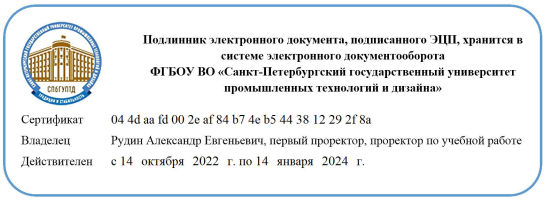
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)


Подлинник электронного документа, подписанного ЭЦП, хранится в системе электронного документооборота
ФГБОУ ВО «Санкт-Петербургский государственный университет промышленных технологий и дизайна»
Сертификат 04 4d aa fd 00 2e af 84 b7 4e b5 44 38 12 29 2f 8a
Владелец Рудин Александр Евгеньевич, первый проректор, проректор по учебной работе
Действителен с 14 октября 2022 г. по 14 января 2024 г.

УТВЕРЖДАЮ
Первый проректор, проректор по УР
_____А.Е. Рудин
«31»___10___ 2023 года

Рабочая программа дисциплины

Б1.В.ДВ.03.02 Методы защиты информации от несанкционированного доступа

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: (специализация) Проектирование систем защиты информации на предприятии

Уровень образования: магистратура

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся			Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия	Лаб. занятия				
4	УП	33	22	22	30,75	0,25	3	Зачет
	РПД	33	22	22	30,75	0,25	3	
Итого	УП	33	22	22	30,75	0,25	3	
	РПД	33	22	22	30,75	0,25	3	

Санкт-Петербург
2023

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	_____	Чалова Е.И.
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 персональных данных, принципов работы с ними и методов их защиты.

1.2 Задачи дисциплины:

– раскрыть теоретические, практические и методические вопросы обеспечения информационной безопасности;

– раскрыть методы защиты информации от несанкционированного доступа;

– 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:

Защищенные информационные системы

Информационно-аналитические системы безопасности

Криптографические средства защиты информации

Защита электронного документооборота

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3: Способен вводить в эксплуатацию и сопровождать системы защиты информации в организации
Знать: способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах
Уметь: применять методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее; проводить контроль (мониторинг) состояния системы защиты информации
Владеть: навыком разработки и реализация организационных мер, обеспечивающих эффективность системы защиты информации; навыками руководства разработкой предложений по совершенствованию организационных и технических мероприятий по технической защите информации и оценке их эффективности, совершенствованию системы технической защиты 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. Ведение. Основные понятия и термины	4						О
Тема 1. Понятие, угрозы, способы и причины несанкционированного доступа к информации Практическое занятие: Методы социальной инженерии и их значение для систем защиты информации Лабораторная работа: Инсайдерская информация, классификация, признаки, методы перехвата.		2	2	2	2		

Тема 2. Организационные методы защиты от НСД. Основные методы, силы и средства , используемые для организации защиты информации от несанкционированного доступа на предприятии. Модели нарушителя и угроз. Практическое занятие: Защита от угрозы нарушения конфиденциальности на уровне содержания информации Лабораторная работа: Субъектно-объектная модель компьютерной системы. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.		4	3	2	4	ИЛ	
Тема 3. Инженерно-технические методы реализации основных требований и построению системы информационной безопасности Практическое занятие: Основные направления и цели использования криптографических методов Лабораторная работа: Построение систем защиты от угрозы утечки по техническим каналам		4	2	2	4		
Раздел 2. Управление доступом							
Тема 4. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах Практическое занятие: Дискреционные модели распространения прав доступа. Модель и теоремы безопасности Харрисона-Руззо-Ульмана. Лабораторная работа: Модель типизованной матрицы доступа		3	2	2	2		О
Тема 5. Определение и содержание политики безопасности для компьютерных систем Практическое занятие: Модель take-grant. Мандатная политика безопасности. Модель Белле-ЛаПадулы. Практическое занятие: Ролевая политика безопасности. Реализация политики безопасности		4	3		4	ИЛ	

Тема 6. Системы аутентификации пользователей компьютерных систем и методы их построения. Элементы, проблемы создания и использования систем аутентификации Практическое занятие: Протоколы аутентификации. Типовые шаблоны систем аутентификации. Сравнение типовых шаблонов аутентификации. Лабораторная работа: Методы защиты в системах локальной аутентификации. Использование многоразовых паролей. Лабораторная работа: Комплект протоколов IP-Security (IP-Sec) Лабораторная работа: Стандарт сетевой аутентификации IEEE 802.1x 18		2	2	6	4,75		
Тема 7. Построение политики информационной безопасности пакетной мультисервисной сети Практическое занятие: Общие требования построения защищенной пакетной мультисервисной сети. Требования к подсистеме обеспечения безопасности сетевого взаимодействия. Лабораторная работа: Мультисервисные сети на технологиях IP-QoS и их основные функциональные элементы. Определение основных приоритетов информационной безопасности.		2	2	2	4		
Раздел 3. Технические методы защиты информации от несанкционированного доступа							Л
Тема 8. Аппаратно-программные средства защиты информации от несанкционированного использования Практическое занятие: Технические решения по защите от НСД межсетевого взаимодействия и передачи информации. Лабораторная работа: Общее описание стека протоколов защиты межсетевого уровняIPsec (Internet Protocol Security). Протокол обмена ключевой информацией IKE (Internet Key Exchange).		4	2	2	2		
Тема 9. Понятие и разновидности скрытых каналов утечки информации в компьютерных системах, теоретико-вероятностные основы их выявления и нейтрализации (автоматная модель Гогена -Мессигера). Практическое занятие: Построение систем защиты от угрозы отказа доступа к информации Лабораторная работа: Меры и средства защиты операционной системы от утечки информации по техническим каналам		4	2	2	2		

Тема 10. Требования к подсистемам криптографической защиты информации и антивирусной защиты Практическое занятие: Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Правила защиты от компьютерных вирусов. Лабораторная работа: Характеристика путей проникновения вирусов в компьютеры. Настройка антивирусной защиты локальной сети		4	2	2	2		
Итого в семестре (на курсе для ЗАО)		33	22	22	30,75		
Консультации и промежуточная аттестация (Зачет)		0,25					
Всего контактная работа и СР по дисциплине		77,25			30,75		

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 и классифицирует как методы несанкционированного доступа, так и средства защиты от него. Осуществляет мониторинг системы на наличие уязвимостей типовыми методами и средствами. Проводит контрольные проверки эффективности средств защиты информации от несанкционированного доступа Предлагает проектные решения по защите информации от несанкционированного доступа	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
Зачтено	Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.	не предусмотрена
Не зачтено	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).	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 4	
1	Основные требования и рекомендации по защите служебной тайны и персональных данных.
2	Каковы способы контроля целостности потока сообщений?

3	Классификация технических каналов утечки информации.
4	Маршрутизация, фильтрация и ограничение вещания. Защита системной инфратруктуры.
5	Основные показатели технического канала утечки информации
6	Классификация функциональных требований безопасности. Классы функциональных требований, описывающие элементарные сервисы безопасности.
7	Классы функциональных требований, описывающие производные сервисы безопасности.
8	Основные понятия и классификация требований доверия безопасности.
9	Оценка профилей защиты и заданий по безопасности.
10	Оценочные уровни доверия безопасности
11	Биометрическая идентификация и аутентификация.
12	Требования к произвольному (дискреционному) управлению доступом.
13	Требования к принудительному (мандатному) управлению доступом.
14	Ролевое управление доступом.
15	Межсетевое экранирование.
16	Системы активного аудита.
17	Анонимизаторы.
18	Выпуск и управление сертификатами.
19	Виртуальные частные сети. Виртуальные локальные сети.
20	Регуляторы безопасности и реализуемые ими цели.
21	Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами
22	Общие принципы выработки официальной политики предприятия в области информационной безопасности.

5.2.2 Типовые тестовые задания

не предусмотрены

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Активировать/ дезактивировать компонент защиты информации Secret Net Studio.
2. Настроить политики аутентификации пользователей в Secret Net Studio.
3. Настроить иерархические уровни конфиденциальности системы мандатного управления доступом в Secret Net Studio.
4. Назначить пользователю привилегии (уровень допуска) системы мандатного управления доступом в Secret Net Studio.
5. Назначить объекту файловой системы метку конфиденциальности системы мандатного управления доступом в Secret Net Studio.
6. Назначить пользователю привилегии (уровень допуска) системы мандатного управления доступом в ОС Astra Linux SE.
7. Настроить парольную политику в ОС Astra Linux SE.
8. Настроить парольную политику в Dallas Lock.

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

Обучающийся тянет билет с практико - ориентированным заданием и теоретическим вопросом, время подготовки - 15 мин, время ответа - 5 мин

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Жук А.П., Жук Е.П., Лепешкин О.М. и др.	Защита информации	Москва: ИЦ РИО	2021	https://ibooks.ru/reading.php?short=1&productid=361250
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	http://www.iprbookshop.ru/87995.html
6.1.2 Дополнительная учебная литература				
Никифоров, С. Н., Ромаданов, М. М.	Защита информации. Пароли, скрытие, удаление данных	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	http://www.iprbookshop.ru/80747.html
Никифоров, С. Н.	Защита информации. Защищенные сети	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	http://www.iprbookshop.ru/74382.html

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

MicrosoftOfficeProfessional

Microsoft Windows

DosBox

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.