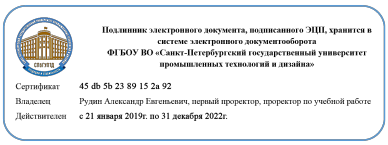
Министерство науки и высшего образования Российской Федерации

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.27	Основы управления информационной безопасностью
(Индекс дисциплины)	*(Наименование дисциплины)*

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

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	40		
	Лекции	20		
	Лабораторные занятия			
	Практические занятия	20		
	Самостоятельная работа	68		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	8		
	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												

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: Целью освоения учебной дисциплины является изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

1.3. Задачи дисциплины

- привитие обучаемым основ культуры обеспечения информационной безопасности;
- формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
- ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем;
- обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации.

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

Код компетенции	Формулировка компетенции	Этап формирования
ОПК- 5	Способность использовать нормативные правовые акты в профессиональной деятельности	Второй
Планируемые результаты обучения Знать: Требования нормативных документов Уметь: Анализировать документацию, связанную с управлением информационной безопасности Владеть: навыками управления информационной безопасностью простых объектов		
ОПК- 7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Второй
Планируемые результаты обучения Знать: современные подходы к управлению ИБ Уметь: анализировать текущее состояние ИБ на предприятии Владеть: опытом управления информационной безопасности		
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: основные стандарты, регламентирующие управление ИБ Уметь: Применять методы оценки уровня информационной безопасности организации Владеть: навыками анализа информационных активов организации		
ПК-13	Способность принимать участие в формировании,	Второй

Код компетенции	Формулировка компетенции	Этап формирования
	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	

Планируемые результаты обучения

Знать:

Основные процессы СУИБ

Уметь:

Использовать методы анализа рисков информационной безопасности

Владеть:

Опытом использования подходов к управлению службой защиты информации

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

- Основы информационной безопасности (ОПК-5, ПК-4)
- Информатика (ОПК-7, ПК-13)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Основы и системы управления информационной безопасностью (ИБ)			
Тема 1. Введение. Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний.	7		
Тема 2. Базовые вопросы управления ИБ. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления.	7		
Тема 3. Стандартизация в области управления ИБ. Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, BS 25999 и др.).	7		
Тема 4. Процессный подход. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.	6		
Тема 5. Область деятельности СУИБ. Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа).	6		
Тема 6. Ролевая структура СУИБ. Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).	7		
Тема 7. Политика СУИБ. Понятие Политики СУИБ. Цели Политики СУИБ.	6		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.			
Текущий контроль 1 (опрос)	3		
Учебный модуль 2. Основы управления рисками, процессы управления ИБ			
Тема 8. Рискология ИБ. Основные определения и положения рискологии. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ.	6		
Тема 9. Анализ рисков ИБ. Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.	7		
Тема 10. Основные процессы СУИБ. Обязательная документация СУИБ. Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».	7		
Тема 11. Внедрение разработанных процессов. Документ «Положение о применимости». Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.	6		
Тема 12. Внедрение мер (контрольных процедур) по обеспечению ИБ. Категории контрольных процедур. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками. Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик.	7		
Тема 13. Процесс «Управление инцидентами ИБ». Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.	6		
Тема 14. Процесс «Обеспечение непрерывности ведения бизнеса». Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.	7		
Тема 15. Эксплуатация и независимый аудит СУИБ. Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001.	7		
Текущий контроль 2 (опрос)	3		
Промежуточная аттестация по дисциплине (зачет с оценкой)	**3**		
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	8	2				
2	8	2				
3	8	1				
4	8	1				
5	8	2				
6	8	1				
7	8	1				
8	8	1				
9	8	1				
10	8	2				
11	8	1				
12	8	1				
13	8	1				
14	8	1				
15	8	2				
	ВСЕГО:	20				

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	Введение. Важность и актуальность дисциплины. (практикум)	8	2				
2	Базовые вопросы управления ИБ. (практикум)	8	2				
3	Стандартизация в области управления ИБ. (практикум)	8	1				
4	Процессный подход. (практикум)	8	1				
5	Область деятельности СУИБ. (практикум)	8	2				
6	Ролевая структура СУИБ. (практикум)	8	1				
7	Политика СУИБ. (практикум)	8	1				
8	Рискология ИБ. (практикум)	8	1				
9	Анализ рисков ИБ. (практикум)	8	1				
10	Основные процессы СУИБ. (практикум)	8	2				
11	Внедрение разработанных процессов. (практикум)	8	1				
12	Внедрение мер (контрольных процедур) по обеспечению ИБ. (практикум)	8	1				
13	Процесс «Управление инцидентами ИБ». (практикум)	8	1				
14	Процесс «Обеспечение непрерывности ведения бизнеса». (практикум)	8	1				
15	Эксплуатация и независимый аудит СУИБ. (практикум)	8	2				
		ВСЕГО:	20				

3.3. Лабораторные занятия

Не предусмотрено

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	Опрос	8	1				
2	Опрос	8	1				

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	8	31				
Подготовка к практическим занятиям	8	34				
Подготовка к зачету	8	3				
ВСЕГО:		68				

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	5		
Практические и семинарские занятия	Диспут, дискуссия	5		
Лабораторные занятия	Не предусмотрено			
	ВСЕГО:	10		

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	50	• 3 балла за каждое занятие (всего 20 занятий в семестре), максимум 60 баллов • 2 балла за каждый правильный ответ на вопрос опроса текущего контроля (всего 10 вопросов в опросе, два опроса в семестр), максимум 40 баллов
2	Сдача зачета	50	• Ответ на теоретический вопрос (полнота, владение терминологией, затраченное время) – максимум 40 баллов; • Решение практической задачи – до 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. Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ А.Н. Кубанков, Н.Н. Куняев— Электрон. текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.html.— ЭБС «IPRbooks»

2. Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс]: учебное пособие/ К.А. Паршин— Электрон. текстовые данные.— М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2015.— 96 с.— Режим доступа: http://www.iprbookshop.ru/45291.html.— ЭБС «IPRbooks»

б) дополнительная учебная литература

1. Пакин А.И. Информационная безопасность информационных систем управления предприятием [Электронный ресурс]: учебное пособие по части курса/ А.И. Пакин— Электрон. текстовые данные.— М.: Московская государственная академия водного транспорта, 2009.— 41 с.— Режим доступа: http://www.iprbookshop.ru/46462.html.— ЭБС «IPRbooks»

2. Обеспечение информационной безопасности бизнеса [Электронный ресурс]/ В.В. Андрианов [и др.].— Электрон. текстовые данные.— М.: ЦИПСиР, 2011.— 373 с.— Режим доступа: http://www.iprbookshop.ru/38525.html.— ЭБС «IPRbooks»

3. Астахов А.М. Искусство управления информационными рисками [Электронный ресурс]/ А.М. Астахов— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 312 с.— Режим доступа: http://www.iprbookshop.ru/63803.html.— ЭБС «IPRbooks»

4. Бирюков А.Н. Процессы управления информационными технологиями [Электронный ресурс]/ А.Н. Бирюков— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 263 с.— Режим доступа: http://www.iprbookshop.ru/52165.html.— ЭБС «IPRbooks»

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Дроботун Н. В. Управление информационной безопасностью [Электронный ресурс]: учебное пособие / Дроботун Н. В., Серова Н. Е. — СПб.: СПГУТД, 2014.— 142 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=2018, 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. 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.

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	• 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
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 зачету необходимо ознакомиться с демонстрационным вариантом задания (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
ОПК-5	Перечисляет основные требования в области управления информационной безопасности Сопоставляет внутреннюю нормативную базу организации с требованиями стандартов по управлению информационной безопасностью Предлагает принципы, подходы и виды управления при решении профессиональных задач	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (30 вопросов) Перечень практических заданий (6 заданий) Перечень практических заданий (6 заданий)
ОПК-7	Излагает основные направления развития в области управления защитой информации Формулирует требования к разрабатываемым процессам управления ИБ Применяет процессный подход построения систем управления ИБ	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (30 вопросов)
ПК-4	Раскрывает архитектуру основных стандартов защиты информации Использует методы анализа процессов для определения актуальных угроз организации Выбирает приемы анализа угроз ИБ и уязвимостей в рамках области деятельности СУИБ	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (30 вопросов) Перечень практических заданий (6 заданий)
ПК-13	Описывает основные этапы построения системы управления информационной безопасностью Осуществляет оценку рисков на основе модели угроз и уязвимостей и на основе модели информационных потоков Предлагает организационно-технические мероприятия по защите информации на предприятии	Вопросы для устного собеседования Практическое задание Практическое задание	Перечень вопросов для устного собеседования (30 вопросов) 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 (удовлетво-рительно)	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 (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.
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, разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Приведите убедительные доводы того, что информационная безопасность-одна из важнейших проблем современной жизни.	1
2	Что понимается под системой безопасности?	1
3	Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процесами?	2
4	Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.	2
5	Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.	3
6	Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?	3
7	Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.	4
8	Дайте определение и перечислите основные способы НСД к конфиденциальной информации. Охарактеризуйте обобщенную модель взаимодействия способов НСД и источников конфиденциальной информации	4
9	Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации?	5
10	Определите понятие «несанкционированный доступ» к конфиденциальной информации, как он реализуется?	5
11	Охарактеризуйте понятия доступности, целостности и конфиденциальности информации.	6
12	Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации?	6
13	Что такое программа безопасности, ее уровни.	7
14	Что такое канал НСД? Назовите типовые причины их возникновения.	7
15	Назовите основные способы добывания конфиденциальной информации злоумышленником.	8
16	Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации.	8
17	В чем специфика деятельности ФСТЭК России?	9
18	Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.	9
19	Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?	10
20	Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?	10
21	Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?	11
22	Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности	11
23	Прокомментируйте возможности биометрической идентификации (аутентификации).	12
24	Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ.	12
25	В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?	13

26	Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?	13
27	Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.	14
28	Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации	14
29	Охарактеризуйте шифрование (криптографию) в качестве основного сервиса безопасности ИС.	15
30	Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?	15

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

№ п/п	Условия типовых задач (задач, кейсов)	Ответ
1	Чем должна руководствоваться служба безопасности для обеспечения безопасности предприятия?	В своей работе служба безопасности должна руководствоваться следующими законодательными актами и внутренними документами: • Конституция РФ; • ГК РФ; • ТК РФ; Устав предприятия, коллективный договор, трудовые договоры, правила внутреннего распорядка, должностные инструкции и т. д. Службе безопасности предприятия рекомендуется подготовить следующие инструкции: • по организации режима и охране предприятия; по работе с конфиденциальной информацией; • по организации хранения дел в архиве, в том числе с конфиденциальной информацией; • по инженерно-технической защите информации.
2	Перечислите основные этапы построения СУИБ в соответствии со стандартом ISO/IEC 27001.	Как правило, проекты по созданию СУИБ включают в себя следующие основные этапы: • Определение области действия (рамок) проекта; • Проведение обследования с целью идентификации информационных активов; • Проведение оценки и анализа рисков информационной безопасности; • Разработка Политики информационной безопасности организации; • Определение защитных мер контроля и их обоснование для минимизации рисков; • Разработка нормативно-методических документов, формализующих процессы СУИБ; • Внедрение системы управления информационной безопасностью; • Подготовка к сертификации СУИБ компании на соответствие требованиям стандарта ISO/IEC 27001.
3	На что могут быть направлены отдельные процессы, процедуры, механизмы и инструменты защиты информации, используемые владельцами информационных ресурсов и информационных систем? Перечислите, опираясь на базовые сервисы технологий по защите	• на ограничение и разграничение доступа; • информационное скрытие; • введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации); • использование методов надежного хранения, преобразования и передачи информации; • нормативно-административное побуждение и принуждение. На практике современные технологии защиты информации основаны на различных базовых сервисах (таких, как аутентификация, обеспечение целостности, контроль доступа и др.), и используют различные механизмы обеспечения безопасности (такие, как шифрование, цифровые подписи, управление маршрутизацией и др.). Однако комплексность и массовость использования информационных технологий, их интеграция в повседневную деятельность предприятий, организаций, правительственных учреждений не

	информации.	позволяют решать задачи информационной безопасности только одними техническими средствами. Во всем комплексе деятельности по защите информации одно из наиболее важных мест занимает организационно-управленческая деятельность – организационное обеспечение информационной безопасности, которое представляет собой одно из четырех основных направлений работы в общей системе мер в сфере информационной безопасности, включающей в себя также разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств и совершенствование криптографических (математических) методов защиты информации.

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 *(экзамена, зачета и / или защите курсовой работы*) **и порядок ликвидации академической задолженности**

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся (принято на заседании Ученого совета 31.08.2013г., протокол № 1)

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная [X] письменная [x] 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. 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.