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

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

Рабочая программа дисциплины

Б1.В.ДВ.03.01 Программно-аппаратные средства защиты информации

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
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 физико-математических наук, Доцент	_____	Васильева Ирина Николаевна
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 обучающегося в области выбора и использования программно-аппаратных средств защиты информации

1.2 Задачи дисциплины:

- Рассмотреть нормативно-правовые требования к средствам технической защиты информации;
- Рассмотреть классификацию и основные принципы функционирования программно-аппаратных средств защиты информации;
- Сформировать представления о функциональной структуре и вариантах исполнения комплексных средств защиты информации от несанкционированного доступа;
- Сформировать навыки установки, настройки и использования программно-аппаратных средств защиты информации.

1.3 Требования к предварительной подготовке обучающегося:

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

Организация и технологии защиты персональных данных

Управление информационной безопасностью

Защита электронного документооборота

Защищенные информационные системы

Криптографические средства защиты информации

Организационно-правовые механизмы обеспечения информационной безопасности

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: нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
Уметь: организовать установку и настройку технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации
Владеть: навыками входного контроля качества и контроля корректности функционирования комплектующих изделий системы защиты информации автоматизированной системы

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-правовое обоснование применения программно-аппаратных средств защиты информации	4						О
Тема 1. Оценка угроз безопасности информации, порядок выбора программно- аппаратных средств защиты информации Практическое занятие: Работа с банками данных угроз и уязвимостей		5	3		2	ИЛ	
Тема 2. Нормативно-правовые требования к средствам технической защиты информации Практическая работа: Работа с документами и реестром сертифицированных средств защиты информации ФСТЭК России		2	2		2		

Раздел 2. Управление доступом							
Тема 3. Системы идентификации и аутентификации Лабораторная работа: Управление учетными записями пользователей и настройка политик пользователя в СЗИ от НСД Dallas Lock		2		3	3	ГД	Л
Тема 4. Системы управления доступом Лабораторная работа: Настройка системы дискреционного управления доступом в СЗИ от НСД Dallas Lock Лабораторная работа: Настройка системы мандатного управления доступом в СЗИ от НСД Dallas Lock		4		6	3,75		
Раздел 3. Комплексные средства защиты информации от несанкционированного доступа							
Тема 5. Принципы построения и функциональная структура комплексных СЗИ от НСД Практическое занятие: Автономная установка и настройка политик безопасности СЗИ от НСД Secret Net Studio Практическое занятие: Настройка подсистемы полномочного управления доступом в СЗИ от НСД Secret Net Studio Практическое занятие: Настройка подсистемы дискреционного управления доступом в СЗИ от НСД Secret Net Studio Практическое занятие: Настройка подсистемы аудита в СЗИ от НСД Secret Net Studio Практическое занятие: Настройка подсистемы контроля целостности и формирование замкнутой программной среды в СЗИ от НСД Secret Net Studio		4	13		4	ИЛ	О
Тема 6. Реализация СЗИ от НСД средствами защищенной операционной системы Лабораторная работа: Настройка политик безопасности и механизмов управления доступом в ОС СН Astra Linux Лабораторная работа: Контроль съемных носителей в ОС СН Astra Linux Лабораторная работа: Контроль целостности в ОС СН Astra Linux		2		9	4		
Раздел 4. Средства сетевой защиты информации							О
Тема 7. Средства защиты и мониторинга корпоративных компьютерных сетей Практическое занятие: Настройка межсетевого экрана и СОВ в СЗИ от НСД Secret Net Studio		6	4		4		
Тема 8. Технология виртуальных частных сетей VPN		2			2		
Раздел 5. Защита от разрушающих программных воздействий							О
Тема 9. Вирусные атаки и средства антивирусной защиты информации Лабораторная работа: Настройка средств антивиусной и сетевой защиты Kaspersky Endpoint Security		4		4	4	ИЛ	

Тема 10. Технологии проактивной защиты, Threat Intelligence и Threat Hunting		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 раскрывает содержание нормативных документов, необходимых при проектировании политик безопасности конкретной организации, учитывая ее юридический статус и специфику работы. Устанавливает технические средства защиты, после чего проводит мониторинг их работы, устанавливает различные уровни доступа, иерархические уровни конфиденциальности систем мандатного управления. Проводит тестирование технических и программно-технических средств защиты информации, используя различный инструментарий для получения максимально точных результатов.	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	студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов,	не предусмотрена
	умение применять теоретические знания. Студент без затруднений ответил на все дополнительные вопросы.	
Не зачтено	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 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	Методика оценки угроз безопасности информации ФСТЭК России
2	Матрицы Mitre. Техники, тактики и процессы проведения атак (TTP)
3	База данных угроз ФСТЭК России
4	База данных уязвимостей ФСТЭК России
5	Базы данных CVE, NVD, CWE, CAPEC

6	Рейтинг критичности уязвимостей CVSS
7	Средства ЗИ, действующие на разных этапах реализации атак: функциональные особенности и назначение
8	Сканеры безопасности
9	Тестирование на проникновение
10	Понятия Threat Intelligence и Threat Hunting
11	Основные этапы (процедуры) процесса идентификации и аутентификации
12	Идентификационная информация, идентификаторы, участники процесса идентификации и аутентификации и их функциональные роли
13	Факторы и способ организации процесса аутентификации
14	Методы и виды аутентификации
15	Уровни доверия к результатам идентификации и аутентификации
16	Понятия доступа, объекта и субъекта доступа, санкционированного доступа
17	Система дискреционного управления доступом
18	Система мандатного управления доступом
19	Системы ролевого управления доступом
20	Реализация управление доступом в ОС Windows
21	Мандатный контроль целостности в ОС Windows
22	Реализация управление доступом в ОС Linux
23	Реализация мандатного контроля доступа в ОС Astra Linux SE
24	Принцип эшелонированной обороны при построении системы ЗИ
25	Варианты реализации средств ЗИ от НСД
26	Функциональная структура комплексных средств ЗИ от НСД
27	Функции модуля доверенной загрузки. Классификация модулей доверенной загрузки согласно ФСТЭК России
28	Назначение и классификация средств контроля съемных машинных носителей информации согласно ФСТЭК России
29	Классификация атак на сетевые ИС
30	Способы реализации атак «отказ в обслуживании»
31	Назначение межсетевого экранирования
32	Понятие сетевого периметра, схема 2-х и 3-х уровневого межсетевого экранирования
33	Концепция нулевого доверия в сети (Zero Trust Network Access)
34	Классификация межсетевых экранов по уровням модели OSI, их функциональные возможности и политики экранирования
35	Классификация межсетевых экранов ФСТЭК России
36	Назначение и принцип работы прокси-серверов
37	Системы обнаружения/ предотвращения вторжений: принципы работы и технологии анализа
38	Классификация систем обнаружения вторжений
39	Комплексные средства сетевой защиты: UTM и NGFW – функциональные возможности и различия
40	Функциональные возможности и архитектура средств мониторинга внутреннего сетевого трафика (NTA- систем)
41	Назначение, функциональные возможности и архитектура SIEM-систем
42	Средства анализа логов (журналов аудита)
43	Понятие SOC, его назначение и техническое оснащение
44	Технология туннелирования и VPN, классификация архитектур VPN
45	Протоколы VPN
46	Архитектура и режимы работы протокола IPSec
47	Протокол SSL/TLS, основное его отличие от IPSec
48	Понятие вредоносного ПО, виды вредоносных объектов
49	Основные тенденции развития вирусных технологий, бесфайловые атаки и способы их обнаружения
50	Понятие и особенности APT-атаки. Этапы жизненного цикла атаки Kill Chain
51	Основные технологии обнаружения вредоносного ПО
52	Основные компоненты САВЗ, классификация САВЗ согласно ФСТЭК России

5.2.2 Типовые тестовые задания

не предусмотрено

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 Произвести безвозвратное удаление объекта файловой системы в Secret Net Studio

7 Настроить аудит изменения прав доступа для объекта файловой системы в Secret Net Studio

8 Отобразить события отказов входа в журнале аудита в Secret Net Studio

9 Настроить иерархические уровни конфиденциальности системы мандатного управления доступом в ОС Astra Linux SE

10 Настроить неиерархические категории системы мандатного управления доступом в ОС Astra Linux SE

11 Назначить пользователю привилегии (уровень допуска) системы мандатного управления доступом в ОС Astra Linux SE

12 Назначить объекту файловой системы метку конфиденциальности системы мандатного управления доступом в ОС Astra Linux SE

13 Настроить парольную политику в ОС Astra Linux SE

14 Настроить политику входа пользователей в Dallas Lock

15 Настроить парольную политику в Dallas Lock

16 Создать нового пользователя Dallas Lock

17 Настроить расписание работы пользователя 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

Промежуточная аттестация проводится в виде устного опроса, время на подготовку - 0,5 часа, в это время входит подготовка к ответу на теоретические вопросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Солонская, О. И.	Средства защиты информации	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики	2021	https://www.iprbookshop.ru/117115.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				
Громов, Ю. Ю., , О. Г., Стародубов, К. В., Кадыков, А. А.	Программно-аппаратные средства защиты информационных систем	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ	2017	http://www.iprbookshop.ru/85968.html
Фомин, Д. В.	Защита информации: специализированные аттестованные программные и программно-аппаратные средства	Саратов: Вузовское образование	2021	http://www.iprbookshop.ru/110329.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

Портал для официального опубликования стандартов Федерального агентства по техническому регулированию и метрологии [Электронный ресурс]. URL: http://standard.gost.ru/wps/portal/

Официальный интернет-портал правовой информации (федеральная государственная информационная система) [Электронный ресурс]. URL: http://pravo.gov.ru

Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. URL: https://fstec.ru/

Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: http://www.iprbookshop.ru/

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

GNU/Linux

Oracle VM VirtualBox

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

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