

УТВЕРЖДАЮ

Первый проректор, проректор по  
УР

\_\_\_\_\_ А.Е. Рудин

«31» \_\_\_\_ 10 \_\_\_\_ 2023 года

## Рабочая программа дисциплины

**Б1.В.02**

Технологии обеспечения информационной безопасности

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.	Трудоё мкость, ЗЕТ	Форма промежуточной аттестации
	Лекции	Практ. занятия				
1	УП	34	17	58,5	34,5	Экзамен
	РПД	34	17	58,5	34,5	
Итого	УП	34	17	58,5	34,5	
	РПД	34	17	58,5	34,5	

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

Составитель (и):

кандидат технических наук, Доцент

\_\_\_\_\_

Егоров И.М.

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:** сформировать компетенции в области технологий обеспечения информационной безопасности

**1.2 Задачи дисциплины:**

- познакомить с требованиями информационной безопасности, их зависимостью от структуры объектов информатизации
- раскрыть методы концептуального проектирования технологий систем обеспечения информационной безопасности
- научить пользоваться методикой разработки технического проекта системы (подсистемы, либо компонента системы) обеспечения информационной безопасности
- способствовать освоению алгоритмов и методов выбора, и обоснований технологий обеспечения информационной безопасности объектов

**1.3 Требования к предварительной подготовке обучающегося:**

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

Дисциплина базируется на компетенциях, сформированных на предыдущем уровне образования

## 2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<b>ПК-4: Способен разрабатывать проектные решения по защите информации в автоматизированных системах</b>
<b>Знать:</b> принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов
<b>Уметь:</b> классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; определять типы субъектов доступа и объектов доступа, являющихся объектами защиты
<b>Владеть:</b> навыками разработки проектов нормативных документов, регламентирующих работу 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)			
Раздел 1. Обеспечение уровня безопасности предприятия	1					О
Тема 1. Основные понятия теории компьютерной информации. Понятие и сущность защиты информации. Место защиты информации в системе информационной безопасности РФ. Классификация информации ограниченного доступа Практическое занятие: Требования информационной безопасности, их зависимость от структуры объектов информатизации		8	2	10	ИЛ	
Тема 2. Специфика технологий обеспечения информационной безопасности объектов защиты. Практическое занятие: Методы анализа информационной системы для выбора технологий обеспечения и информационной безопасности объектов		4	2	8		

Раздел 2. Комплекс средств и технологий обеспечения информационной безопасности объектов защиты					
Тема 3. Требования к технологиям обеспечения информационной безопасности объектов защиты Практическое занятие: Классификация видов, методов и способов защиты информации. Назначение и структура систем защиты информации. Практическое занятие: Подсистемы комплексной системы защиты информации	6	4	10		О
Тема 4. Современные технологии защиты объектов информатизации. Объекты защиты информации. Практическое занятие: Каналы утечки информации и методы несанкционированного доступа к конфиденциальной информации. Практическое занятие: Подбор и обоснование технологий обеспечения информационной безопасности в зависимости от характера объекта информатизации.	6	5	10,5	ИЛ	
Раздел 3. Проектные решения в области обеспечения информационной безопасности объектов информатизации					
Тема 5. Информационно-коммуникационные технологии для выявления и анализа фундаментальных и прикладных проблем информационной безопасности Практическое занятие: Технологии формирования алгоритмов обработки информации.	4	2	10	ГД	О
Тема 6. Технологии для формирования проектных решений по защите объектов информатизации Практическое занятие: План защиты информации на предприятии	6	2	10		
Итого в семестре (на курсе для ЗАО)	34	17	58,5		
Консультации и промежуточная аттестация (Экзамен)	10		24,5		
<b>Всего контактная работа и СР по дисциплине</b>	61		83		

#### 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-4	Перечисляет основные подсистемы, описывает элементы и возможные связи внутри корпоративных систем защиты информации. Классифицирует информацию по уровню ее конфиденциальности, целостности и доступности. Составляет алгоритм разработки регламентирующих документов для конкретной системы защиты информации	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

### 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 1	
1	Основные понятия информационной безопасности.
2	Информационные технологии и необходимость информационной безопасности
3	Информационная безопасность предпринимательской деятельности.
4	Система защиты информации и ее структуры.
5	Организационно-правовой статус службы безопасности.
6	Методы и средства защиты информации.
7	Фрагментарный и системный подход к защите информации.
8	Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
9	Персональные данные и их защита.
10	Информационные угрозы, их виды и причины возникновения.
11	Действия и события, нарушающие информационную безопасность.
12	Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13	Основные угрозы безопасности информации и информационной инфраструктуры. Методы противодействия этим угрозам
14	Организационная основа и основные направления деятельности системы защиты информации
15	Классификация информации в зависимости от категории доступа и порядка ее предоставления.
16	Основные стадии создания систем защиты информации, основные элементы проектных решений.
17	Основные методы защиты информации
18	Основные требования по обеспечению уровней защищенности персональных данных при их обработке в информационных системах.
19	Актуальные угрозы безопасности конфиденциальной информации. Типы угроз.
20	Факторы, влияющие на инциденты информационной безопасности, анализ условий их возникновения (угрозы, уязвимости, ущерб, риск, каналы утечки).

21	Порядок формирования перечня сведений, отнесенных к коммерческой тайне, уровни коммерческой ценности. Общие подходы к категорированию объектов. Категория важности
22	Права и обязанности работодателя и работника по сохранению коммерческой тайны

### 5.2.2 Типовые тестовые задания

не предусмотрены

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

Задача 1:

1. Запустить Wireshark.
2. Организовать чат между двумя компьютерами с помощью утилит netcat/nc/ncat. Передать несколько сообщений друг другу.
3. Найти пакеты с сообщениями в Wireshark.

Задача 2:

1. С помощью nmap просканировать машину Metasploitable 2 или 3 с определением версий сервисов.
2. Найти уязвимый сервис, определить список его уязвимостей по базам.
3. Подобрать эксплойт и с помощью него получить доступ к машине.

Требования к сдаче: эксплойты/сервисы должны отличаться у разных студентов. Студент должен знать за что отвечает и как работает сервис, а также примерный принцип работы эксплойта.

## 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

На экзамене обучающийся тянет билет с двумя теоретическими вопросами и одним практико-ориентированным заданием время подготовки - 40 минут. Ответ - не более 10 минут.

## 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>				
Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства	Саратов: Вузовское образование	2018	<a href="http://www.iprbookshop.ru/77317.html">http://www.iprbookshop.ru/77317.html</a>
Ревнивых, А. В.	Информационная безопасность организаций	Москва: Ай Пи Ар Медиа	2021	<a href="https://www.iprbookshop.ru/108227.html">https://www.iprbookshop.ru/108227.html</a>
<b>6.1.2 Дополнительная учебная литература</b>				
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	<a href="http://www.iprbookshop.ru/87995.html">http://www.iprbookshop.ru/87995.html</a>
Куликов, С. С.	Информационная безопасность локальных компьютерных сетей	Воронеж: Воронежский государственный технический университет, ЭБС АСВ	2021	<a href="https://www.iprbookshop.ru/118614.html">https://www.iprbookshop.ru/118614.html</a>

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

Электронная база данных «Scopus» (<http://www.scopus.com>);  
 Научная электронная библиотека eLibrary (<http://elibrary.ru>).

### 6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

Python

### 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, система «Шепот». Многофункциональный поисковый прибор ST 031M "Пиранья". СЗИ НСД «Аккорд-АМДЗ». Универсальный досмотровый набор.