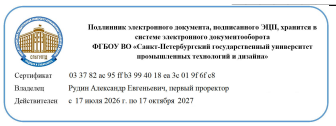
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)

УТВЕРЖДАЮ

Первый проректор, проректор по УР

_____А.Е. Рудин



Рабочая программа дисциплины

Б1.О.26 Защита информации

Учебный план: 2026-2027 09.03.01 ВШПМ Разр IT-сист и мультим прил ОО №1-1-55.plx

Кафедра: 21 Информационных и управляющих систем

Направление подготовки: (специальность) 09.03.01 Информатика и вычислительная техника

Профиль подготовки: (специализация) Разработка IT-систем и мультимедийных приложений

Уровень образования: бакалавриат

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				
8	УП	18	36	89,75	0,25	4	Зачет
	РПД	18	36	89,75	0,25	4	
Итого	УП	18	36	89,75	0,25	4	
	РПД	18	36	89,75	0,25	4	

Санкт-Петербург
2026

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника, утверждённым приказом Минобрнауки России от 19.09.2017 г. № 929

Составитель (и):

кандидат технических наук, Доцент	_____	Белая Т.И.
От кафедры составителя: Заведующий кафедрой информационных и управляющих систем	_____	Дроздова Елена Николаевна
От выпускающей кафедры: Заведующий кафедрой	_____	Дроздова Елена Николаевна

Методический отдел:

_____

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: формирование компетенций обучающегося в области применения принципов обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности.

1.2 Задачи дисциплины:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации, использовании современной научно-технической литературой для решения задач по вопросам защиты информации;
- приобретение навыков анализа информационной инфраструктуры государства с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

1.3 Требования к предварительной подготовке обучающегося:

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

Дискретная математика

Вычислительная математика

Математика

Базы данных

Методы программирования

Экономико-правовые основы рынка программного обеспечения

Правоведение

Операционные системы

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
Знать: виды угроз информационной безопасности; основные источники угроз информационной безопасности и их последствия
Уметь: применять методы экспертного оценивания для задач защиты информации; применять математические методы для анализа системы защиты информации
Владеть: выявления угроз информационной безопасности объекта; обеспечения режима и секретности на объекте

3 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Форма текущего контроля
		Лек. (часы)	Пр. (часы)		
Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации	8				Т,К
Тема 1. Понятие национальной безопасности и ее виды. Национальные интересы РФ и стратегические приоритеты. Роль аналитика в обеспечении безопасности государства. Составляющие интересов РФ в информационной сфере включая интересы личности, общества и государства. Внутренние и внешние источники угроз информационной безопасности государства. Проблемы региональной информационной безопасности.		2		12	
Тема 2. Основные понятия аналитической защиты информации. Документированная информация и принципы обеспечения ее конфиденциальности, целостности и доступности. Права обладателя информации. Виды защищаемой информации включая государственную, служебную, профессиональную и коммерческую тайну, а также персональные данные. Понятие интеллектуальной собственности и особенности аналитической оценки ее защищенности. Практическое занятие №1. Аналитический аудит личных цифровых активов и оценка рисков нарушения банковской и коммерческой тайны		2	8	12	
Раздел 2. Информационная война, методы и средства ее ведения					Т,К
Тема 3. Понятие угрозы безопасности и дестабилизирующих факторов. Субъекты и стратегические цели информационного противоборства в современном мире. Методы ведения информационных войн. Архитектура скоординированных кампаний дезинформации. Информационное оружие, его классификация, возможности и деструктивный потенциал влияния на общество и критическую инфраструктуру.		2		17	
Тема 4. Анализ методов нарушения конфиденциальности, целостности и доступности данных в условиях информационного противоборства. Причины, виды и скрытые каналы утечки информации. Особенности компьютерных систем как ключевых объектов и мишеней в информационной войне. Основные направления стратегического анализа и защиты объектов информационной сферы государства. Практическое занятие №2. OSINT-расследование цифрового следа субъекта и моделирование сценария таргетированной фишинговой атаки		2	9	10	
Раздел 3. Обеспечения информационной безопасности компьютерных систем					Т,К
Тема 5. Компьютерная система как комплексный объект анализа безопасности. Аналитический обзор способов и средств защиты. Правовые, технические, криптографические и физические методы защиты информации. Организационно-правовое обеспечение и программно-аппаратные средства контроля безопасности.		2		12,75	

Тема 6. Анализ сервисов безопасности программно-технического уровня. Механизмы идентификации, аутентификации и авторизации пользователей. Управление доступом, протоколирование и аудит событий. Криптографические методы контроля целостности и шифрования. Технологии экранирования, туннелирования и анализа защищенности сетей. Практическое занятие №3. Исследование журналов аудита программно-технического уровня для обнаружения сетевых аномалий		2	5	4	
Тема 7. Назначение и анализ формальных моделей безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели управления доступом. Математический анализ моделей Харрисона-Руззо-Ульмана и Белла-ЛаПадулы. Модели целостности Кларка-Вилсона и Биба. Ролевое управление доступом и гибридные политики безопасности. Практическое занятие №4. Построение матриц доступа и верификация безопасности информационных потоков в формальных моделях		2	5	8	
Тема 8. Методы и критерии аналитической оценки защищенности систем. Критерии безопасности «Оранжевой книги» и международные Общие критерии. Руководящие документы ФСТЭК России. Стандарты управления информационной безопасностью линейки ISO 27000. Риск-ориентированный подход к оценке соответствия систем.		2		8	
Тема 9. Защита автоматизированных систем от технических разведок. Классификация и потенциал технической и компьютерной разведки противника. Анализ технических каналов утечки информации. Электромагнитные воздействия, опасные эффекты и методы защиты вычислительной техники от внешних наводок и перехвата сигналов. Практическое занятие №5. Оценка защищенности объекта от утечек по техническим каналам и проектирование систем зашумления помещения под государственную тайну		2	9	6	
Итого в семестре (на курсе для ЗАО)		18	36	89,75	
Консультации и промежуточная аттестация (Зачет)		0,25			
Всего контактная работа и СР по дисциплине		54,25		89,75	

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5 БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ

Использование балльно-рейтинговой системы не предусмотрено.

6. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ, КРИТЕРИЕВ, СИСТЕМЫ И СРЕДСТВ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

6.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения
ОПК-3	1. Анализирует и классифицирует актуальные виды угроз информационной безопасности государства и бизнеса, выявляет скрытые каналы утечки данных и механизмы ведения современных информационных войн. 2. Проводит комплексную аналитическую оценку профессиональных задач с позиции рисков информационной безопасности, применяет математический аппарат формальных моделей доступа для верификации защищенности информационных

	систем. 3. Выявляет уязвимости и технические каналы утечки информации как в физических помещениях, так и в цифровой инфраструктуре объекта, разрабатывает и контролирует эффективный режим секретности и конфиденциальности организации.

6.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Обучающийся обнаруживает базовое или полное знание учебного материала, демонстрирует системный характер знаний по предметной области. Ответ в целом полный и правильный, подтвержден примерами; аргументация выводов может содержать незначительные недочеты, собственная точка зрения выражена слабо. Материал изложен в определенной логической последовательности, при этом допущены 2–3 несущественные погрешности, исправленные по требованию преподавателя. Обучающийся испытывает незначительные трудности в ответах на дополнительные вопросы, но успешно с ними справляется. Материал изложен осознанно, самостоятельно, с использованием профильной терминологии. При ответе обучающийся укладывается в отведенное регламентом время. Предусмотренные программой задания текущего контроля выполнены в полном объеме или на оценку не ниже «удовлетворительно».	
Не зачтено	Обучающийся обнаруживает существенные пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в формулировках базовых понятий, правил или законов изучаемой области. Ответ является неполным, несистематизированным или полностью отсутствует. Демонстрируется незнание ключевой терминологии, неспособность ориентироваться в структуре и принципах применения изученных методов и инструментов. Дополнительные и наводящие вопросы преподавателя не позволяют обучающемуся исправить допущенные ошибки. Предусмотренные программой обязательные задания текущего контроля не выполнены, либо качество их выполнения оценивается ниже оценки "удовлетворительно".	

6.3 Типовые контрольные задания и/или иные материалы, используемые для оценки результатов обучения

6.3.1 Типовые контрольные вопросы

№ п/п	Формулировки вопросов
	Семестр 8
1	Основные положения Концепции национальной безопасности Российской Федерации и Доктрины информационной безопасности Российской Федерации.

2	Понятие, предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.
3	Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну.
4	Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.
5	Защита государственной тайны. Субъекты защиты государственной тайны, их функции в данной сфере. Контроль и надзор за обеспечением защиты государственной тайны.
6	Особенности правовой защиты сведений, составляющих государственную тайну.
7	Основные объекты института коммерческой тайны.
8	Субъекты информационных правоотношений, возникающих по поводу коммерческой тайны.
9	Правовой режим коммерческой тайны.
10	Защита прав на коммерческую тайну. Ответственность за нарушения при работе с коммерческой тайной.
11	Институты профессиональных тайн и их значение для обеспечения защиты прав и свобод человека и гражданина, коммерческих интересов организаций и учреждений.
12	Основные категории сведений, защищаемых в режиме профессиональной тайны.
13	Основные категории сведений, защищаемых в режиме профессиональной тайны.
14	Система правового регулирования отдельных институтов профессиональных тайн.
15	Понятие и характеристика правонарушений в информационной сфере.
16	Криминалистическая характеристика преступлений в сфере компьютерной информации.
17	Ответственность за правонарушения в сфере компьютерной информации.
18	Основные понятия и определения информационной безопасности.
19	Основные причины уязвимости сети Internet.
20	Анализ угроз безопасности корпоративных информационных систем, обусловленных действиями субъектов.
21	Анализ угроз безопасности корпоративных информационных систем, обусловленных техническими средствами и стихийными источниками.
22	Формы сетевых атак на информацию.
23	Назначение системы защиты информации.
24	Способы защиты информации. Средства защиты информации.
25	Комплексный подход к решению проблемы защиты информации.
26	Принципы построения системы безопасности. Политика безопасности.
27	Основные понятия и определения криптографической защиты информации.
28	Процесс построения подсистемы информационной безопасности корпоративной сети. Модель адаптивного управления безопасностью сети.
29	Средства анализа защищенности всех уровней корпоративной информационной системы.
30	Классификация систем обнаружения атак. Системы обнаружения атак на сетевом и операционном уровнях. Компоненты систем обнаружения атак. Методы анализа информации. Методы реагирования. Стандарты безопасности.

6.3.2 Типовые тестовые задания

1. Основные виды защищаемой информации по содержанию:

1) секретная; 2) признаковая; 3) семантическая; 4) несекретная

2. Информацией, подлежащей защите, является…

1) информация о состоянии операционной системы; 2) сведения об окружающем мире; 3) информация, приносящая выгоду; 4) информация об учреждении профессионального образования

3. Показателями безопасности информации являются:

1) вероятность предотвращения угрозы; 2) время, в течение которого обеспечивается определенный уровень безопасности; 3) время, необходимое на взлом защиты информации; 4) вероятность возникновения угрозы информационной безопасности

4. Результатом реализации угроз ИБ может быть …

1) изменение конфигурации периферийных устройств; 2) уничтожение устройств ввода-вывода информации; 3) несанкционированный доступ к информации; 4) внедрение дезинформации в периферийные устройства

5. Абсолютная защита ПК от сетевых атак возможна при:

1) отсутствии соединения; 2) использовании лицензионного программного обеспечения; 3) установке межсетевого экрана; 4) использовании новейших антивирусных средств

6. В человеко-компьютерных системах необходимо обеспечивать ЗИ от трех

угроз:

1) случайной потери или изменения; 2) преднамеренного искажения; 3) санкционированного просмотра; 4) сбоев оборудования; 5) резервного копирования

7. Угрозами информационной войны для РФ являются:

1) ориентированность на отечественные технические средства; 2) несовершенство законодательной базы; 3) значительная протяженность территории; 4) открытость границ

8. Брандмауэр (Firewall) – это…

1) графический редактор; 2) Интернет-браузер; 3) почтовая программа; 4) межсетевой экран

9. Принципиальным отличием межсетевых экранов (МЭ) от систем обнаружения атак или вторжений (СОВ) является то, что:

1) МЭ были разработаны для активной или пассивной защиты, а СОВ - для активного или пассивного обнаружения; 2) МЭ работает только на сетевом уровне, а СОВ ещё и на физическом;

3) МЭ были разработаны для активного или пассивного обнаружения, а СОВ - для активной или пассивной защиты; 4) МЭ работает только на физическом уровне, а СОВ ещё и на сетевом

10. Предотвратить проникновение вредоносных программ на подключенный к сети компьютер помогает…

1) резервное копирование данных; 2) электронная подпись; 3) наличие электронного ключа; 4) антивирусный монитор

11. Защитить личный электронный почтовый ящик от несанкционированного доступа позволяет …

1) скрытие личного пароля; 2) электронная подпись; 3) отключение компьютера; 4) включение режима сохранения логина

12. Наиболее защищёнными от несанкционированного доступа линиями связи на сегодня являются:

1) оптоволоконные; 2) электрические; 3) инфракрасные; 4) радио

6.3.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Провести классификацию информационных ресурсов организации и составить карту актуальных внешних и внутренних угроз безопасности для корпоративной инфраструктуры в условиях таргетированной информационной атаки.

2. Выполнить аналитический аудит личных цифровых устройств и используемых программных сервисов с целью выявления рисков несанкционированного раскрытия персональных данных и компрометации банковской тайны.

3. Осуществить контролируемый сбор и критический анализ цифрового следа заданного объекта в открытых источниках медиасреды и на основе полученных данных разработать модель гипотетической фишинговой атаки.

4. Провести исследование журналов аудита программно-технического уровня (логов сервера) для обнаружения аномальной активности и верификации попыток несанкционированного доступа.

5. Построить матрицу доступа для автоматизированной системы и провести математический аудит информационных потоков на предмет наличия скрытых каналов утечки данных в рамках модели Белла-ЛаПадулы.

6. Провести сравнительный анализ соответствия организационных мер защиты ИТ-компании требованиям стандартов линейки ISO 27000 и нормативных документов ФСТЭК России.

7. Провести комплексное обследование физического помещения (учебного класса или офиса) на соответствие требованиям регуляторов к обработке сведений составляющих государственную тайну.

8. Идентифицировать потенциальные акустические и электромагнитные каналы утечки информации на объекте и разработать проектное решение по размещению технических средств зашумления и экранирования.

6.4 Методические материалы, определяющие процедуры оценивания результатов обучения

6.4.1 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»

6.4.2 Форма проведения промежуточной аттестации по дисциплине

Устная	+	Письменная		Компьютерное тестирование		Иная	

6.4.3 Особенности проведения промежуточной аттестации по дисциплине

При проведении зачета время, отводимое на подготовку к ответу, составляет не более 40 мин. Для выполнения практического задания обучающему предоставляется необходимая справочная информация.

Сообщение результатов обучающемуся производится непосредственно после устного ответа.

Выставление оценок промежуточной аттестации только по результатам выполнения практических работ и текущей аттестации в семестре не допускается.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
7.1.1 Основная учебная литература				
Штеренберг С. И.	Защита информации в компьютерных системах	Санкт-Петербург: СПбГУПТД	2022	http://publish.sutd.ru/tp_ext_inf_publish.php?id=2022163
Скрипник, Д. А.	Общие вопросы технической защиты информации	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2024	https://www.iprbookshop.ru/133955.html
Киренберг, А. Г., Коротин, В. О.	Защита информации от утечки по техническим каналам	Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева	2023	https://www.iprbookshop.ru/135100.html
7.1.2 Дополнительная учебная литература				
Боровкова, Г. С.	Анализ конечных изменений в управлении и защита информации	Липецк: Липецкий государственный технический университет, ЭБС АСВ	2018	https://www.iprbookshop.ru/92843.html
Никифоров, С. Н.	Защита информации. Защищенные сети	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	https://www.iprbookshop.ru/74382.html
Никифоров, С. Н.	Защита информации. Защита от внешних вторжений	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	http://www.iprbookshop.ru/74381.html
Никифоров, С. Н., Ромаданов, М. М.	Защита информации. Пароли, скрытие, удаление данных	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	https://www.iprbookshop.ru/80747.html
Горев, А. И., Симаков, А. А.	Обработка и защита информации в компьютерных системах	Омск: Омская академия МВД России	2016	http://www.iprbookshop.ru/72856.html

7.2 Перечень профессиональных баз данных и информационно-справочных систем

ФСТЭК России Федеральная служба по техническому и экспортному контролю - https://fstec.ru/
Система Консультант Плюс - http://www.consultant.ru/

7.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

DosBox

Python

Notepad++

Microsoft Visual C++ 2010 Express

7.4 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
Учебная аудитория	Специализированная мебель, доска