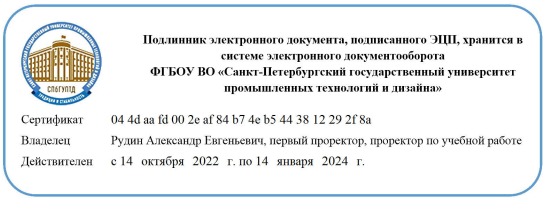
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)


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.05 Проектирование систем комплексной 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: (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				
3	УП	17	34	56,75	0,25	3	Зачет
	РПД	17	34	56,75	0,25	3	
4	УП	22	22	65,5	34,5	4	Экзамен
	РПД	22	22	65,5	34,5	4	
Итого	УП	39	56	122,25	34,75	7	
	РПД	39	56	122,25	34,75	7	

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):

доктор технических наук, Профессор	_____	Макаров А.Г.
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 обучающихся в области проектирования систем комплексной безопасности, в области ее организации и управления

1.2 Задачи дисциплины:

- познакомить с определением принципов и этапов разработки КСЗИ;
- познакомить с технологией установления состава защищаемой информации и объектов защиты;
- научить использованию методов оценки уязвимости защищаемой информации;
- научить верно определять параметры и структуры КСЗИ;
- раскрыть состав мероприятий по обеспечению функционирования КСЗИ;
- раскрыть структуру и методы управления КСЗИ;
- научить определять показатели эффективности КСЗИ и методикам ее оценки.

1.3 Требования к предварительной подготовке обучающегося:

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

Организационно-правовые механизмы обеспечения информационной безопасности

Управление проектами

Математическое моделирование технических объектов и систем управления

Управление информационной безопасностью

Технологии обеспечения информационной безопасности

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3: Способен вводить в эксплуатацию и сопровождать системы защиты информации в организации
Знать: стандарты ЕСКД, ЕСТД и ЕСПД; порядок создания автоматизированных систем в защищенном исполнении
Уметь: осуществлять ввод системы защиты информации в эксплуатацию, организовать выполнение работ по техническому обслуживанию и устранению неисправностей технических и программно-технических средств защиты информации входящих в состав системы защиты информации организации
Владеть: навыками разработки организационно-распорядительных документов, определяющих 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)			
Раздел 1. Основные положения проектирования систем комплексной безопасности	3					О
Тема 1. Разработка концепции системы обеспечения информационной безопасности, определение объектов защиты. Практическое занятие: Этапы построения систем информационной безопасности на предприятии. Предпроектное обследование, техническое задание		2	4	8	ИЛ	
Тема 2. Принципы и методология разработки и внедрения комплексной системы защиты информации на предприятии. Практическое занятие: Определение состава и связей объектов защиты. Классификация информации по видам тайны и степеням конфиденциальности. Техническое проектирование,		2	4	8		

Раздел 2. Нормативные документы применяемые при проектировании систем комплексной безопасности						
Тема 3. Нормативная база Российской Федерации по защищенным информационным системам Практическое занятие: Оценка безопасности информационных технологий на основе «Общих критериев». Стандарт ISO 15408		2	4	6,75		О
Тема 4. Виды и типы нормативно - распорядительных документов применяемых для организации и управления системой комплексной безопасности предприятия Практическое занятие: Разработка инструкции по организации и управлению системой безопасности предприятия		1	2	6		
Раздел 3. Стандарты применяемые при проектировании систем комплексной безопасности						О
Тема 5. Стандарты информационной безопасности. Гармонизированные критерии европейских стран ITSEC. Германский стандарт BSI.Стандарт «Критерии оценки доверенных компьютерных систем» («Оранжевая книга»). Стандарт COBIT. Британский стандарт BS 7799 Практическое занятие: Создание протокола оценки безопасности автоматизированной системы на основе изученных стандартов. Структуризация нормативной информации		4	4	6	ИЛ	
Тема 6. Международный стандарт управления информационной безопасностью ISO 17799 Практическое занятие: Стандарт ISO 17799. Организационные меры по обеспечению информационной безопасности. Классификация ресурсов и их контроль		2	4	6	ГД	
Раздел 4. Методика проектирования систем комплексной безопасности						
Тема 7. Моделирование как инструментарий проектирования Практическое занятие: Моделирование угроз безопасности Практическое занятие: Выявление каналов утечки и методов несанкционированного воздействия на информацию		2	8	8		О

Тема 8. Анализ угроз и уязвимостей объекта информатизации Практическое занятие: Формирование требований защищенности объекта информатизации		2	4	8		
Итого в семестре (на курсе для ЗАО)		17	34	56,75		
Консультации и промежуточная аттестация (Зачет)		0,25				
Раздел 5. Технические особенности проектирования систем комплексной безопасности	4					О
Тема 9. Технологическое и организационной построение системы комплексной безопасности Практическое занятие: Кадровое и материально - техническое обеспечение защиты информации. Политика системы управления информационной безопасностью		4	4	11,5	ИЛ	
Тема 10. Программно-аппаратные комплексы для создания защищенных информационных систем Практическое занятие: Полномочное управление доступом. Контроль целостности и замкнутая программная среда. Дискретное управление доступом. Защита сетевой инфраструктуры		4	4	12		
Тема 11. Методика и принципы комплексного анализа и оценки угроз, уязвимостей и существующих мер защиты информации Практическое занятие: Алгоритм подбора необходимых мер и средств защиты на основе проведенного анализа. Моделирование процессов защиты информации.		4	4	12		
Раздел 6. Внедрение и аудит и системы комплексной безопасности						О
Тема 12. Состав компонентов комплексной системы обеспечения информационной безопасности, функциональные и обеспечивающие подсистемы, технология, управление. Практическое занятие: Формирование и оценка эффективности комплексного проекта мер обеспечения защищенности объекта информатизации		4	4	10	ИЛ	
Тема 13. Нормативно -правовая база в области аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ) в Российской Федерации Практическое занятие: Аудит информационной безопасности и методы его проведения. Анализ и управление рисками информационной безопасности.		4	4	10		

Тема 14. Порядок внедрения разработанных процессов системы управления информационной безопасностью и мер по обеспечению информационной безопасности Практическое занятие: Аттестация объектов информатизации.		2	2	10		
Итого в семестре (на курсе для ЗАО)		22	22	65,5		
Консультации и промежуточная аттестация (Экзамен)		10		24,5		
Всего контактная работа и СР по дисциплине		105,25		146,75		

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 основные положения стандартов безопасности. Формулирует алгоритм проектирования и внедрения систем комплексной безопасности. Осуществляет мониторинг процессов установки и внедрения технических и программно-технических средств защиты информации, входящих в состав системы защиты информации организации. Прописывает инструкции по организации управления информационной безопасности организации.	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)	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
Зачтено	Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Могут присутствовать 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 3	
1	С какого этапа необходимо начинать разработку системы информационной безопасности? Какие мероприятия могут быть заложены на данном этапе?
2	Особенности доступа к конфиденциальной документированной информации, составляющей персональные данные?
3	Основные виды угроз информационной безопасности организации?
4	Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе?
5	Что включает в себя комплексная система информационной безопасности?
6	Перечислите план мероприятий (задач), которые необходимо реализовать для защиты коммерческой тайны согласно N98 ФЗ «О коммерческой тайне»?
7	Приведите примеры стадий проектирования системы информационной безопасности.
8	Как определить необходимый набор требования по защите информации для ИСПДн?
9	Дайте определение технического задания на создание системы.
10	Из каких основных подсистем строится система защиты информации в автоматизированной системе?
11	Действующие стандарты в области информационной безопасности. Содержание и основные позиции.
12	Документационное сопровождение комплексной системы защиты информации (КСЗИ).
13	Направления работ по созданию КСЗИ. Аспекты планирования инженерно-технического обеспечения КСЗИ.
14	Этапы работ по созданию КСЗИ. Определение и анализ объектов защиты. Базовые понятия и элементы.
15	Определение и анализ объектов защиты. Определение исходного уровня защищенности.
16	Классификация защищенности АС в соответствии с РД. Основные требования.
17	Модель угроз и принцип ее формирования. Базовая модель угроз безопасности персональных данных (ФСТЭК).
18	Модель угроз и принцип ее формирования. Методология формирования модели угроз в соответствии с рекомендациями ФСБ.
Семестр 4	
19	Что такое аттестация объектов информатизации? Эта процедура обязательный или добровольная?

20	Какие структурно-функциональные характеристики определяются в ходе анализа необходимости обеспечения защиты объекта?
21	Приведите примеры организационных мер защиты информации, принимаемых при разработке и реализации проектов в сфере информационной безопасности.
22	Сформулируйте причину(ы) привлечения к процессу анализа информационных рисков при автоматизированной обработке информации специалистов из различных подразделений компании?
23	Основные требования к разрешительной системе доступа?
24	Что относится к организационным мерам защиты информации?
25	Раскройте понятие «аудит информационной безопасности».
26	Приведите примеры управленческих (организационных) мер защиты информации в автоматизированных системах.
27	Какие методы аутентификации можно применять при защите АС?
28	В чем заключается дискреционный метод разграничения доступа?
29	Перечислите методы разграничения доступа в автоматизированных системах.
30	Что такое политика информационной безопасности автоматизированной системы?
31	Сформулируйте цель обеспечения безопасности автоматизированной системы
32	Приведите примеры преднамеренных угроз информационной безопасности КСЗИ
33	Приведите примеры непреднамеренных угроз информационной безопасности КСЗИ
34	Оценка угроз ИБ. Выявление способов НСД и каналов утечки информации.
35	Объективные и субъективные факторы, воздействующие на информацию (по ГОСТ).
36	Виды угроз и основные последствия их реализации. Понятие «нарушителя» и модели нарушителя. Классификации.
37	Методики оценки рисков. Применяемые на практике подходы.
38	Структура процесса управления рисками.
39	Оценка эффективности КСЗИ. Общая характеристика применяемых методов.
40	Контроль мероприятий КСЗИ. Основные аспекты.
41	Средства защиты информации и механизмы обеспечения безопасности информации. Идентификация и аутентификация.
42	Средства защиты информации и механизмы обеспечения безопасности информации. Разграничение доступа. Регистрация и аудит.
43	Средства защиты информации и механизмы обеспечения безопасности информации. Криптографическая подсистема.
44	Средства защиты информации и механизмы обеспечения безопасности информации. Межсетевое экранирование.
45	Планирование мероприятий КСЗИ.

5.2.2 Типовые тестовые задания

не предусмотрены

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Аттестация автоматизированной системы предприятия ООО "Х" (модельная задача).
2. Классификация угроз безопасности системы предприятия ООО "Х" (модельная задача).
3. Описание процесса оценки угроз системы комплексной безопасности с указанием регламентирующей документации организации

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: Обучающийся тянет билет, в котором теоретический вопрос и практическое задание. После этого готовится в течении как минимум 20 минут с использованием конспекта лекций. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. После ответа на теоретический вопрос обучающийся приступает к решению практического задания, при необходимости отвечает на дополнительные вопросы преподавателя.

Экзамен: Обучающийся тянет билет, в котором два теоретических вопроса и практическое задание. После этого готовится в течении как минимум 20 минут. Обучающийся в устной форме доводит до преподавателя ответы на вопросы, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. После ответа на теоретические вопросы обучающийся приступает к решению практического задания (время подготовки 20 минут), при необходимости отвечает на дополнительные вопросы преподавателя.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Сычев, Ю. Н.	Стандарты информационной безопасности. Защита и обработка конфиденциальных документов	Саратов: Вузовское образование	2018	http://www.iprbookshop.ru/72345.html
Газизов, А. Р., Петренкова, С. Б., Фатхи, Д. В.	Управление информационной безопасностью	Ростов-на-Дону: Донской государственный технический университет	2019	https://www.iprbookshop.ru/117771.html
Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах	Москва: Форум	2020	https://ibooks.ru/reading.php?short=1&productid=361312
6.1.2 Дополнительная учебная литература				
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	http://www.iprbookshop.ru/87995.html
Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей	Москва: Форум	2021	https://ibooks.ru/reading.php?short=1&productid=361273

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/

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

1С-Битрикс: Внутренний портал учебного заведения

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.