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 01 51 53 c3 00 f5 b0 ab be 4e a6 e7 63 84 98 d0 69
Владелец Рудин Александр Евгеньевич, первый проректор, проректор по учебной работе
Действителен с 12 января 2024 г. по 12 апреля 2025 г.

УТВЕРЖДАЮ
Первый проректор, проректор по УР
_____А.Е. Рудин

Рабочая программа дисциплины

Б1.О.10 Защищенные информационные системы

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				
3	УП	17	34	17	41,5	34,5	4	Экзамен
	РПД	17	34	17	41,5	34,5	4	
Итого	УП	17	34	17	41,5	34,5	4	
	РПД	17	34	17	41,5	34,5	4	

Санкт-Петербург
2024

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 Екатерина Игорьевна
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 разработки, проектирования, наладки и мониторинга защищенных информационных систем, обучить их принципам и методам защиты информации, обслуживания и анализа защищенных автоматизированных систем, а также содействовать формированию научного мировоззрения и развитию системного мышления.

1.2 Задачи дисциплины:

- раскрыть методики анализа угроз при разработке и эксплуатации защищенных информационных систем;
- раскрыть: методики оценки рисков ИБ на объекте информатизации, концептуального проектирования защищенных систем обработки информации, требований к уровню и средствам защиты информации в ИС на основе

отечественных и международных стандартов;

- сформировать знания и навыки по технологиям обеспечения защиты информации в информационных системах (в т.ч. ЗИС)

1.3 Требования к предварительной подготовке обучающегося:

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

Математическое моделирование технических объектов и систем управления

Организационно-правовые механизмы обеспечения информационной безопасности

Организация и управление исследованиями

Технологии обеспечения информационной безопасности

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-2: Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности
Знать: области применения, основные принципы работы защищенных информационных систем, современные научные проблемы и задачи в области автоматизированных систем
Уметь: оценивать уровень защищенности информационной системы на основе статистических данных и моделировании
Владеть: навыками составления отчета о защищенности информационной системы от несанкционированного доступа

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. Теоретические вопросы защиты информации и построения информационных систем	3						К
Тема 1. Основы теории надежности. Связь с основными задачами информационной безопасности. Практическое занятие: Надежность программно-аппаратных реализаций информационных систем Лабораторная работа "Защищенная web- ориентированная информационная система"		2	2	4	5		
Тема 2. Автоматизированная информационная система. Классификации задач, решаемых с использованием информационных систем. Свойства систем. Классификации систем. Ранги систем. Практическое занятие: Закон необходимости разнообразия (закон Эшби).		2	2		4	ИЛ	

Тема 3. Подходы к проектированию и реализации информационных систем. Жизненный цикл информационной системы. Практическое занятие: Вопросы информационной безопасности и аспекты построения защищенных систем.		4	6		4		
Раздел 2. Способы и методы защиты информации в информационных системах.							
Тема 4. Типология распределенных информационных систем. Процессы в информационных системах. Практическое занятие: Методы и способы, тенденции и подходы к защите информации в информационных системах. Лабораторная работа "Пен-тест защищенной web-ориентированной системы"		2	2	2	5,5	ГД	
Тема 5. Методы и способы обеспечения идентификации, аутентификации и авторизации в информационных системах. Практическое занятие: Криптографическая защита информации. Понятие несанкционированного доступа и принципы защиты от несанкционированного доступа. Мониторинг и аудит в информационных системах. Лабораторная работа "Защищенная система архитектуры Клиент-Сервер"		2	4	2	6		Л
Тема 6. Стандарты и нормативные документы в области информационной безопасности. Построение защищенной информационной системы в соответствии с нормативами и требованиями. Практическое занятие: Защита информационных систем, обрабатывающих персональные данные. Государственные информационные системы. Лабораторная работа "Пен-тест защищенной системы архитектуры Клиент- Сервер"		2	4	2	6		
Тема 7. Подходы к аудиту и оценке защищенности информационных систем. Практическое занятие: Мониторинг и оценка защищенности информационных систем Лабораторная работа "Защита информационной системы, обрабатывающей персональные данные"			4	3	4		

Раздел 3. Установка и сопровождение функционирования средств защиты информации в защищенных информационных системах							
Тема 8. Особенности использования специализированного прикладного программного обеспечения защищенных информационных систем Практическое занятие: Методики обеспечения информационной безопасности информационной системы Лабораторная работа "Настройка и применение системы защиты информации Secret Net Studio"		2	2	2	4	ИЛ	О
Тема 9. Особенности построения и применения операционных систем на базе ядра Linux Практическое занятие: Исследование файловых объектов с правами пользователя		1	4				
Тема 10. Исследование процессов в ОС Linux Практическое занятие:Монтирование файловых систем Лабораторная работа"Исследование сетевых возможностей ОС Linux"			4	2	3		
Итого в семестре (на курсе для ЗАО)		17	34	17	41,5		
Консультации и промежуточная аттестация (Экзамен)			10		24,5		
Всего контактная работа и СР по дисциплине			78		66		

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
ОПК-2	Обучающийся излагает основные принципы работы защищенных информационных систем, современных научных проблемах и задачах в области автоматизированных систем Реализует алгоритмы оценки уровня защищенности информационной системы на основе статистических данных и моделировании Составляет отчет о защищенности информационной системы от несанкционированного доступа в соответствии с нормативными документами и учитывая специфику предприятия	вопросы для устного собеседования и практик-ориентированные задания

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания. Студент без затруднений ответил на все дополнительные вопросы.	не предусмотрено

4 (хорошо)	студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.	не предусмотрено
3 (удовлетворительно)	при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос	не предусмотрено
2 (неудовлетворительно)	если студент отказался от ответа или не смог ответить на вопросы билета, ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний.	не предусмотрено

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	Угрозы и риски информационной безопасности, связанные с использованием информационных
2	Понятие защищенной информационной системы. Области применения защищенных ИС. Примеры защищенных ИС.
3	Методы хранения данных при реализации ЗИС. СУБД для организации защищенных ИС. Встроенные инструменты защиты данных в СУБД (с учетом модели организации данных).
4	Штатные и добавленные средства и способы программной реализации защиты информации (на конкретных примерах).
5	Методологии проектирования ИС. Принципы проектирования и разработки ЗИС.
6	Этапы проектирования и создания защищенной информационной системы.
7	Этапы создания системы защиты информационной системы.
8	Стандарты и нормативные документы, регламентирующие создание АС в защищенном исполнении
9	Стандарты и нормативные документы, регламентирующие построение системы защиты для информационной системы
10	Возможные уязвимости информационной безопасности для ИС и меры по их снижению, реализуемые на этапе разработки ИС.
11	Требования нормативных документов ФСТЭК, ФСБ и др. отечественных регуляторов к уровню защищенности информационных систем различных классов (на конкретных примерах классов ИС).
12	Классификация информационных систем. Нормативные документы, порядок определения класса защищенности ИС.
13	Программно-аппаратные средства защиты информации. Проблема интеграция средств защиты и компонентов информационных систем при проектировании СЗИ ИС (или ЗИС).
14	Роль специалиста по информационной безопасности в разработке, модернизации, внедрении ИС, в т.ч. защищенных ИС.
15	Этапы разработки информационных систем. Язык нотаций UML и виды диаграмм и моделей, используемые для проектирования ИС
16	Сценирование (описание сценариев) актуальных угроз ИБ, согласно методике ФСТЭК: исходные данные для сценирования, элементы сценария угроз, инструменты для описания сценария.
17	Методологии моделирования критических информационных/рабочих процессов (idef0, dfd, idef3, bpmn, flow chart и др.). Входные и выданные данные для построения модели
18	Задачи обеспечения ИБ, угрозы ИБ, источники уязвимостей ИС. Способы, средства выявления и оценки уязвимостей ИС.
19	Требования к уровню защищенности ИС и обрабатываемой в них информации, в зависимости от уровня конфиденциальности и критичности информации.

20	Меры и подходы к обеспечению защищенности ИС на этапах разработки.
21	Проектирование СЗИ для ИС (этапы). Технические средства защиты информации в ИС
22	ГИС и требования ФСТЭК и ФСБ к их уровню защищенности
23	ИСПДн и требования ФСТЭК и ФСБ к их уровню защищенности
24	АИС, АСУ и требования ФСТЭК и ФСБ к их уровню защищенности
25	ИС реального времени и требования к надежности таких ИС.
26	Особенности построения СЗИ для обработки ИСПДн
27	Угрозы для ИСПДн. Нормативные документы регуляторов в области требований к обеспечению защищенности ПДн..
28	Особенности построения СЗИ для обработки ГИС
29	Особенности построения СЗИ для обработки информации, содержащей коммерческую и служебную тайны.
30	Особенности построения СЗИ для обработки информации, содержащей государственную тайну.
31	Принципы организации документирования разработки, процесса сопровождения программного обеспечения
32	Функциональные возможности современных систем управления базами данных в части средств защиты. Архитектура, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных. Основные модели данных, модели представления знаний и программные средства работы с ними. Инфологическая модель предметной области.
33	Проектирование, документирование, разработке, тестирование и отладка компонентов обеспечивающей части ИАС при разработке ЗИС/ЗАС. Принципы организации документирования разработки, процесса сопровождения программного обеспечения.
34	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Обоснование необходимости использования криптографических средств защиты информации.
35	Эксплуатация ЗИС: администрирование ЗИС. Доступ к данным безопасности. Монитор безопасности, протоколирование, аудит, шифрование, контроль целостности данных, использование электронной цифровой подписи.

5.2.2 Типовые тестовые задания

не предусмотренны

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

Подготовка отчетов по итогу проведения лекционных и практических занятий (по разделам) на темы:

1. Классификация угроз безопасности. Этапы создания модели угроз
2. Классификации уязвимостей системы
3. Модель нарушителя
4. Классификация нарушителей в соответствии с документами регуляторов.
5. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей
6. Нетехнические меры защиты от внутренних угроз.
7. Криптографическая защита информации. Требования к шифрованию.
8. Требования к аутентификации в ИС. Аутентификация по IP-адресу.
9. Информационные системы: содержание термина, определения ИС в ГОСТах, Приказах («Требованиях …», и др. нормативных документах) регуляторов в области ИБ.
10. Представление о защищенных ИС: определение, виды, требования к ЗИС, связанные с защищенностью).
11. Отличия ЗИС от ОИС. Области и специфика применения защищенных ИС (цели, задачи обеспечения ИБ объектов; области применения ЗИС (медицина, госуправление, правоохранительные органиы/МВД); примеры.
12. Классы информационных систем с точки зрения их функционала и видов обрабатываемой в них информации.
13. Проблемы информационной безопасности при использовании ИС, АИС, АСУ.
14. Виды и свойства информации. Угрозы информационной безопасности, реализуемые в отношении ИС.
15. Нормативно-законодательные положения/документы по защите информационной безопасности в защищенных информационных системах.
16. АИС, АС в защищенном исполнении – конкретные примеры с характеристиками, функциональности и описанием штатных средств безопасности.

Практическое занятие . Представление об информационной безопасности в ЗИС.

Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Вдвоем на одну тему готовить материалы нельзя.

Темы проведения исследования:

1. Международные стандарты, ГОСТы и нормативные документы, определяющие требования к защищенности ИС/АС.
2. Нормативная база, регламентирующая разработку и эксплуатацию ИАС.
3. Нормативные и методические документы регуляторов (ФСТЭК, ФСБ) - про ЗИС («Меры защиты информации в ГИС» и проч.) Уровни защищенности и классы ИС.
4. Угрозы ИБ, предпосылки уязвимости ИС.
5. Источники, способы и результаты дестабилизирующего воздействия на информацию; Их выявление и оценка (общий алгоритм и особенности).
6. Требования к уровню защищ

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»

Студент допускается до сдачи экзамена при наличии конспекта и посещения не менее 80% аудиторных занятий в противном случае ему необходимо решить дополнительное практико-ориентированное задание

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, в котором два теоретических вопроса 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, гарантированно на решение задачи времени дается 20 минут, решение формулируется с использованием конспекта лекций и иных материалов, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Алексеев, В. В., Ивановский, М. А., Елисеев, А. И., Громов, Ю. Ю., Губсков, Ю. А.	Интеллектуальные информационные системы и технологии их построения	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ	2021	https://www.iprbookshop.ru/123026.html
Лопушанский, В. А., Макеев, С. В., Бунин, Е. С.	Информационные системы. Системы управления базами данных: теория и практика	Воронеж: Воронежский государственный университет инженерных технологий	2021	https://www.iprbookshop.ru/119640.html
Гладких, Т. В., Коробова, Л. А., Ивлиев, М. Н.	Информационные системы учета и контроля ресурсов предприятия	Воронеж: Воронежский государственный университет инженерных технологий	2020	https://www.iprbookshop.ru/106440.html
6.1.2 Дополнительная учебная литература				
Терещенко, П. В.	Информационные системы в управлении инновационной деятельностью	Новосибирск: Новосибирский государственный технический университет	2022	https://www.iprbookshop.ru/126493.html
Васильева, Е. В., Громова, А. А.	Корпоративные информационные системы на базе решения Oracle E-Business Suite	Москва: Прометей	2022	https://www.iprbookshop.ru/125689.html
Чекотило, Е. Ю., Кичигина, О. Ю.	Информационные системы управления бизнес-процессами организации	Самара: Самарский государственный технический университет, ЭБС АСВ	2020	https://www.iprbookshop.ru/105014.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

Справочно-правовая система КонсультантПлюс
ГОСТ Эксперт - единая база ГОСТов Российской Федерации
Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00
Электронная библиотека диссертаций Российской государственной библиотеки

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Windows
Microsoft Office Standart Russian Open No Level Academic
MicrosoftOfficeProfessional
Python

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

Аудитория	Оснащение
Компьютерный класс	Мультимедийное оборудование, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду
Лекционная аудитория	Мультимедийное оборудование, специализированная мебель, доска