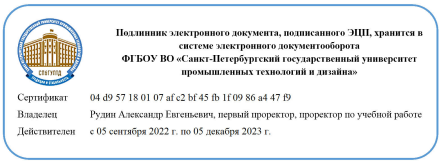
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)


Подлинник электронного документа, подписанного ЭЦП, хранится в системе электронного документооборота
ФГБОУ ВО «Санкт-Петербургский государственный университет промышленных технологий и дизайна»
Сертификат 04 d9 57 18 01 07 af c2 bf 45 fb 1f 09 86 a4 47 f9
Владелец Рудин Александр Евгеньевич, первый проректор, проректор по учебной работе
Действителен с 05 сентября 2022 г. по 05 декабря 2023 г.

УТВЕРЖДАЮ
Первый проректор, проректор по УР
_____А.Е. Рудин
«28»____06____ 2022 года

Рабочая программа дисциплины

Б1.О.26 Защита информации

Учебный план: 2022-2023 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
2022

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 Министерства образования и науки Российской Федерации от 19.09.2017 г. № 929

Составитель (и):

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

Методический отдел:

_____

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: формирование компетенций обучающегося в области 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 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. Информационная безопасность в системе национальной безопасности Российской Федерации	8					О
Тема 1. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Национальные интересы РФ и стратегические национальные приоритеты. Цели и смысл государственной службы. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.		2		12	ИЛ	
Тема 2. Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности. Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты. Практическое занятие 1: Понятие и виды защищаемой информации. Понятие и виды угроз информационной безопасности.		2	6	12	ИЛ	

Раздел 2. Информационная война, методы и средства ее ведения						
Тема 3. Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.		2		17	ИЛ	О
Тема 4. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Компьютерная система как объект информационной войны.		2		10	ИЛ	
Раздел 3. Обеспечения информационной безопасности компьютерных систем						
Тема 5. Компьютерная система как объект информационной безопасности. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программноаппаратные средства обеспечения информационной безопасности. Практическое занятие 2: Механизмы защиты информации в автоматизированных системах		2	6	12,75	ИЛ	О
Тема 6. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление. Практическое занятие 3: Особенности дискреционной и мандатной модели безопасности		2	6	4	ИЛ	

Тема 7. Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасностию Ролевое управление доступом. Практическое занятие 4: Формальные модели безопасности автоматизированных систем		2	6	8	ИЛ	
Тема 8. Методы и критерии оценки защищенности компьютерных систем. Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000. Практическое занятие 5: Руководящие документы ФСТЭК России (Гостехкомиссии)		2	6	8	ИЛ	
Тема 9. Защита информации, обрабатываемой в автоматизированных системах от технических разведок. Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем. Электромагнитное воздействие и эффекты его воздействия. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия. Практическое занятие 6: Защита информации, обрабатываемой в автоматизированных системах от технических разведок		2	6	6	ИЛ	
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. 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-3	1. Формулирует основные виды угроз информационной безопасности, называет основные каналы утечки информации 2. Проводит оценку текущих задач с точки зрения защиты информации, использует математический аппарат для кодирования информации 3. Выявляет каналы утечки информации как в помещении, так и в информационной системе, разрабатывает режим секретности на объекте	Вопросы для устного собеседования Вопросы для тестирования Практическое задание

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопросы, способен правильно применить основные методы и инструменты при решении практических задач, владеет необходимыми навыками и приемами их выполнения.	
Не зачтено	Обучающийся не может изложить значительной части программного материала, допускает существенные ошибки, допускает неточности в формулировках и доказательствах, нарушения в последовательности изложения программного материала; неуверенно, с большими затруднениями выполняет практические задания.	

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 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.

5.2.2 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

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Сформулировать основные виды угроз информационной безопасности.
2. Провести оценку задачи с точки зрения защиты информации.
3. Выявить каналы утечки информации в помещении.
4. Выявить каналы утечки информации в информационной системе.

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

При проведении зачета время, отводимое на подготовку к ответу, составляет не более 40 мин. Никакой справочной информации обучающему не предоставляется. Сообщение результатов обучающемуся производится непосредственно после устного ответа

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная 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	https://www.iprbookshop.ru/80747.html
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. Защита от внешних вторжений	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	http://www.iprbookshop.ru/74381.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
6.1.2 Дополнительная учебная литература				
Бусыгин К. Н.	Защита информации в Internet	СПб.: СПбГУПТД	2014	http://publish.sutd.ru/tp_ext_inf_publish.php?id=2043
Голиков, А. М.	Защита информации от утечки по техническим каналам	Томск: Томский государственный университет систем управления и радиоэлектроники	2015	http://www.iprbookshop.ru/72090.html
Макаров А. Г., Переборова Н. В., Вагнер В. И.	Комплексная защита информации на предприятии	СПб.: СПбГУПТД	2014	http://publish.sutd.ru/tp_ext_inf_publish.php?id=1841
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
Федоров, В. В.	Информационные технологии и защита информации в правоохранительной деятельности таможенных органов Российской Федерации	Москва: Российская таможенная академия	2014	http://www.iprbookshop.ru/69725.html
Прохорова, О. В.	Информационная безопасность и защита информации	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ	2014	http://www.iprbookshop.ru/43183.html

6.2 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/

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

DosBox

Python

Notepad++

Microsoft Visual C++ 2010 Express

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
Учебная аудитория	Специализированная мебель, доска