

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» 06 2020 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06 <small>(Индекс дисциплины)</small>	Комплексная защита информации на предприятии <small>(Наименование дисциплины)</small>
Кафедра: 20 <small>Код</small>	Интеллектуальных систем и защиты информации <small>Наименование кафедры</small>
Направление подготовки:	10.03.01 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	51		
	Лекции	17		
	Лабораторные занятия	17		
	Практические занятия	17		
	Самостоятельная работа	57		
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	7		
	Контрольная работа			
	Курсовой проект (работа)			
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												

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 Обязательная Дополнительно является факультативом
 Вариативная По выбору

1.2. Цель дисциплины

Формирование компетентности в области разработки комплексной системы защиты информации предприятия, на основе оценки угроз безопасности информации, способов моделирования, технологии организации, кадрового, технологического и нормативно-методического обеспечения, методах оценки эффективности подобных систем.

1.3. Задачи дисциплины

- изучение сущности, целей и задач комплексной системы защиты информации;
- изучение принципов и этапов разработки комплексной системы защиты информации;
- освоение технологии установления состава защищаемой информации и объектов защиты информации на предприятии;
- овладение методами оценки угроз безопасности информации;
- изучение параметров и структуры комплексной системы защиты информации;
- установление состава мероприятий по обеспечению функционирования комплексной системы защиты информации;
- изучение показателей и методик эффективности системы защиты информации.

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

Код компетенции	Формулировка компетенции	Этап формирования
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Второй
Планируемые результаты обучения Знать: Теоретические аспекты комплексной системы защиты информации Уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности Владеть: Опытном работы с методами и моделями оценки эффективности КСЗИ		
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Второй
Планируемые результаты обучения Знать: Организационную структуру организации Уметь: Проводить аттестационные мероприятия Владеть: Опытном оценки эффективности защиты информации		
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Второй
Планируемые результаты обучения Знать: виды моделей, описывающих процессы защиты информации Уметь: формировать комплекс мер по защите информации на предприятии		

Код компетенции	Формулировка компетенции	Этап формирования
Владеть: Навыками разработки методических положений		
ПК-8	Способность оформлять рабочую документацию с учетом действующих нормативных и методических документов	Второй
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	Второй
Планируемые результаты обучения Знать: Архитектуру подсистем защиты информации в операционных системах Уметь: Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах Владеть: Навыками управления антивирусной защитой операционных систем в соответствии с действующими требованиями		
ПК-14	Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	Второй
Планируемые результаты обучения Знать: Современные тенденции развития организации, основные положения организационного развития Уметь: Ставить цели и формулировать задачи коллективу Владеть: Навыками организации доступа к информационным ресурсам		
ПСК-2	Готовность к администрированию средств защиты информации прикладного и системного программного обеспечения	Второй
Планируемые результаты обучения Знать: Порядок обеспечения безопасности при эксплуатации программного обеспечения Уметь: Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Владеть: Навыками формулирования требований к параметрам средств антивирусной защиты для корректной		

Код компетенции	Формулировка компетенции	Этап формирования
	работы программного обеспечения	

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

- Основы информационной безопасности (ПК-4, ПК-5, ПК-7, ПК-9, ПСК-2)
- Учебная практика (практика по получению первичных профессиональных умений и навыков) (ПК-9)
- Учебная практика (технологическая практика) (ПК-4, ПК-5, ПК-14)
- Аппаратные средства вычислительной техники (ПК-7)
- Программно-аппаратные средства защиты информации (ПК-7)
- Информационные технологии (ПК-7)
- Производственная практика (проектно-технологическая практика) (ПК-7)
- Информатика (ПК-14)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Понятие и задачи комплексной системы защиты информации.			
Тема 1. Сущность и задачи комплексной системы защиты информации (КСЗИ). Факторы, влияющие на организацию КСЗИ. Определение и нормативное закрепление состава защищаемой информации.	12		
Тема 2. Определение объектов защиты. Анализ и оценка угроз безопасности информации. Источники угроз безопасности информации. Системная классификация и общий анализ угроз безопасности. Методы оценки уязвимости информации. Определение возможностей несанкционированного доступа к защищаемой информации. Определение потенциальных каналов и методов несанкционированного доступа к информации	13		
Тема 3. Принципы организации и этапы разработки КСЗИ: Концепция создания КСЗИ. Этапы создания КСЗИ. Научно-исследовательская разработка КСЗИ. Определение компонентов КСЗИ. Определение условий функционирования КСЗИ.	11		
Текущий контроль 1 (опрос)	2		
Учебный модуль 2. Построение комплексной системы защиты информации на предприятии			
Тема 4. Технологическое и организационное построение КСЗИ. Кадровое обеспечение функционирования КСЗИ. Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. Назначение, структура и содержание управления КСЗИ.	13		
Тема 5. Принципы и методы планирования функционирования КСЗИ. Сущность и содержание контроля функционирования КСЗИ. Управление КСЗИ в условиях чрезвычайных ситуаций.	11		
Текущий контроль 2 (опрос)	2		
Учебный модуль 3. Разработка и эксплуатация комплексной системы защиты на предприятии			
Тема 6. Разработка модели КСЗИ: Моделирование КСЗИ. Математическая постановка задачи разработки КСЗИ. Состав методов и моделей оценки эффективности КСЗИ. Выбор показателей эффективности и критериев оптимизации. Подходы к оценке эффективности КСЗИ	13		
Тема 7. Функционирование КСЗИ: Пути и проблемы практической реализации КСЗИ. Внедрение КСЗИ. Техническая эксплуатация КСЗИ. Методы оптимизации КСЗИ.	13		
Тема 8. Перспективы комплексной защиты информации: Анализ зарубежного и отечественного опыта. Защищённые информационные технологии.	13		
Текущий контроль 3 (опрос)	2		
Промежуточная аттестация по дисциплине (зачет с оценкой)	3		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
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	7	2				
2	7	2				
3	7	2				
4	7	2				
5	7	2				
6	7	2				
7	7	3				
8	7	2				
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	Сущность и задачи комплексной системы защиты информации (КСЗИ). (семинар)	7	2				
2	Определение объектов защиты. Методы оценки уязвимости информации. (семинар)	7	2				
3	Принципы организации и этапы разработки КСЗИ: Концепция создания КСЗИ. (семинар)	7	2				
4	Кадровое обеспечение функционирования КСЗИ. (семинар)	7	2				
5	Сущность и содержание контроля функционирования КСЗИ. Управление КСЗИ в условиях чрезвычайных ситуаций. (семинар)	7	2				
6	Математическая постановка задачи разработки КСЗИ. Состав методов и моделей оценки эффективности КСЗИ. (семинар)	7	2				
7	Внедрение КСЗИ. Техническая эксплуатация КСЗИ. (семинар)	7	3				
8	Защищённые информационные технологии. (семинар)	7	2				
ВСЕГО:			17				

3.3. Лабораторные занятия

Номера изучаемых тем	Наименование лабораторных занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1,2	Выявление и оценка угроз безопасности информации	7	3				
3	Определение каналов несанкционированного доступа	7	2				
4	Оценка эффективности элементов КЗСИ	7	2				
5	Математическое моделирование элементов КЗСИ	7	3				
6	Методы оптимизации элементов КЗСИ	7	2				
7	Оценка экономической эффективности КЗСИ	7	2				
8	Выявление и оценка угроз безопасности информации	7	3				
ВСЕГО:			17				

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1,2,3	опрос	7	3				

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	7	20				
Подготовка к практическим занятиям	7	16				
Выполнение лабораторных работ (проектов)	7	18				
Подготовка к зачету	7	3				
ВСЕГО:			57			

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,	5		

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Практические и семинарские занятия	диспут, дискуссия	5		
Лабораторные занятия	наблюдение за процессом,	5		
ВСЕГО:		15		

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, лабораторных и практических (семинарских) занятий, прохождение промежуточного опроса	30	<ul style="list-style-type: none"> 2 балла за посещение лекционных занятий (баллы начисляются за ак. час, всего 17 ак.ч. лекций) максимум 34 балла 2 балла за посещение и активность на практических занятиях (баллы начисляются за ак. час, всего 17 ак.ч. практических занятий), максимум 34 балла 1 балл за правильный ответ на вопрос текущего контроля (10 вопросов, 3 опроса в семестр) + 2 доп. балла за ответ на дополнительный вопрос текущего контроля №3) – максимум 32 балла
2	Подготовка и предоставление отчетов по лабораторным работам	30	<ul style="list-style-type: none"> 10 баллов за подготовленный отчет по лабораторным работам (всего 7 лабораторных в семестре), максимум 70 баллов; 30 баллов за защиту работы можно получить при полном и правильном выполнении задания, предоставлении отчета с корректным оформлением и правильных ответах на вопросы по лабораторной. За недочеты и ошибки баллы снижаются
3	Сдача зачета	40	<ul style="list-style-type: none"> Ответ на теоретический вопрос (полнота, владение терминологией, затраченное время) – максимум 40 баллов; Решение практической задачи – до 60 баллов за каждую (всего 1 задача), 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		
40 – 50	3 (удовлетворительно)	Не зачтено
17 – 39	2 (неудовлетворительно)	
1 – 16		
0		

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: <http://www.iprbookshop.ru/63594.html>.— ЭБС «IPRbooks»
2. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 с. — 978-5-9963-0237-6. — Режим доступа: <http://www.iprbookshop.ru/52182.html>
- 3 Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52153.html>

б) дополнительная учебная литература

1. Сагдеев К.М. Физические основы защиты информации [Электронный ресурс]: учебное пособие/ К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 394 с.— Режим доступа: <http://www.iprbookshop.ru/63152.html>.— ЭБС «IPRbooks»
2. Бутакова Н.Г. Криптографические методы и средства защиты информации [Электронный ресурс]: учебное пособие/ Н.Г. Бутакова, Н.В. Федоров— Электрон. текстовые данные.— СПб.: Интермедия, 2017.— 384 с.— Режим доступа: <http://www.iprbookshop.ru/66791.html>.— ЭБС «IPRbooks»
3. Гатчин Ю.А. Введение в комплексную защиту объектов информатизации [Электронный ресурс]: учебное пособие/ Ю.А. Гатчин, Е.В. Климова— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2011.— 112 с.— Режим доступа: <http://www.iprbookshop.ru/65808.html>.— ЭБС «IPRbooks»
4. Коваленко Ю.И. Методика защиты информации в организациях [Электронный ресурс]: монография/ Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин— Электрон. текстовые данные.— М.: Русайнс, 2016.— 162 с.— Режим доступа: <http://www.iprbookshop.ru/61625.html>.— ЭБС «IPRbooks»

8.2. Перечень учебно-методического обеспечения для самостоятельной работы

обучающихся по дисциплине

1. Макаров А. Г. Комплексная защита информации на предприятии [Электронный ресурс]: учебное пособие / Макаров А. Г., Переборова Н. В., Вагнер В. И. — СПб.: СПГУТД, 2014.— 91 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1841, по паролю.
2. 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.
3. Защита информации в Интернет [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=2043, по паролю.
4. 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.
5. 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • подготовка ответов к контрольным вопросам, опросам; • решение задач по алгоритму, решение кейсов
Лабораторные занятия	<p>Лабораторные занятия способствуют развитию практических навыков владения изучаемыми методами, оборудованием, технологиями и др. в процессе взаимодействия со специально разработанными модельными установками и/или образцами реально действующего оборудования, предполагают проведение учебного эксперимента на лабораторной установке (самостоятельно либо под руководством преподавателя); наблюдение за процессом, и др.</p> <p>На лабораторных работах обучающийся изучает процесс или объект на основе взаимодействия с ним или его моделью (натурной или математической). В результате проведения лабораторного занятия обучающийся должен либо понять принципы устройства и работы изучаемого предмета (прикладные работы), либо освоить методику исследования предметов сходного типа (исследовательские работы).</p> <p>Следует предварительно изучить методические указания по выполнению лабораторных работ.</p>
Самостоятельная работа	<p>Следует предварительно изучить методические указания по выполнению самостоятельной работы, курсовой работы (проекта), контрольной работы (можно указать реквизиты изданий и электронный ресурс, где они находятся).</p> <p>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.</p>

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
ПК-4	Выделяет понятие, сущность, цели и задачи комплексной системы защиты информации Проводит классификацию информации, подлежащую защите согласно действующему законодательству РФ Определяет показатели уровня защищенности, основанные на экспертных оценках.	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (2 вопроса), Перечень практических заданий (6 заданий)
ПК-5	Описывает организационную структуру предприятия и делает оценку эффективности системы обеспечения безопасности Составляет план аттестационных мероприятий объекта информатизации Выявляет достоинства и недостатки средств и	Вопросы для устного собеседования Практическое задание Практическое	Перечень вопросов для устного собеседования (3 вопроса), Перечень практических

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
	мероприятий по обеспечению информационной безопасности	задание	заданий (6 заданий)
ПК-6	Классифицирует основные модели защиты информации Определяет состав мероприятий и условия, обеспечивающие функционирование системы защиты информации на предприятии Предлагает методику обеспечения комплексной защиты информации	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (3 вопроса), Перечень практических заданий (6 заданий)
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 (3 вопроса), Перечень практических заданий (6 заданий)
ПК-9	Перечисляет основные функции защиты операционной системы и дает характеристику построения ее архитектуры Оценивает параметры функционирования основных средств обеспечения безопасности на предприятии Сравнивает работу различных антивирусных программ и интерпретирует полученные результаты	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (2 вопроса), Перечень практических заданий (6 заданий)
ПК-14	называет основные этапы жизненного цикла организации и ее развития формулирует цели и задачи, связанные с командной реализацией профессиональных функций по разработке и управлению проектами в сфере информационной безопасности Предлагает организационные мероприятия для обеспечения оптимальной работы с информационными ресурсам	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (3 вопроса), Перечень практических заданий (6 заданий)
ПСК-2	Определяет критерии безопасности применения программного обеспечения Проводит анализ уязвимостей программного обеспечения с помощью специальных средств Составляет перечень требований к средствам антивирусной защиты информации на предприятии	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (3 вопроса), Перечень практических заданий (6 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
86 - 100	5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу. Качество исполнения всех элементов задания полностью соответствует всем требованиям. Учитываются баллы, накопленные в течение семестра.
75 – 85	4 (хорошо)	Ответ полный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный. Учитываются баллы, накопленные в течение семестра.
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.

51 - 60	3 (удовлетворительно)	Ответ воспроизводит в основном только лекционные материалы, без самостоятельной работы с рекомендованной литературой. Демонстрирует понимание предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам. Учитываются баллы, накопленные в течение семестра.
40 – 50		Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов. Учитываются баллы, накопленные в течение семестра.
17 – 39	2 (неудовлетворительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Не учитываются баллы, накопленные в течение семестра.
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 КЗСИ	1
2	Понятие системы управления. Виды систем управления	1
3	Обобщённый алгоритм принятия решения	2
4	Факторы, влияющие на организацию КЗСИ	2
5	Моделирование КЗСИ	3
6	Методы моделирования	3
7	Системный подход к проектированию КЗСИ	4
8	Принципы системного подхода	4
9	Прямые и косвенные факторы реализации угроз	5
10	Понятие и условия разведывательного контакта	5
11	Методика проектирования КЗСИ	6
12	Этапы проектирования КЗСИ	6
13	Оценка эффективности КЗСИ	7
14	Виды обеспечения КЗСИ	7
15	Управление КЗСИ	8
16	Особенности управления КЗСИ	8

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

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

№ п/п	Условия типовых задач (задач, кейсов)	Ответ
1	Что обязан сделать руководитель проверяемого подразделения при обнаружении нарушений первой категории?	<ul style="list-style-type: none"> организовать в установленном порядке служебное расследование по фактам утраты документов с грифом «Коммерческая тайна» либо разглашения информации, составляющей коммерческую тайну при необходимости прервать работу на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению
2	Для установления режима коммерческой тайны на предприятии по изготовлению игрушек необходимы разработка и реализация мер. Предложите перечень этих мер.	<p>определение порядка ведения конфиденциального делопроизводства, обращения документов и изделий, содержащих коммерческую тайну, организация их учета, хранения и уничтожения</p> <p>разработка перечня сведений, составляющих коммерческую тайну организации, его последующая корректировка</p> <p>предварительное изучение различных направлений деятельности организации с целью выявления реальных и потенциальных угроз и разработка мер по их предупреждению или нейтрализации</p>
3	Укажите вероятные источники утечки информации на	<ul style="list-style-type: none"> Технические средства и системы обработки информации, составляющей коммерческую тайну, в том числе линии связи, по

	предприятия, занимающимся изготовлением мебели	которым она передается <ul style="list-style-type: none"> • Документы, содержащие информацию, составляющие коммерческую тайну • персонал, имеющий доступ к информации, составляющей коммерческую тайну
--	--	--

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 письменная компьютерное тестирование иная*

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

10.3.3. Особенности проведения зачета

Обучающийся тянет билет, в котором теоретический вопрос 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.

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.