора мер и разработка матрицы доступа.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	6/7	Самостоятельное изучение учебных материалов
ОПК-6 ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 6. ЗАЩИТА ПРИ НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ, ПЕРЕДАЧЕ И ХРАНЕНИИ ДАННЫХ** Содержание лекции: Особенности обработки без использования средств автоматизации по постановлению Правительства РФ № 687. Обособление персональных данных от иной информации, требования к материальным носителям и типовым формам документов.	4/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
	Разделение обработки по целям, контроль доступа к местам хранения, учет выдачи и возврата. Предотвращение ознакомления посторонних лиц с журналами и списками. Печать, копирование, сканирование и уничтожение бумажных документов. Учет съемных носителей, транспортирование, хранение и вывод из эксплуатации. Передача данных адресату: проверка полномочий и реквизитов, минимизация состава, защищенные каналы, подтверждение получения. Облачные сервисы и обработка по поручению: границы ответственности и контроль договора. Удаленная работа и личные устройства. Сроки хранения, блокирование, удаление и подтверждение уничтожения; восстановление из резервных копий как часть жизненного цикла.					
	Практическая работа 6. Разработка регламента обращения с носителями и передачи персональных данных.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	6/7	Самостоятельное изучение учебных материалов
ОПК-6 ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ТЕМА 7. ЭКСПЛУАТАЦИЯ СИСТЕМЫ ЗАЩИТЫ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ** Содержание лекции: Поддержание мер защиты в процессе эксплуатации. Контроль учетных записей, изменений конфигурации, обновлений и резервного копирования. Регистрация и анализ событий, признаки инцидента и источники подтверждающей информации. Сообщение пользователя, первичная оценка, ограничение распространения, сохранение доказательств и восстановление. Разграничение инцидента безопасности и нарушения прав субъектов персональных данных. Обязанности оператора при выявлении неправомерной или случайной передачи данных. Содержание первичного и дополнительного уведомлений уполномоченного органа; определение сроков по действующей редакции закона. Взаимодействие руководства, ответственного за обработку, службы безопасности, юриста и подрядчика. Учет инцидентов и документирование решений. Разбор причин, корректирующие меры и повторная проверка. Учебные тренировки и проверка готовности персонала.	4/3	-	-	-	Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 7. Разработка порядка реагирования и разбор учебного инцидента.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	5/7	Самостоятельное изучение учебных материалов
ОПК-6	**ТЕМА 8. КОНТРОЛЬ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ И СОВЕРШЕНСТВОВАНИЕ**	4/3	-	-	-	Лекция-визуализация (в

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ИОПК-6.1 ИОПК-6.2 ПК-1 ИПК-1.1 ИПК-1.2	**ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ** Содержание лекции: Внутренний контроль и оценка эффективности мер защиты: цели, критерии, периодичность и основания внеплановой проверки. Планирование проверки по процессам и информационным системам. Проверка документов, интервью и анализ технических свидетельств. Прослеживаемость от требования до доказательства; достаточность и достоверность выборки. Оценка соответствия мер модели угроз, уровню защищенности и фактической инфраструктуре. Различие внутренней проверки, оценки эффективности и аттестации; недопустимость подмены одного вида работ другим. Документирование несоответствий: факт, критерий, доказательство, риск, мероприятие, срок и ответственный. Контроль устранения и повторная проверка. Обновление документации и обучение сотрудников по результатам контроля. Подготовка доказательств для взаимодействия с надзорным органом. Итоговое обоснование системы защиты учебной организации.					т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа 8. Проведение внутренней проверки и защита проекта организации защиты данных.	-	-	4/3	-	Отчёт по практической работе
	Самостоятельная работа.	-	-	-	5/7	Самостоятельное изучение учебных материалов
	ИТОГО	**32/24**	**0/0**	**32/24**	**44/56**	

Примечание: -/- объем часов соответственно для очной, очно-заочной форм обучения.

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- электронное обучение;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом по ней подлежит защите преподавателю.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;

- качество оформления отчета по работе;

- качество устных ответов на контрольные вопросы при защите работы.

Лабораторные работы организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа / на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также

решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;

- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.
2. Работу с ресурсами Интернет
3. Самостоятельное изучение учебных материалов

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учеб. пособие / С. Н. Никифоров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.]: Лань, 2023. - 93 с. - Прил. - URL: https://reader.lanbook.com/book/288974 (дата обращения: 02.09.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45868-4. - Текст: электронный.

2. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб. пособие / С. Н. Никифоров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.]: Лань, 2023. - 121 с. - Прил. - URL: https://reader.lanbook.com/book/338018 (дата обращения: 02.09.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-47181-2. - Текст: электронный.

3. Сычев, Ю. Н. Защита информации и информационная безопасность: учеб. пособие для студентов высш. учеб. заведений по направлению подгот. 10.03.01. "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю. Н. Сычев. - Документ read. - Москва: ИНФРА-М, 2023. - 201 с. - (Высшее образование - Бакалавриат). - Прил. - URL: https://znanium.ru/read?id=420080 (дата обращения: 02.09.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-107471-8. - Текст: электронный.

Дополнительная литература

4. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. - Документ read. - Москва [и др.]: Инфра-Инженерия, 2020. - URL: https://znanium.com/read?id=361651 (дата обращения: 02.09.2023). - Режим доступа: для авториз. пользователей. - Текст: электронный.

5. Брюхомицкий, Ю. А. Искусственные иммунные системы в информационной безопасности: учеб. пособие / Ю. А. Брюхомицкий ; ФГАОУ ВО "Юж. федер. ун-т", Инж.-технол. акад. – Документ read. – Ростов-на-Дону [и др.]: Изд-во Юж. федер. ун-та, 2019. – 147 с. – URL: https://znanium.com/read?id=357432 (дата обращения: 02.09.2023). - Режим доступа: для авториз. пользователей. – ISBN 978-5-9275-3212-4. – Текст: электронный.

6. Зверева, В. П. Организация и технология работы с конфиденциальными документами: учеб. для сред. проф. образования по специальности 2.10.02.1 "Орг. и технология защиты информации" / В. П. Зверева, А. В. Назаров. - Документ read. - Москва: Курс [и др.], 2023. - 320 с. - (Среднее профессиональное образование). - Глоссарий. - URL: https://znanium.ru/read?id=428073 (дата обращения: 02.09.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-906818-96-6. - 978-5-16-105466-6. - Текст: электронный.

7. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учеб. пособие для студентов вузов по специальностям 090103 "Орг. и технология защиты информ.", 090104 "Комплексная защита объектов информатизации" / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ФОРУМ [и др.], 2014. - 255 с. - ISBN 978-5-91134-856-4. - 978-5-16-009578-3: 380-00. - Текст: непосредственный.

8. Чепурнова, Н. М. Правовые основы прикладной информатики: учеб. пособие / Н. М. Чепурнова, Л. Л. Ефимова. - Документ read. - Москва: Курс [и др.], 2019. - 192 с. - URL: https://znanium.com/read?id=354636 (дата обращения: 02.09.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-906818-01-0. - 978-5-16-102928-2. - Текст: электронный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. 3DNEWS.RU: Электронное периодическое издание: сайт. – Москва, 1997 - . - URL: https://3dnews.ru/ (дата обращения: 09.11.2023). – Текст: электронный.
2. eLIBRARY.RU: научная электронная библиотека: сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 09.11.2023). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
3. КонсультантПлюс: справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения: 09.11.2023). - Текст : электронный.
4. Электронная библиотека. Техническая литература : сайт. - URL : http://techliter.ru/ (дата обращения: 09.11.2023). - Текст : электронный.
5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.
6. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный.
7. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения: 09.11.2023). - Режим доступа: для авториз. пользователей. - Текст : электронный

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (доступ через ЭИОС университета)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук). Для проведения лабораторных работ используется учебная аудитория «Лаборатория информационных технологий, информатики и методов программирования // Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации // Помещение для хранения и профилактического обслуживания учебного оборудования (Г-413)», оснащенная следующим оборудованием: рабочие места обучающихся; Рабочее место преподавателя; Учебно-наглядные пособия, обеспечивающие тематические иллюстрации. Компьютер Асус Intel G530\iH61\GeForceGT430\4096 Mb DDR3\500Gb\LCD 22" - 14 шт., Компьютер в сборе iP2.0 LCD - 1 шт., принтер HP 1200 - 1 шт., мобильный экран проекционный DraperLuma - 1 шт., мобильный проектор Sanyo PLC, Сетевое оборудование D-Link DES-1024D, 24-портовый; локальная сеть 100 мб с доступом в Интернет 50 мб. Лаборатория оснащена кондиционером.

Лабораторные работы. Для проведения лабораторных работ используется учебная аудитория «Лаборатория информационных технологий, информатики и методов программирования // Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации // Помещение для хранения и профилактического обслуживания учебного оборудования (Г-413)», оснащенная следующим оборудованием: рабочие места обучающихся; Рабочее место преподавателя; Учебно-наглядные пособия, обеспечивающие тематические иллюстрации. Компьютер Аксус Intel G530\iH61\GeForceGT430\4096 Mb DDR3\500Gb\LCD 22" - 14 шт., Компьютер в сборе iP2.0 LCD - 1 шт., принтер HP 1200 - 1 шт., мобильный экран проекционный DraperLuma - 1 шт., мобильный проектор Sanyo PLC, Сетевое оборудование D-Link DES-1024D, 24-портовый; локальная сеть 100 мб с доступом в Интернет 50 мб. Лаборатория оснащена кондиционером.

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

- компьютерные классы университета;
- библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

- формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма промежуточной аттестации	Уровень сформированности	100-балльная шкала, %	Шкала освоения, %	5-балльная дифференцированная оценка/балл
зачет	допороговый	ниже 61	ниже 61	не зачтено
	пороговый	61–85,9	61–69,9	зачтено
	пороговый	61–85,9	70–85,9	зачтено
	повышенный	86–100	86–100	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Посещение лекционного занятия (конспект лекций)	8	2	16
Выполнение лабораторных работ	8	8	64
Самостоятельная работа (портфолио по темам)	8	2	16
Творческий рейтинг (итоговая защита проекта)	1	4	4
Итого по дисциплине			**100 баллов**

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа 1. Идентификация персональных данных и составление карты нормативных требований

Задание 1. Разделите сведения по процессам и категориям. Объясните, почему фотография или видеозапись не во всех случаях является биометрическими персональными данными.

Задание 2. Установите оператора, субъектов, пользователей и возможного обработчика по поручению. Не смешивайте правовую роль оператора с ролью системного администратора.

Задание 3. Для каждого процесса определите применимые нормативные документы и вопросы, которые необходимо уточнить у владельца процесса. Проверьте необходимость каждого поля анкеты.

Задание 4. Составьте карту «процесс - данные - цель - нормативное требование - ответственное лицо». Сформулируйте не менее пяти выводов об организации защиты.

Практическая работа 2. Обоснование обработки и подготовка документов для взаимодействия с субъектом

Задание 1. Составьте отдельные записи о целях обработки и основаниях для трудовых отношений, исполнения договора и рекламы. Не считайте согласие универсальным основанием для любой операции.

Задание 2. Разработайте отдельный проект согласия для рекламной коммуникации; укажите данные и операции в минимально необходимом объеме, порядок отзыва и способ подтверждения согласия.

Задание 3. Подготовьте алгоритм рассмотрения обращения: проверка полномочий заявителя, регистрация, определение оснований дальнейшей обработки, прекращение необязательных операций, ответ и документирование результата.

Задание 4. Сформулируйте условия поручения обработки подрядчику и порядок контроля их исполнения. Отдельно укажите обязанности оператора, которые поручение не устраняет.

Практическая работа 3. Обследование ИСПДн и разработка комплекта организационных документов

Задание 1. Выделите процессы обработки, источники и получателей данных. Постройте схему потоков с обозначением каналов, носителей и границ ответственности.

Задание 2. Составьте реестр ИСПДн: назначение, категории субъектов и данных, места хранения, компоненты, пользователи, внешние соединения и владельцы процессов.

Задание 3. Подготовьте матрицу ответственности для руководителя, ответственного за обработку, специалиста по безопасности, администратора и пользователя. Устраните конфликт самоконтроля.

Задание 4. Сформируйте перечень локальных актов и календарный план внедрения. Для каждого мероприятия задайте ответственного, результат и способ приемки; разработайте фрагмент политики и порядок допуска.

Практическая работа 4. Разработка модели угроз и обоснование уровня защищенности

Задание 1. Охарактеризуйте активы, границы системы и возможных нарушителей. Отделите исходные факты от допущений; перечислите недостающие сведения.

Задание 2. Разработайте не менее пяти сценариев угроз по схеме «источник - доступ - уязвимость или условие - действие - последствие». Свяжите каждый сценарий с конкретным компонентом.

Задание 3. Определите уровень защищенности для основного задания и варианта Б. Приведите нормативное обоснование; не выводите тип угроз только из факта подключения к Интернету.

Задание 4. Составьте решение об уровне защищенности и перечень событий для пересмотра модели. Обоснуйте меры ограничения удаленного доступа подрядчика.

Практическая работа 5. Обоснование набора мер и разработка матрицы доступа

Задание 1. На основании модели угроз и уровня защищенности сформируйте применимый набор мер. Укажите исходный базовый набор, причины адаптации и дополнительные меры по актуальным угрозам.

Задание 2. Составьте матрицу «роль - ресурс - операция - условие доступа». Предусмотрите выдачу, изменение и отзыв полномочий, персональные учетные записи и контроль привилегированных действий.

Задание 3. Определите регистрируемые события, требования к защите журналов и порядок их анализа. Обоснуйте меры против неконтролируемых выгрузок и несанкционированного удаленного доступа.

Задание 4. Разработайте план проверки эффективности: предпосылка, действие проверяющего, ожидаемый результат, подтверждающий материал и критерий приемки. Включите сценарий восстановления резервной копии.

Практическая работа 6. Разработка регламента обращения с носителями и передачи персональных данных

Задание 1. Определите недостатки типовой формы журнала и порядка его использования. Предложите изменение состава данных и способ регистрации, исключающий ознакомление посетителей с чужими записями.

Задание 2. Разработайте правила хранения, учета, выдачи и возврата документов и носителей. Укажите должностных лиц, записи учета и порядок проверки наличия.

Задание 3. Составьте алгоритм согласованной передачи: проверка правового основания и получателя, отбор данных, выбор канала, контроль отправки и регистрация результата. Опишите порядок отказа от личных носителей.

Задание 4. Подготовьте процедуру прекращения обработки и подтверждения уничтожения по всем местам хранения. Разграничьте удаление файла, уничтожение данных и физическое уничтожение носителя.

Практическая работа 7. Разработка порядка реагирования и разбор учебного инцидента

Задание 1. Составьте хронологию фактов и список проверяемых гипотез. Определите первичные меры ограничения ущерба и сохранения журналов, не подменяя расследование недоказанными выводами.

Задание 2. Распределите задачи между руководителем, ответственным за обработку, специалистом по безопасности и администратором. Определите, кто принимает решение и кто документирует его.

Задание 3. Подготовьте карточку инцидента и проекты первичного и дополнительного уведомлений при наличии установленного законом основания. Определите сроки по нормативному источнику и отметьте неизвестные на момент подготовки сведения.

Задание 4. Разработайте план восстановления, устранения причин и проверки результата. Укажите меры, которые предотвратят повторение ошибочной отправки и неконтролируемого экспорта.

Практическая работа 8. Проведение внутренней проверки и защита проекта организации защиты данных

Задание 1. Составьте программу проверки с критериями, источниками доказательств, ответственными и объемом выборки. Охватите правомерность обработки, организационные меры и технические проверки.

Задание 2. Оформите каждое несоответствие по схеме «требование - факт - доказательство - последствия». Отделите установленное нарушение от недостаточности доказательств.

Задание 3. Разработайте план корректирующих мероприятий с приоритетами, сроками, ответственными и критериями закрытия. Обоснуйте необходимость пересмотра модели угроз и правил доступа.

Задание 4. Представьте итоговый комплект документов и защитите согласованность решений. Покажите, как изменение цели обработки или компонента системы отражается в остальных документах.

8.2.2. Типовые задания для лабораторных работ

Лабораторные работы учебным планом не предусмотрены. Типовые лабораторные задания не формируются; оценивание за лабораторные работы не проводится.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Устно-письменная форма по билетам предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов и заданий для подготовки к зачету

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

1. Понятие персональных данных. Идентификация субъекта по прямым и косвенным признакам. Приведите примеры спорных случаев.
2. Оператор и лицо, осуществляющее обработку по поручению. Распределение обязанностей и ответственности.
3. Категории персональных данных. Условия отнесения сведений к специальным категориям и биометрическим данным.
4. Автоматизированная и неавтоматизированная обработка: признаки и применимые требования к защите.
5. Система нормативного регулирования. Полномочия Роскомнадзора, ФСТЭК России и ФСБ России.
6. Принципы обработки персональных данных. Проверка соответствия состава данных цели обработки.
7. Правовые основания обработки данных работника и клиента. Случаи обработки без согласия.
8. Согласие на обработку персональных данных: содержание, доказуемость, отдельное оформление и отзыв.
9. Обработка данных, разрешенных субъектом для распространения. Отличие от предоставления определенному получателю.
10. Права субъекта и порядок рассмотрения обращения. Проверка полномочий заявителя и документирование ответа.
11. Уведомление об обработке персональных данных и поддержание сведений об операторе в актуальном состоянии.
12. Поручение обработки, локализация и трансграничная передача. Разграничение требований и проверяемые документы.
13. Обследование процессов обработки. Состав исходных данных и методы выявления неучтенных копий.
14. Границы ИСПДн и ее состав. Учет внешних сервисов, удаленного доступа и резервных копий.
15. Реестр процессов обработки и схема потоков данных. Назначение и взаимосвязь документов.
16. Ответственный за организацию обработки и ответственный за безопасность данных. Разделение функций.
17. Политика обработки персональных данных и внутренние локальные акты. Порядок утверждения и актуализации.
18. Обучение и допуск персонала к обработке. Подтверждение ознакомления и контроль соблюдения правил.
19. Модель угроз ИСПДн: назначение, исходные данные, структура и основания пересмотра.
20. Модель нарушителя: внутренние и внешние нарушители, возможности и условия доступа.
21. Связь активов, уязвимостей, угроз и негативных последствий. Обоснование актуальности угрозы.

22. Применение банка данных угроз ФСТЭК России. Почему выгрузка банка не заменяет модель угроз?

23. Типы угроз по постановлению Правительства РФ № 1119 и их учет при выборе уровня защищенности.

24. Критерии определения уровня защищенности ИСПДн. Документирование исходных данных и решения.

25. Порядок выбора организационных и технических мер: базовый набор, адаптация, уточнение, дополнение.

26. Идентификация, аутентификация и управление доступом. Принципы минимальных привилегий и разделения обязанностей.

27. Учетные записи и матрица доступа. Выдача, пересмотр и отзыв полномочий.

28. Регистрация событий безопасности. Состав событий, защита журналов и организация анализа.

29. Защита от вредоносного программного обеспечения, анализ защищенности и управление обновлениями.

ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно- аппаратных (в том числе криптографических) и технических средств защиты информации

30. Криптографическая защита персональных данных: условия применения, выбор средств и организация эксплуатации.

31. Требования к неавтоматизированной обработке. Обособление данных, типовые формы и доступ к местам хранения.

32. Учет, хранение и передача бумажных документов и машинных носителей. Контроль выдачи и возврата.

33. Передача персональных данных по сети: проверка получателя, минимизация состава и выбор мер защиты.

34. Организация защиты при удаленной работе и использовании услуг подрядчика.

35. Хранение, блокирование, удаление и уничтожение данных. Подтверждающие документы и учет копий.

36. Обезличивание, шифрование и уничтожение: различия целей, результатов и ограничений.

37. Эксплуатационный контроль системы защиты. Учет изменений и периодический пересмотр мер.

38. Признаки инцидента безопасности и первичные действия работника. Регистрация и эскалация.

39. Сохранение доказательств при расследовании инцидента. Источники, целостность и ограничение доступа.

40. Обязанности оператора при нарушении прав субъектов вследствие неправомерной или случайной передачи данных.

41. Содержание первичного и дополнительного уведомлений об инциденте. Определение сроков по действующему закону.

42. Восстановление после инцидента, устранение причин и проверка корректирующих мер.

43. Оценка эффективности мер до ввода ИСПДн в эксплуатацию. Критерии и подтверждающие материалы.

44. Программа внутреннего контроля. Документальная проверка, интервью, технические свидетельства и выборка.

45. Оформление несоответствия и план корректирующих мероприятий. Проверка закрытия нарушения.

46. Внутренний контроль, оценка эффективности и аттестация: цели и границы применимости.

47. Подготовка документов и доказательств выполнения требований для взаимодействия с уполномоченным органом.

48. Согласованность реестра процессов, модели угроз, уровня защищенности, мер защиты и локальных актов.