Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»

УТВЕРЖДАЮ
Первый проректор, проректор по учебной работе

_____ А.Е. Рудин

«30» июня 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.13	Основы информационной безопасности
(Индекс дисциплины)	*(Наименование дисциплины)*

Кафедра: 20 Интеллектуальных систем и защиты информации
Код *Наименование кафедры*

Направление подготовки: Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем (в коммерческих структурах)

Уровень образования: **Бакалавриат**

План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	108		
	Аудиторные занятия	34		
	Лекции	17		
	Лабораторные занятия			
	Практические занятия	17		
	Самостоятельная работа	74		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	2		
	Контрольная работа			
	Курсовой проект (работа)	2		
Общая трудоемкость дисциплины (зачетные единицы)		3		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам											
	1	2	3	4	5	6	7	8	9	10	11	12
Очная		3										
Очно-заочная												
Заочная												

Санкт-Петербург
2020

Программа государственной итоговой аттестации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по соответствующему направлению подготовки

и на основании учебного плана № 1/1/704

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1:	Базовая	X	Обязательная	X	Дополнительно является факультативом
	Вариативная		По выбору		

1.2. Цель дисциплины - изучение 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.

1.3. 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.

1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ОК- 5	способность понимать социальную значимость своей будущей профессии обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности общества и государства, соблюдать нормы профессиональной этики	Первый
Планируемые результаты обучения Знать: основные системы защиты информации в России и в ведущих зарубежных странах. Уметь: организовывать безопасную работу в сети Интернет. Владеть: Опытом применения аппарата исследования различных систем защиты информации.		
ОПК- 5	Способность использовать нормативные правовые акты в профессиональной деятельности	Первый
Планируемые результаты обучения Знать: вопросы административного и нормативно-правового обеспечения защиты информации. Уметь: Использовать современные методологии защиты информации. Владеть: опытом составления конфиденциальных документов.		
ПК- 4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Первый

Код компетенции	Формулировка компетенции	Этап формирования
Планируемые результаты обучения Знать: Стандарты информационной безопасности. Уметь: Выявлять требования и потребности в области информационной безопасности. Владеть: Навыками контроля изменений процесса управления информационной безопасностью ресурсов ИТ.		
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Первый
Планируемые результаты обучения Знать: жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Уметь: классифицировать основные угрозы безопасности информации. Владеть: Опытом работы со средствами защиты информации в сетях ЭВМ.		
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Первый
Планируемые результаты обучения Знать: основные функции, назначение составных частей и принципы построения систем компьютерной безопасности. Уметь: грамотно использовать элементы системы защиты информации при решении практических задач. Владеть: навыками анализа информационной архитектуры организации.		
ПК-8	Способность оформлять рабочую документацию с учетом действующих нормативных и методических документов	Первый
Планируемые результаты обучения Знать: основные причины, виды, каналы утечки и искажения информации. Уметь: использовать соответствующие методы обеспечения информационной безопасности выбранных объектов. Владеть: Навыками разработки документации для решения задач информационной безопасности.		
ПК-9	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Первый
Планируемые результаты обучения Знать: основы информационной безопасности сетей и систем и средства ее обеспечения. Уметь: принимать решения на основе анализа и оценки информации. Владеть: навыками поиска информации в глобальной информационной сети Интернет.		

Код компетенции	Формулировка компетенции	Этап формирования
ПК-10	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Первый
Знать: Виды и формы функционирования вредоносного программного обеспечения Уметь: Обосновывать правила безопасной эксплуатации программного обеспечения Владеть: навыками проведения организационных технических и программных мероприятий по защите информации		
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Первый
Знать: Основные компоненты прикладного программного обеспечения, технологии и методы его построения. Уметь: Применять методы информационной безопасности для решения задач профессиональной деятельности. Владеть: Опытом управления проектами по защите информации в своей предметной области.		
ПК-15	Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской федерации, Федеральной службы по техническому и экспортному контролю	Первый
Знать: Регламенты безопасности, принятые в организации. Уметь: Распознавать факты нарушения регламентов обеспечения безопасности на уровне БД. Владеть: Навыками выявления действий, нарушающих регламент обеспечения безопасности на уровне БД.		
ПСК-2	Готовность к администрированию средств защиты информации прикладного и системного программного обеспечения	Первый
Планируемые результаты обучения Знать: Уязвимости используемого программного обеспечения и методы их эксплуатации. Уметь: Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения. Владеть: Навыками определения порядка установки программного обеспечения с целью соблюдения требований по защите информации.		

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

Дисциплина базируется на компетенциях, сформированных на предыдущем уровне образования

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Информационная безопасность в системе национальной безопасности Российской Федерации			
Тема 1. Национальная безопасность Российской Федерации. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства.	3		
Тема 2. Национальные интересы РФ и стратегические национальные приоритеты. Цели и смысл государственной службы. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.	3		
Тема 3. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере. 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.	4		
Тема 4. 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.	3		
Тема 5. Основные понятия и общеметодологические принципы теории информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации.	3		
Тема 6. Общеметодологические принципы теории информационной безопасности. Источники понятий в области информационной безопасности.	3		
Тема 7. Понятие и виды защищаемой информации. 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.	4		
Текущий контроль 1 (Опрос)	2		
Учебный модуль 2. Информационная война, методы и средства ее ведения			
Тема 8. Понятие и виды угроз информационной безопасности. Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности.	3		
Тема 9. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации	3		
Тема 10. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.	3		
Тема 11. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации.	4		
Тема 12. Основные направления обеспечения информационной безопасности	3		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
объектов информационной сферы государства в условиях информационной войны. Компьютерная система как объект информационной войны.			
Текущий контроль 2 (Опрос)	2		
Учебный модуль 3 Обеспечения информационной безопасности компьютерных систем			
Тема 13. Методы и средства обеспечения информационной безопасности компьютерных систем. Компьютерная система как объект информационной безопасности. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации.	4		
Тема 14. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.	4		
Тема 15. Механизмы защиты информации в автоматизированных системах. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит.	4		
Тема 16. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.	4		
Тема 17. Формальные модели безопасности автоматизированных систем. 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 безопасностью. Ролевое управление доступом.	4		
Тема 18. 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».	3		
Тема 19. Общие критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.	3		
Тема 20. 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.	3		
Текущий контроль 3 (Опрос)	2		
Курсовая работа (проект)	**30**		
Промежуточная аттестация по дисциплине (Зачет с оценкой)	**4**		
ВСЕГО:	**108**		

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	2	1				
2	2	1				
3	2	1				

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
4	2	1				
5	2	1				
6	2	1				
7	2	1				
8	2	1				
9	2	1				
10	2	1				
11	2	1				
12	2	1				
13	2	1				
14	2	1				
15,16	2	1				
17,18	2	1				
19,20	2	1				
	ВСЕГО:	17				

3.2. Практические и семинарские занятия

Номера, изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Национальная безопасность Российской Федерации.(семинар)	2	1				
3	Основные составляющие национальных интересов Российской Федерации в информационной сфере. (семинар)	2	1				
4	Источники угроз информационной безопасности Российской Федерации. (семинар)	2	1				
6	Источники понятий в области информационной безопасности. (семинар)	2	2				
7	Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. (семинар)	2	1				
8	Фактор, воздействующий на защищаемую информацию. (семинар)	2	1				
10	Информационное оружие, его классификация и возможности. (семинар)	2	1				
11	Причины, виды, каналы утечки и искажения информации. (семинар)	2	1				
13	Общая характеристика способов и средств защиты информации. (семинар)	2	2				
14	Программно-аппаратные средства обеспечения информационной безопасности. (семинар)	2	1				

Номера, изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
15	Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. (семинар)	2	1				
17	Политика безопасности. (семинар)	2	1				
18	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. (семинар)	2	2				
20	Электромагнитное воздействие и эффекты его воздействия. (семинар)	2	1				
	ВСЕГО:		17				

3.3. Лабораторные занятия

Не предусмотрены

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

4.1. Цели и задачи курсовой работы (проекта)

- Реализация конкретной задачи аудита защиты информации;
- Получение знаний и навыков по испытаниям функций комплексной защиты информации методом моделирования действий нарушителя;
- Изучение программных и программно-аппаратных средств защиты информации и встроенных механизмов защиты общесистемного программного обеспечения;
- Привитие навыка работы в рабочей группе, команде.

4.2. Тематика курсовой работы (проекта)

- Классификация и способы нейтрализации вредоносных программ;
- Инфраструктура открытых ключей;
- Криптографические способы защиты информации;
- Защита информации в мобильных устройствах;
- Источники угроз информационной безопасности РФ;
- Доктрина информационной безопасности;
- Виды угроз информационной безопасности Российской Федерации;
- Понятие информационной безопасности;
- Основы информационной безопасности;
- Конфиденциальные документы;
- Общие методы обеспечения информационной безопасности Российской Федерации;
- Противодействие техническим каналам утечки информации;
- Средства защиты информации.

4.3. Требования к выполнению и представлению результатов курсовой работы

Работа выполняется индивидуально, с использованием электронных и печатных ресурсов.

Результаты представляются в виде отчета объемом до 20 страниц, содержащего следующие обязательные элементы:

- Цели и задачи, которые будут рассмотрены в работе;
- Вывод о проделанном исследовании.

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных	Форма	Очное обучение	Очно-заочное обучение	Заочное обучение

модулей, по которым проводится контроль	контроля знаний	Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1	Опрос	2					
2	Опрос	2					
3	Опрос	2					

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	2	28				
Подготовка к практическим занятиям	2	12				
Выполнение курсовых работ (проектов)	2	30				
Подготовка к зачету	2	4				
ВСЕГО:		74				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Лекции	проблемная лекция, разбор конкретных ситуаций, лекция-диалог	10		
Практические и семинарские занятия	решения проблемных ситуаций (case-study), командное соревнование малых групп	6		
	ВСЕГО:	16		

7.2. Балльно-рейтинговая система оценивания успеваемости и достижений обучающихся

Перечень и параметры оценивания видов деятельности обучающегося

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов
1	Аудиторная активность: посещение лекций и практических (семинарских) занятий, прохождение промежуточного опроса	20	• 3 балла за каждое занятие (всего 17 занятия в семестре), максимум **51** баллов • 1 балл за каждый правильный ответ на вопрос опроса **текущего контроля** (всего 16 вопросов в опросе, три опроса в семестр), максимум **49** баллов
2	Выполнение и защита курсовой работы	40	• Представление в срок и качество оформления – максимум **15** баллов; • Содержание (соответствие заданию, наличие всех требуемых элементов, наличие и значимость ошибок) – максимум **50** баллов; • Качество защиты (полнота ответов на вопросы, владение специальной терминологией, затраченное на ответы время) – максимум **35** баллов.
3	Сдача зачета	40	• Ответ на теоретический вопрос (полнота, владение

			терминологией, затраченное время) – максимум **40** баллов; • Решение практической задачи – до 30 баллов за каждую (всего 2 задачи), максимум **60** баллов.
		Итого (%):	100

Перевод балльной шкалы в традиционную систему оценивания

Баллы	Оценка по нормативной шкале	
86 - 100	5 (отлично)	Зачтено
75 – 85	4 (хорошо)	
61 – 74		
51 - 60	3 (удовлетворительно)	
40 – 50		
17 – 39	2 (неудовлетворительно)	Не зачтено
1 – 16		
0		

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс]: учебник для магистров и аспирантов/ А.В. Морозов, Л.В. Филатова, Т.А. Полякова— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 604 c.— Режим доступа: http://www.iprbookshop.ru/66771.html.— ЭБС «IPRbooks»

2. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ С.В. Петров, П.А. Кисляков— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 c.— Режим доступа: http://www.iprbookshop.ru/33857.html.— ЭБС «IPRbooks»

б) дополнительная учебная литература

1. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс]: учебное пособие/ А.О. Горбенко— Электрон. текстовые данные.— СПб.: Интермедия, 2017.— 335 c.— Режим доступа: http://www.iprbookshop.ru/66797.html.— ЭБС «IPRbooks»

2. Методические указания по дисциплине Информационная безопасность [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2013.— 20 c.— Режим доступа: http://www.iprbookshop.ru/61736.html.— ЭБС «IPRbooks»

3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 c.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»

4. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ В.А. Галатенко— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС «IPRbooks»

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине http://publish.sutd.ru/

1 Штеренберг С. И. Информационная безопасность. Стеганография [Электронный ресурс]: учебное пособие / Штеренберг С. И. — СПб.: СПбГУПТД, 2017.— 76 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=201733, по паролю.

2 Основы информационной безопасности [Электронный ресурс]: методические указания / Сост. Бусыгин К. Н. — СПб.: СПГУТД, 2014.— 44 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1719, по паролю.

3 Защита информации и информационная безопасность [Электронный ресурс]: методические указания / Сост. Бусыгин К. Н., Васильева Е. К., Дружкина Ю. Д. — СПб.: СПГУТД, 2016.— 32 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=3007, по паролю.

4 Информационная безопасность и защита информации [Электронный ресурс]: методические указания / Сост. Бусыгин К. Н. — СПб.: СПГУТД, 2014.— 36 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1723, по паролю.
5 Информационная безопасность [Электронный ресурс]: методические указания / Сост. Кравец Т. А., Суздалов Е. Г. — СПб.: СПГУТД, 2014.— 46 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=2004, по паролю
6. Спицкий, С. В. Эффективная аудиторная и самостоятельная работа обучающихся: методические указания / С. В. Спицкий. – СПб.: СПбГУПТД, 2015. – Режим доступа: http://publish.sutd.ru/tp_get_file.php?id=2015811, по паролю.
7. Караулова, И. Б. Организация самостоятельной работы обучающихся / И. Б. Караулова, Г. И. Мелешкова, Г. А. Новоселов. – СПб.: СПГУТД, 2014. – 26 с. – Режим доступа http://publish.sutd.ru/tp_get_file.php?id=2014550, по паролю

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1 http://www.iprbookshop.ru
2 http://publish.sutd.ru/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем *(при необходимости)*

1. Microsoft Office Standart 2016 Russian Open No Level Academic)
2. Microsoft Windows 10 Home Russian Open No Level Academic Legalization Get Genuine (GGK) + Microsoft Windows 10 Professional (Pro – профессиональная) Russian Upgrade Open No Level Academic

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

1 стандартно оборудованная аудитория
2 компьютер

8.6. Иные сведения и (или) материалы

Компьютерные презентации, каталоги, модели

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	• проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины; • конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; помечать важные мысли, выделять ключевые слова, термины. • Проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь; • работа с теоретическим материалом (конспектирование источников): найти ответ на вопросы в рекомендуемой литературе.
Практические занятия	• подготовка ответов к контрольным вопросам, опросам; • решение задач по алгоритму, решение кейсов
Лабораторные занятия	Не предусмотрено
Самостоятельная работа	Следует предварительно изучить методические указания по выполнению самостоятельной работы, курсовой работы (проекта), контрольной работы (можно указать реквизиты изданий и электронный ресурс, где они находятся). При подготовке к экзамену (зачету) необходимо ознакомиться с демонстрационным вариантом задания (теста, перечнем вопросов, пр.), проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя, подготовить презентацию материалов.

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ОК-5	Перечисляет основные этапы становления и развития проблем защиты информации в мировой и российской практике. Систематизирует правила работы в сети при решении задач профессиональной деятельности. Составляет обзор существующих российских и зарубежных систем защиты информации.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ОПК-5	Перечисляет основные правовые акты и документы в области обеспечения информационной безопасности. Проводит классификацию основных методов защиты информации. Осуществляет определение и классификацию конфиденциальной информации необходимой для решения профессиональных задач.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПК-4	Приводит примеры и дает краткое описание стандартов в области информационной безопасности. Оценивает необходимость проведения мероприятий по обеспечению информационной безопасности. Предлагает рекомендации по разработке политики информационной безопасности для решения профессиональных задач.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПК-5	Перечисляет риски и угрозы конфиденциальной информации в процессе документооборота. Систематизирует защищаемую информацию по видам угроз, возникающих в профессиональной деятельности. Обосновывает выбор средств защиты информации для решения профессиональных задач.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПК-7	Объясняет основные задачи обеспечения безопасности в компьютерных системах на предприятии. Оценивает область применения элементов системы защиты информации в профессиональной деятельности. Приводит примеры уязвимостей в коммерческих структурах и предлагает меры по их устранению.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ПК-8	Описывает основные проблемы, возникающие в области защиты информации на предприятии. Оценивает эффективность современных методологий информационной безопасности. Составляет план мероприятий с учетом организационно-распорядительной документации по вопросам защиты информации.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПК-9	Описывает методы и средства обеспечения информационной безопасности в компьютерных системах. Составляет перечень средств и методов защиты информации. Осуществляет поиск материалов по вопросам обеспечения информационной безопасности в базах данных и Интернет-ресурсах.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПК-10	Раскрывает механизмы действия вредоносных программ. Анализирует объект защиты с помощью методик представленных в нормативно-технических документах. Аргументированно использует различные методы защиты информации при решении профессиональной задачи.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПК-12	Определяет структуру и формулирует этапы развития прикладного программного обеспечения и приводит его классификацию. Строит информационные модели профессиональных процессов и задач защиты информации. Проводит обоснование и выбора информационных средств для решения управленческих задач на предприятии.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПК-15	Формулирует место и роль информационной безопасности в системе национальной безопасности Российской Федерации сопоставляет нарушения целостности, конфиденциальности и доступности информации оценивает соответствия применяемых требований для информационной безопасности	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)
ПСК-2	Перечисляет основные уязвимости применяемого программного обеспечения в процессе решения профессиональных задач. Компонует требования, предъявляемые к средствам обеспечения безопасности информации. Проводит поэтапную установку специализированного программного обеспечения для решения профессиональных задач.	Вопросы для устного собеседования Практическое задание	Перечень вопросов для устного собеседования (40 вопросов) Перечень практических заданий (10 заданий)

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Баллы	Оценка по традиционной шкале	Критерии оценивания сформированности компетенций	
		Устное собеседование	Курсовая работа
86 - 100	5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.. Учитываются баллы, накопленные в течение семестра.	Качество исполнения всех элементов задания полностью соответствует всем требованиям
75 – 85	4 (хорошо)	Ответ полный, основанный на проработке всех обязательных источников информации.. Учитываются баллы, накопленные в течение семестра.	Подход к материалу ответственный, но стандартный
61 – 74		Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки. Учитываются баллы, накопленные в течение семестра.	Работа выполняется индивидуально, с использованием электронных и печатных ресурсов.
51 - 60	3 (удовлетво-рительно)	Ответ воспроизводит в основном только лекционные материалы, без самостоятельной работы с рекомендованной литературой. Учитываются баллы, накопленные в течение семестра.	Демонстрирует понимание предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам.
40 – 50		Ответ неполный, основанный только на лекционных материалах. Учитываются баллы, накопленные в течение семестра.	При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов.
17 – 39	2 (неудовлетво-рительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Не учитываются баллы, накопленные в течение семестра.	Работа не выполнена
1 – 16		Непонимание заданного вопроса. Неспособность сформулировать хотя бы отдельные концепции дисциплины. Не учитываются баллы, накопленные в течение семестра.	
0		Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки). Не учитываются баллы, накопленные в течение семестра.	

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов (тестовых заданий), разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Понятие национальной безопасности Российской Федерации.	1
2	Национальные интересы РФ и стратегические национальные приоритеты.	1
3	Роль информационной безопасности в обеспечении национальной безопасности государства.	2
4	Основные составляющие национальных интересов Российской Федерации в информационной сфере.	2
5	Интересы личности общества и государства в информационной сфере.	3

6	Виды угроз информационной безопасности Российской Федерации.	3
7	Методы обеспечения информационной безопасности Российской Федерации	4
8	Источники понятий в области информационной безопасности.	4
9	Основные понятия информационной безопасности.	5
10	Общеметодологические принципы теории информационной безопасности.	5
11	Виды защищаемой информации.	6
12	Перечень сведений конфиденциального характера.	6
13	Понятие интеллектуальной собственности и особенности ее защиты.	7
14	Понятие угрозы информационной безопасности.	7
15	Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.	8
16	Классификация и виды угроз информационной безопасности.	8
17	Внутренние и внешние источники угроз информационной безопасности.	9
18	Угрозы утечки информации и угрозы несанкционированного доступа.	9
19	Основные способы защиты информации.	10
20	Понятие и классификация средств защиты информации	10
21	Уровни информационной безопасности и их характеристика.	11
22	Сервисы безопасности программно-технического уровня.	11
23	Управление доступом и его виды.	12
24	Авторизация как сервис безопасности.	12
25	Назначение формальных моделей безопасности. Политика безопасности.	13
26	Формальные модели целостности.	13
27	Модели, стратегии и системы обеспечения информационной безопасности.	14
28	Критерии безопасности компьютерных систем «Оранжевая книга».	14
29	Анализ защищенности как сервис безопасности.	15
30	Туннелирование как сервис безопасности.	15
31	Формальные модели целостности.	16
32	Понятие ролевого управления доступом	16
33	Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.	17
34	Мандатная модель безопасности. Модель Белла-ЛаПадулы.	17
35	Стандарты по управлению информационной безопасностью ISO/IEC 27000.	18
36	Критерии и классы защищенности СВТ и АС. Руководящие документы ФСТЭК России.	18
37	Классификация и возможности технических разведок.	19
38	Компьютерная разведка.	19
39	Электромагнитное воздействие и эффекты его воздействия.	20
40	Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.	20

Вариант тестовых заданий, разработанных в соответствии с установленными этапами формирования компетенций

Не предусмотрено

10.2.2. Перечень тем докладов *(рефератов, эссе, пр.)***, разработанных в соответствии с установленными этапами формирования компетенций**

Не предусмотрено

Вариант типовых заданий (задач, кейсов), разработанных в соответствии с установленными этапами формирования компетенций

	Условия типовых задач (задач, кейсов)	Ответ
1	Программист Субдеев несколько лет работал в акционерном обществе "Восход". При приеме его на работу явным образом не оговаривались и не были записаны в договоре его имущественные права на создаваемые программы За время трудовой деятельности Субдеев разработал эффективную систему автоматизации учета товаров на предприятии. Но, неудовлетворенный своей заработной платой, он уволился, предложив руководству общества "Восход" свои	Так как, при приеме на работу явным образом не оговаривались и не были записаны в договоре его имущественные права на создаваемые программы, то согласно пункту 2. Ст.1295 ГК РФ. « Исключительное право на служебное произведение принадлежит работодателю, если трудовым или иным договором между работодателем и автором не предусмотрено иное.» Значит, действия программиста не законны. Его действия можно квалифицировать ст. 273 УК РФ «**Создание, использование и распространение вредоносных программ для ЭВМ.** 1. Создание программ для ЭВМ или внесение изменений

	платные услуги по сопровождению и модернизации программного обеспечения созданной им системы Руководство сочло запрошенную Субдеевым оплату слишком высокой и отвергло его предложение. Впоследствии в акционерное общество "Восход" был принят на работу программист Новичков, на которого тоже были возложены обязанности по развитию и сопровождению системы автоматизированного учета товаров на предприятии. Субдеев, предвидя, что ему не удастся добиться желаемого соглашения с администрацией общества, модифицировал свою программу, в результате чего она перестала нормально функционировать, а это практически парализовало всю систему учета в "Восход". Оцените сложившуюся ситуацию с информационно — правовых позиций. Как квалифицировать действия программиста Субдеева?	в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев. 2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.
2	Школьники нашли легенду о древнем императоре, который для общения со своими генералами использовал тайный шифр, и с помощью этого шифра зашифровали некоторый текст, расшифруйте. ылчущзкгув— ахселжылчугтсжфхгрсенл,енсхсуспнгй жюмфлпесоесхнуюхспхзнфхзкгпзрвзх фвфлпесосп,ргшсжвьлпфвргрзнсхсусп тсфхсвррспълфозтсклщлмозеззлолтуг еззрзёсегочгелхз.ргтулпзу,еылчузфсф желёспетугесрг3,гдюогдюкгпзрзргргё,д фхгрзхж,лхгнжгозз.	Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.
3	В организации произошел инцидент информационной безопасности. Расскажите основные этапы реагирования на инцидент.	1) Подготовка к факту возникновения инцидента ИБ. Предпринимаются действия для подготовки компании к ситуации возникновения инцидента (чтобы минимизировать его последствия и обеспечить быстрое восстановление работоспособности компании). Формирование комиссии по расследованию (CSIRT) инцидентов. Этот этап является одним из самых важных, от него зависит успех в проведении расследования потенциального инцидента. 2) Обнаружение инцидента - идентификация инцидента ИБ. 3) Начальное реагирование - проведение начального расследования, запись основных деталей событий, сопровождающих инцидент, сбор комиссии по расследованию и информирование лиц, которые должны знать о произошедшем инциденте. Пресечение незаконных действий. 4) Формулирование стратегии реагирования. Стратегия базируется на всех известных фактах и определяет

		лучший путь реагирования на инцидент. Подтверждается топ-менеджментом компании. Стратегия также определяет, какие действия будут предприняты по факту возникновения инцидента (возбуждение гражданского или уголовного дела, административное воздействие), в зависимости от предполагаемых причин и последствий возникновения инцидента. 5) Расследование инцидента - проводится через сбор и анализ данных. Проверяются все собранные данные о том, что произошло, когда произошло, кто совершил неприемлемые действия, и как все это может быть предупреждено в будущем. 6) Отчет - детализированный отчет, содержащий полученную в ходе расследования информацию. Представляется в форме, удобной для принятия решения. 7) Решение - применение защитных механизмов и проведение изменений в процедурах ИБ, запись "полученных уроков".

10.3. Методические материалы,
определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска, обучающегося к сдаче зачета и порядок ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная	X	письменная		компьютерное тестирование		иная*	

**В случае указания формы «Иная» требуется дать подробное пояснение*

10.3.3. Особенности проведения зачета

Обучающийся тянет билет, в котором два теоретических вопроса и задача. После этого готовится в течении как минимум 15 минут с использованием конспекта лекций и других материалов. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. Отвечает на сопутствующие вопросы преподавателя, которые могут выходить за рамки билетов, но в рамках изучаемого материала дисциплины.

После ответа на теоретический вопрос обучающийся приступает к решению задачи, гарантированно на решение задачи времени дается 30 минут, решение формулируется с использованием конспекта лекций и иных материалов, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения, вопросы могут касаться всего материала изучаемой дисциплины.