

УТВЕРЖДАЮ

Первый проректор, проректор по  
УР

\_\_\_\_\_ А.Е. Рудин

«31» \_\_\_ 10 \_\_\_ 2023 года

## Рабочая программа дисциплины

**Б1.В.03**

Организация и технологии защиты персональных данных

Учебный план: 2024-2025 10.04.01 ИИТА ПСЗИнП ОО №2-1-159.plx

Кафедра: **20** Интеллектуальных систем и защиты информации

Направление подготовки:  
(специальность) 10.04.01 Информационная безопасность

Профиль подготовки: Проектирование систем защиты информации на предприятии  
(специализация)

Уровень образования: магистратура

Форма обучения: очная

### План учебного процесса

Семестр (курс для ЗАО)	Контактная работа обучающихся			Сам. работа	Контроль, час.	Трудоём- кость, ЗЕТ	Форма промежуточной аттестации	
	Лекции	Практ. занятия	Лаб. занятия					
2	УП	34	34	17	22,75	0,25	3	Зачет
	РПД	34	34	17	22,75	0,25	3	
3	УП	17	34	17	41,5	34,5	4	Экзамен
	РПД	17	34	17	41,5	34,5	4	
Итого	УП	51	68	34	64,25	34,75	7	
	РПД	51	68	34	64,25	34,75	7	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455

Составитель (и):

кандидат технических наук, Доцент

\_\_\_\_\_

Бусыгин К.Н.

От кафедры составителя:

Заведующий кафедрой интеллектуальных систем и  
защиты информации

\_\_\_\_\_

Макаров Авинир  
Геннадьевич

От выпускающей кафедры:

Заведующий кафедрой

\_\_\_\_\_

Макаров Авинир  
Геннадьевич

Методический отдел:

\_\_\_\_\_

## 1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

**1.1 Цель дисциплины:** Формирование компетенций обучающихся в области работы с персональными данными и методам их защиты в корпоративных системах

**1.2 Задачи дисциплины:**

- раскрыть теоретические, практические и методические вопросы обеспечения информационной безопасности;
- научить применению методов защиты персональных данных;
- продемонстрировать процесс работы с персональными данными в организации;
- научить разработке документов, регламентирующих работу с персональными данными в организации.

**1.3 Требования к предварительной подготовке обучающегося:**

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

- Современные технические средства охраны объектов
- Технологии обеспечения информационной безопасности
- Математическое моделирование технических объектов и систем управления
- Криптографические средства защиты информации

## 2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<b>ПК-3: Способен вводить в эксплуатацию и сопровождать системы защиты информации в организации</b>
<b>Знать:</b> типовые средства, методы и протоколы идентификации, аутентификации и авторизации; виды политик управления доступом и информационными потоками в компьютерных сетях
<b>Уметь:</b> администрировать системы защиты информации от несанкционированного доступа; проводить анализ структурных и функциональных схем защищенной автоматизированной системы
<b>Владеть:</b> навыками организации контроля состояния системы защиты информации; разработки организационно-распорядительные документы, определяющие мероприятия по защите информации в организации

## 3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа			СР (часы)	Инновац. формы занятий	Форма текущего контроля
		Лек. (часы)	Пр. (часы)	Лаб. (часы)			
Раздел 1. Нормативно - правовые основы дисциплины							
Тема 1. Информационная безопасность как компонент национальной безопасности государства.  Практическое занятие: Система государственного контроля и надзора за обеспечением безопасности персональных данных Лабораторная работа: Разбор и структуризация механизма защиты персональных данных на основании Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) "О персональных данных"	2	4	4	2	4		О

<p>Тема 2. Правовое обеспечение защиты персональных данных</p> <p>Практическое занятие: Разбор и структуризация нормативных документов:  Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;  Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;  Приказ ФСТЭК №21 от 18 февраля 2013 года «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;  Приказ ФСТЭК №17 от 11.02.2013 года «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;</p>		4	4		2,75	ИЛ	
<p>Тема 3. Основные права и обязанности оператора персональных данных</p> <p>Практическое занятие: Методология и алгоритм работы операторов персональных данных. Особенности организации защиты конфиденциальности.  Лабораторная работа: Оценка вреда, в случае нарушения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;</p>		2	4	2	4		
<p>Раздел 2. Введение. Основные понятия.</p>							
<p>Тема 4. Типы и классификация информационных систем персональных данных</p> <p>Практическое занятие: Определения уровня защищенности ИСПДн  Лабораторная работа: Законодательные требования к ИСПДн с разным уровнем защищенности</p>		4	2	2	2		
<p>Тема 5. Угрозы безопасности персональных данных</p> <p>Практическое занятие: Методика определения актуальных угроз безопасности персональных данных  Практическое занятие: Создание модели угроз ИСПДн  Лабораторная работа: Работа с банком данных угроз безопасности информации - ФСТЭК</p>		4	6	3	2	ИЛ	

<p>Тема 6. Обработка персональных данных без использования средств автоматизации</p> <p>Практическое занятие: Процесс неавтоматизированной обработки ПНД на основании Постановления Правительства от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;</p> <p>Лабораторная работа: Виды защищаемой информации. Разработка Инструкции по обработке персональных данных без использования средств автоматизации</p>	4	4	2	2		
<p>Раздел 3. Методология защиты персональных данных</p>						
<p>Тема 7. Построение защищенной информационной системы в соответствии с нормативами и требованиями. Защита информационных систем, обрабатывающих персональные данные</p> <p>Практическое занятие: Мероприятия по защите персональных данных при их обработке в информационных системах</p> <p>Лабораторная работа: Регламент определения уровня защищенности персональных данных</p>	4	4	2	2	ИЛ	
<p>Тема 8. Организационно - управленческие меры обеспечения защиты персональных данных на предприятии. Цели, задачи, методология и нормативное обеспечение разработки документов регламентирующих работу с персональными данными</p> <p>Практическое занятие: Состав, функции и области применения документального обеспечения деятельности оператора персональных данных.</p> <p>Лабораторная работа: Концепция информационной безопасности, структура, функции и области применения.</p>	4	2	2	2		0

<p>Тема 9. Организационно - технические меры обеспечения защиты персональных данных на предприятии.</p> <p>Практическое занятие: Настройка управление доступом к съемным носителям информации, механизмов замкнутой программной среды и контроля целостности</p> <p>Лабораторная работа: Выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и к возникновению угроз безопасности персональных данных</p>		4	4	2	2		
<p>Итого в семестре (на курсе для ЗАО)</p>	34	34	17	22,75			
<p>Консультации и промежуточная аттестация (Зачет)</p>		0,25					
<p>Раздел 4. Организация системы защиты персональных данных на предприятии</p>							
<p>Тема 10. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности.</p> <p>Практическое занятие: Подходы к аудиту и оценке защищенности информационных систем. Проведение внешнего аудита или внутреннего контроля обработки ПДн на предприятии</p> <p>Лабораторная работа: Регистрация событий безопасности. Разработка пакета локальной организационно-распорядительной документации.</p>	3	6	1	6	ИЛ		
<p>Тема 11. Особенности защиты персональных данных при их обработке в государственных информационных системах. Регуляторы в области защиты персональных данных. Проверки Роскомнадзора. Проверки ФСБ. Проверка ФСТЭК.</p> <p>Аттестация информационных систем персональных данных. Особенности проведения, функции и области применения.</p> <p>Практическое занятие: Методика проведения аттестации информационной системы по требованиям защиты персональных данных. Правовые обоснования проведения аттестации информационных систем персональных данных.</p> <p>Лабораторная работа: Этапы проведения аттестационных испытаний. Подготовка объекта к аттестации. Типовые формы документов. Методы обезличивания персональных данных.</p>	3	4	6	3	6,5	0	

Раздел 5. Управление информационной системой персональных данных						О
<p>Тема 12. Управление конфигурацией информационной системы и системы защиты персональных данных.</p> <p>Практическое занятие: Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа. Лабораторная работа: Идентификация по порогу, идентификация при помощи ранжирования. Понятие отрицательной аутентификации.</p>	2	6	3	8		
<p>Тема 13. Системы контроля, управления и разграничения доступа. Основные понятия о ключах, идентификаторах и блокирующих устройствах. Обзор средств криптографической защиты конфиденциальной информации.</p> <p>Практическое занятие: Основы электронной подписи. Взаимосвязь между протоколами аутентификации и электронной подписи. Схемы ЭП. Подготовка рабочего места к работе с электронной подписью. Выработка и проверка электронной подписи. Лабораторная работа: Защита информационной системы, обрабатывающей персональные данные. Установка и настройка совместной работы КриптоПро CSP, Rutoken, eToken</p>	4	4	4	5	ГД	
Раздел 6. Технические методы защиты персональных данных						
<p>Тема 14. Программная или программно-техническая защита от несанкционированного доступа к информационным ресурсам автоматизированных рабочих мест информационных систем персональных данных (ИСПДн);</p> <p>Практическое занятие: Классификация и области применения технических средств перекрытия технических каналов утечки информации. Лабораторная работа: Организация безопасного межсетевое взаимодействия при подключении ИСПДн к локальным сетям общего пользования или к сети Интернет, программное обеспечение для защиты персональных данных сетевыми экранами, программами: анти-спам, анти-шпион.</p>	2	6	4	8	ИЛ	Л

Тема 15. Защита биометрических персональных данных						
Практическое занятие: Обработка, хранение и защита биометрических персональных данных: требования к материальным носителям биометрических персональных данных Лабораторная работа: Организационные и технические меры безопасности при хранении персональных данных на носителях		2	6	2	8	
Итого в семестре (на курсе для ЗАО)		17	34	17	41,5	
Консультации и промежуточная аттестация (Экзамен)		10		24,5		
<b>Всего контактная работа и СР по дисциплине</b>		163,25		88,75		

#### 4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

#### 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

##### 5.1 Описание показателей, критериев и системы оценивания результатов обучения

##### 5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ПК-3	Перечисляет типовые средства, методы разграничения доступа и защиты конфиденциальной информации; На основе нормативной и технической документации анализирует структурные и функциональные связи защищенной автоматизированной системы Осуществляет организацию и мониторинг защищенности ИСПДн организации, формировать необходимые пакеты документов для обработки и защиты ПНд на предприятии	вопросы для устного собеседования и практико-ориентированные задания

##### 5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.	не предусмотрена
4 (хорошо)	Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.	не предусмотрена
3 (удовлетворительно)	Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов.	не предусмотрена



2 (неудовлетворительно)	<p>Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки.</p> <p>Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).</p>	не предусмотрена
Зачтено	<p>Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.</p>	не предусмотрена
Не зачтено	<p>Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки.</p> <p>Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).</p>	не предусмотрена

## 5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

### 5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
Семестр 2	
1	Правовые механизмы защиты информации на разных уровнях
2	Понятие тайны, секрета и конфиденциальности
3	Персональные данные
4	Информация, составляющая коммерческую тайну
5	Объекты информационной безопасности
6	Информационные системы и их классификация
7	Случайные и целенаправленные угрозы нарушения сохранности информации
8	Нормативные требования к сетям в ИСПДн.
9	Нормативные требования к сетям в ГИС.
10	Основные положения Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
11	Основные положения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»
12	Основные положения Приказа ФСТЭК №21 от 18 февраля 2013 года «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
13	Основные положения Приказа ФСТЭК №17 от 11.02.2013 года «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
Семестр 3	
14	Риски ИБ
15	Технические средства промышленного шпионажа
16	Классы безопасности
17	Аудит информационной безопасности
18	Политика безопасности администратора сети и брандмауэра
19	Цели интеграции межсетевых экранов
20	Методы и средства защиты информации в сетях.
21	Средства разграничения доступа к телекоммуникационному оборудованию.
22	Средства контроля доступа к среде передачи данных. Технология VLAN.

23	Протоколы и средства терминального доступа.
24	Назначение, принцип работы и классификация виртуальных частных сетей.
25	Назначение, принцип работы и классификация межсетевых экранов
26	Информационная безопасность. Основные определения. Стандарты
27	Электронная цифровая подпись.
28	Идентификация, аутентификация и авторизация.
29	Проблемы обеспечения безопасности операционных систем.
30	Системы хранения паролей
31	Системы обнаружения вторжений.

### 5.2.2 Типовые тестовые задания

не предусмотрены

### 5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Определите области применения Федерального закон от 27.07.2006 № 152-ФЗ «О персональных данных» и постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

2. Какие локальные распорядительные документы должны быть разработаны на предприятии ООО "Х" для защиты ПНД? (модельная задача)

3. Составить алгоритм обработки и защиты персональных данных на бизнес - мероприятии на 300 человек с 3-мя уровнями доступа.

4. Спроектируйте процесс аттестации ИСПДн предприятия ООО "Х", указав сроки, список нормативной и сопроводительной документации (модельная задача)

5. Распишите методологию работы с банком данных угроз информации ФСТЭК при составлении модели угроз ООО "Х"

### 5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

#### 5.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

#### 5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная

Письменная

Компьютерное тестирование

Иная

#### 5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Зачет. Студент допускается к зачету при предъявлении принятых отчетов по всем лабораторным работам. Зачет проводится в устной форме, студентам рандомно раздаются билет в которых есть теоретический вопрос и практико-ориентированное задание, время подготовки 20 мин, время ответа 5 мин

Экзамен. Студент вытягивает билет с двумя теоретическими вопросами и практико - ориентированным заданием, время подготовки 40 мин.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
<b>6.1.1 Основная учебная литература</b>				
Штеренберг С. И.	Защита информации в компьютерных системах	Санкт-Петербург: СПбГУПТД	2022	<a href="http://publish.sutd.ru/tp_ext_inf_publish.php?id=2022163">http://publish.sutd.ru/tp_ext_inf_publish.php?id=2022163</a>
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	<a href="https://www.iprbooks.hop.ru/87995.html">https://www.iprbooks.hop.ru/87995.html</a>
<b>6.1.2 Дополнительная учебная литература</b>				
Фомин, Д. В.	Защита информации: специализированные аттестованные программные и программно-аппаратные средства	Саратов: Вузовское образование	2021	<a href="http://www.iprbookshop.ru/110329.html">http://www.iprbookshop.ru/110329.html</a>

Никифоров, С. Н.	Защита информации. Защита от внешних вторжений	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	<a href="https://www.iprbooks.hop.ru/74381.html">https://www.iprbooks.hop.ru/74381.html</a>
Алексеев, А. П.	Многоуровневая защита информации	Самара: Поволжский государственный университет телекоммуникаций и информатики	2017	<a href="https://www.iprbooks.hop.ru/75387.html">https://www.iprbooks.hop.ru/75387.html</a>
Петренко, В. И., Мандрица, И. В.	Защита персональных данных в информационных системах	Ставрополь: Северо-Кавказский федеральный университет	2018	<a href="http://www.iprbookshop.ru/83198.html">http://www.iprbookshop.ru/83198.html</a>
Бахаров, Л. Е.	Информационная безопасность и защита информации (разделы криптография и стеганография)	Москва: Издательский Дом МИСиС	2019	<a href="https://www.iprbooks.hop.ru/98171.html">https://www.iprbooks.hop.ru/98171.html</a>

## 6.2 Перечень профессиональных баз данных и информационно-справочных систем

1. Информационно-справочная система «Консультант Плюс» [Электронный ресурс] // Режим доступа: <http://www.consultant.ru/>
2. Научная электронная библиотека [Электронный ресурс] // Режим доступа: <https://elibrary.ru/>
3. Справочно-правовая система «Гарант» [Электронный ресурс] // Режим доступа: <http://www.garant.ru/>
4. Электронная библиотека диссертаций [Электронный ресурс] // Режим доступа: <http://diss.rsl.ru/>
5. Официальный сайт ФСТЭК России [Электронный ресурс] // Режим доступа: <http://www.fstec.ru>
6. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс] // Режим доступа: <https://bdu.fstec.ru/>
7. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс] // Режим доступа: <https://reestrinform.ru/reestr-szi.html>
8. ГОСТ Эксперт - единая база ГОСТов Российской Федерации [Электронный ресурс] // Режим доступа: <https://gostexpert.ru/>

## 6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Office Professional  
Microsoft Windows

## 6.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория	Оснащение
Компьютерный класс	Специализированная мебель; компьютерная техника; наборы демонстрационного оборудования, служащие для представления учебной информации (стационарное мультимедийное оборудование) - мультимедийная проекционная система (мультимедиа проектор и экран). Рабочие станции, программно-аппаратные комплексы ЗИ; локальная вычислительная сеть с выходом в Интернет