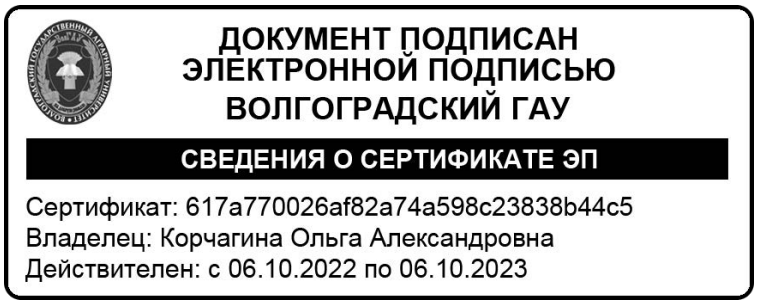
Министерство науки и высшего образования Российской Федерации
Департамент координации деятельности организаций
в сфере сельскохозяйственных наук
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Волгоградский государственный аграрный университет»

Эколого-мелиоративный факультет
наименование факультета

УТВЕРЖДАЮ
Декан эколого-мелиоративного
наименование факультета

_____ О.А. Корчагина
подпись *инициалы фамилия*

26 октября 2022 г.
дата



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.Б.20 Информационная безопасность
индекс и наименование дисциплины

Кафедра_____Информационные системы и технологии_____
наименование кафедры

Уровень высшего образования бакалавриат_____
бакалавриат / специалитет / магистратура

Направление подготовки (специальность) 38.03.05 Бизнес-информатика
шифр и наименование направления подготовки

Направленность (профиль) Бизнес-информатика в АПК_____
наименование направленности (профиля) программы

Форма обучения очная/заочная_____
очная / очно-заочная / заочная

Год начала реализации образовательной программы 2020

Волгоград
2022

Автор(ы):

доцент	_____	А.С. Матвеев
должность	*подпись*	*инициалы фамилия*
ст. преподаватель	_____	М.П. Васильев
должность	*подпись*	*инициалы фамилия*

Рабочая программа дисциплины согласована с руководителем основной профессиональной образовательной программы высшего образования по направлению подготовки 38.03.05 Бизнес-информатика
шифр и наименование направления подготовки (специальности)

Бизнес-информатика в АПК
наименование направленности (профиля) программы

Заведующий кафедрой	_____	О.В. Кочеткова
должность	*подпись*	*инициалы фамилия*

Рабочая программа дисциплины обсуждена и одобрена на заседании кафедры Информационные системы и технологии
наименование кафедры

Протокол № 2 от 20 октября 2022 г.

Заведующий кафедрой _____ О.В. Кочеткова
подпись *инициалы фамилия*

Рабочая программа дисциплины обсуждена и одобрена на заседании методической комиссии эколого-мелиоративного факультета
наименование факультета

Протокол № 2 от 25 октября 2022 г.
дата

Председатель
методической комиссии факультета _____ А.К. Васильев
подпись *инициалы фамилия*

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

Целью изучения дисциплины «Информационная безопасность» является приобретение студентами теоретических знаний и практических навыков в области информационной безопасности Изучение дисциплины направлено на решение следующих задач:

- анализ, теоретическое и экспериментальное исследование методов, алгоритмов, программ, информационной безопасности систем;
- выбор технологии, инструментальных средств и средств ВТ при организации процесса информационной безопасности систем;
- инсталляция, настройка и обслуживание системного, инструментального и прикладного программного обеспечения при организации процесса информационной безопасности систем;

Изучение дисциплины направлено на формирование профессиональных компетенций, а также знаний, умений, навыков, необходимых для решения профессиональных задач в проектной и производственно-технологической деятельности.

Процесс изучения дисциплины направлен на формирование следующих компетенций.

Индекс компетенции	**Содержание компетенции**	**Планируемые результаты:**		
		знать	**уметь**	**владеть**
ОК-9	способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях	Основные приемы первой помощи, методы защиты в чрезвычайных ситуациях	применять приемы первой помощи, методы защиты в чрезвычайных ситуациях	знаниями в использовании приемов первой помощи, методы защиты в чрезвычайных ситуациях
ПК-21	умение консультировать заказчиков по вопросам совершенствования управления информационной безапасностью ИТ-инфраструктуры предприятия	Основы консультирования заказчиков по вопросам совершенствования управления информационной безапасностью ИТ-инфраструктуры предприятия	применять знания по вопросам совершенствования управления информационной безапасностью ИТ-инфраструктуры предприятия	знаниями в консультировании заказчиков по вопросам совершенствования управления информационной безапасностью ИТ-инфраструктуры предприятия

2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.20 «Информационная безопасность» относится к базовой части учебного плана бакалавриата. Для ее успешного освоения студент должен обладать знаниями и умениями, полученными при изучении дисциплин: Б1.Б.15 Теоретические основы информатики, Б1.Б.16 Программирование, Б1.Б.17 Вычислительные системы, сети, телекоммуникации.

Знания и умения, полученные в ходе изучения дисциплины будут полезными при изучении дисциплин: Б1.Б.10 ИТ консалтинг, Б1.Б.23 Управление жизненным циклом информационных систем, Б1.В.ОД.6 Управление разработкой информационных систем.

3. **Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Очная форма обучения

Вид учебной работы		**Всего часов**	**Распределение часов по семестрам**	
			6	
Контактная работа обучающихся с преподавателем (по учебным занятиям), всего		36	36	
Лекции (Л)		18	18	
Практические занятия (ПЗ) / Семинары (С)				
Лабораторные работы (ЛР)		18	18	
Самостоятельная работа обучающихся, всего		72	72	
Курсовой проект (КП)				
Курсовая работа (КР)				
Расчетно-графическая работа (РГР)				
Реферат (Реф)				
Самостоятельное изучение разделов и тем		72	72	
Вид промежуточной аттестации (часов по учебному плану)	зачет			
	зачет с оценкой			
	экзамен	**36**	36	
Общая трудоемкость	**часов**	**144**	**144**	
	зачетных единиц	**4**	**4**	

Заочная форма обучения

Вид учебной работы		Всего часов	Распределение часов по курсам	
			4	
Контактная работа обучающихся с преподавателем (по учебным занятиям), всего		10	10	
Лекции (Л)		4	4	
Практические занятия (ПЗ) / Семинары (С)				
Лабораторные работы (ЛР)		6	6	
Самостоятельная работа обучающихся, всего		125		
Курсовой проект (КП)				
Курсовая работа (КР)				
Расчетно-графическая работа (РГР)				
Реферат (Реф)				
Самостоятельное изучение разделов и тем		125		
Вид промежуточной аттестации (часов по учебному плану)	зачет			
	зачет с оценкой			
	экзамен	**9**	9	
Общая трудоемкость	**часов**	**144**		
	зачетных единиц	**4**		

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание лекций

№	Наименование и содержание лекции	Объем, ч	
		Форма обучения	
		очная	заочная
1.	Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности	1	1

2.	Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности	1	**1**
3.	Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности	2	**1**
4.	Виды защищаемой информации. Модель угроз и модель информационной безопасности	2	
5.	Понятие защищенной информационной системы. Программа информационной безопасности	2	1
6.	Организационно-распорядительные документы в сфере информационной безопасности. Политика информационной безопасности	2	
7.	Управление информационными рисками	2	
8.	Стандартизация в сфере информационной безопасности Математические модели систем и процессов защиты информации.	2	
9.	Криптографические методы защиты информации	2	1
10.	Защита информационной инфраструктуры от атак. Антивирусные средства защиты	1	1
11.	Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ	1	
Всего		18	6

4.1. Практические (семинарские) занятия

Не предусмотрены

4.2. Лабораторные работы

№	Наименование и содержание занятия	Объем, ч	
		Форма обучения	
		очная	заочная
1	Управление информационными рисками	4	2
2	Стандартизация в сфере информационной безопасности Математические модели систем и процессов защиты информации.	4	
3	Криптографические методы защиты информации	6	2
4	Защита информационной инфраструктуры от атак. Антивирусные средства защиты	6	2
Всего		18	6

4.3. Перечень тем для самостоятельного изучения

№	Темы самостоятельной работы	Объем, ч	
		Форма обучения	
		очная	заочная
1	Проблемная область формирования информационной безопасности	4	4
2	Правовые основы реализации информационной безопасности	4	7
3	Защита интеллектуальной собственности как одна из форм защиты информации	8	18
4	Использование принципа системного подхода при анализе информационной защищенности предприятия	8	16
5	Методологии и инструменты формирования информационной защиты предприятия	8	15
6	Современные международные стандарты реализации ИБ	8	10
7	Принципы построения системы ИБ	8	10
8	Модели «нарушителя» и модели угроз ИБ	8	10
9	Разработка системы качественных и количественных показателей для оценки защищенности информационной инфраструктуры	8	10
10	Особенности информационных рисков, современные стандарты и программные продукты для оценки информационных рисков.	8	10
всего		72	110

4.4. Другие виды самостоятельной работы

№ п/п	Содержание самостоятельной работы	Объем, ч	
		Форма обучения	
		Очная	Заочная
1	Подготовка и написание контрольной работы	---	15

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

Для самостоятельной работы обучающихся по дисциплине рекомендуется следующая учебно-методическая литература:

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5
2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-627-0, 1000 экз.
3. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60x90 1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8, 300 экз.
4. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: 60x90 1/16. - (Высшее образование) (Переплёт) ISBN 978-5-369-01450-9

5. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2

6. Оценочные материалы для проведения промежуточной аттестации обучающихся по

6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Индекс компетенции	Содержание компетенции
ОК-9	способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях
ПК-21	умение консультировать заказчиков по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия

Этапы формирования компетенций в результате изучения дисциплины в процессе освоения образовательной программы

Участвующие в формировании компетенций дисциплины, модули, практики			Курсы обучения				
			1 курс	2 курс	3 курс	4 курс	5 курс
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях							
Б1.Б.20	Информационная безопасность	Очная			+		
		Заочная			+		
Б1.Б.27	Безопасность жизнедеятельности	Очная		+			
		Заочная		+			
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия							
Б1.Б.10	ИТ консалтинг	Очная				+	
		Заочная				+	
Б1.Б.20	Информационная безопасность	Очная			+		
		Заочная			+		
Б2.П.1	Получение профессиональных умений и опыта профессиональной	Очная	+				
		Заочная	+				

	деятельности						
Б2.П.2	Преддипломная практика	Очная			+		
		Заочная			+		

Основными этапами формирования указанных компетенций при освоении дисциплины является последовательное изучение содержательно связанных между собой модулей (разделов, тем). Изучение каждого модуля (раздела, темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации на различных этапах формирования компетенций показывает уровень освоения их обучающимися.

Этапы формирования компетенций
в процессе изучения дисциплины

Контролируемые модули / разделы / темы дисциплины	Оценочные средства по этапам формирования компетенций	
	Текущий контроль	Промежуточная аттестация
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях		
Управление информационными рисками	Доклад (сообщение) Лабораторная работа	Зачет
Стандартизация в сфере информационной безопасности	Доклад (сообщение) Лабораторная работа	Зачет
Математические модели систем и процессов защиты информации.	Доклад (сообщение) Лабораторная работа	Зачет
Криптографические методы защиты информации	Доклад (сообщение) Лабораторная работа	Зачет
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ- инфраструктуры предприятия		
Управление информационными рисками	Доклад (сообщение) Лабораторная работа	Зачет
Стандартизация в сфере информационной безопасности	Доклад (сообщение) Лабораторная работа	Зачет
Математические модели систем и процессов защиты информации.	Доклад (сообщение) Лабораторная работа	Зачет
Криптографические методы защиты информации	Доклад (сообщение) Лабораторная работа	Зачет

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

6.2.1 Текущий контроль

Показатели оценивания компетенций

на различных этапах их формирования в процессе изучения дисциплины

Контролируемые модули / разделы / темы дисциплины	Показатели оценивания компетенций	
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях		
Управление информационными рисками	Знать:	приемы первой помощи, методы защиты в чрезвычайных ситуациях при управлении рисками
	Уметь:	применять приемы первой помощи, методы защиты в чрезвычайных ситуациях при управлении рисками
	Владеть:	приемами первой помощи, методы защиты в чрезвычайных ситуациях
Математические модели систем и процессов защиты информации.	Знает	математические модели систем и процессов защиты информации и методы защиты в чрезвычайных ситуациях
	Умеет	применять математические модели систем и процессов защиты информации и методы защиты в чрезвычайных ситуациях
	Владеет	знаниями методы защиты в чрезвычайных ситуациях
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ- инфраструктуры предприятия		
Управление информационными рисками	Знает	консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ- инфраструктуры предприятия в управлении рисками
	Умеет	консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ- инфраструктуры предприятия при управлении рисками
	Владеет	навыками консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ- инфраструктуры предприятия
Криптографические методы защиты	Знает	Криптографические методы защиты информации и консультирует заказчиков по вопросам совершенствования управления информационной безопасностью ИТ- инфраструктуры предприятия

информации		
	Умеет	консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ- инфраструктуры предприятия и криптографической защите информации
	Владеет	Методами консультирования заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия

Шкала и критерии оценивания формируемых компетенций

в процессе изучения дисциплины, соотнесенные с этапами их формирования

Контролируемые модули / разделы / темы дисциплины	Форма оценочного средства	Шкала оценивания	Критерии оценки
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях			
Управление информационными рисками	Доклад (сообщение)	«Отлично» (8-10 баллов)	Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция. Выводы сформулированы. Тема раскрыта полностью. Работа выполнена творчески, самостоятельно. Соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны правильные ответы на дополнительные вопросы
		«Хорошо» (5-7 баллов)	Основные требования к докладу (сообщению) и его представлению в целом выполнены, но при этом допущены отдельные недочеты. Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему, однако не изложена собственная позиция. Выводы сформулированы. Работа выполнена самостоятельно. В целом соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны неточные ответы на дополнительные вопросы
		«Удовлетворительно» (2-4 балла)	Имеются существенные отступления от требований к докладам (сообщениям). Тема освещена частично. Имеются неточности в изложении материала. Отсутствует логическая последовательность в суждениях. Допущены фактические ошибки в содержании доклада (сообщения) или при ответе на дополнительные вопросы. Отсутствуют выводы. Имеются недостатки в оформлении работы. Представление доклада (сообщения) было без мультимедийного сопровождения
		«Неудовлетворительно» (0-1 балл)	Тема доклада (сообщения) не раскрыта. Обнаруживается существенное непонимание проблемы. Работа выполнена несамостоятельно. Представление доклада (сообщения) было без мультимедийного сопровождения
			Доклад (сообщение) не представлен
	лабораторн	«Отлично»	Полные ответы. Точное раскрытие поставленных вопросов. Свободное владение понятийно-

	ая работа	(8-10 баллов)	категориальным аппаратом и терминологией соответствующего раздела. Логически корректное и убедительное изложение ответа
		«Хорошо» (5-7 баллов)	Неполные ответы на поставленные вопросы, но большая часть материала изложена (отражена). Умение пользоваться понятийно-категориальным аппаратом и терминологией соответствующего раздела. В целом логически корректное, но не всегда точное и аргументированное изложение ответа
		«Удовлетворительно» (1-4 балла)	Неточное раскрытие поставленных вопросов. Затруднения с использованием понятийно-категориального аппарата и терминологии соответствующего раздела. Присутствует стремление логически определенно и последовательно изложить ответ
		«Неудовлетворительно» (0 баллов)	Поставленные вопросы не раскрыты либо содержание ответа не соответствует сути вопроса. Неумение использовать понятийно-категориальный аппарат и терминологию соответствующего раздела. Отсутствие логической связи в ответе
Математические модели систем и процессов защиты информации.	Доклад (сообщение)	«Отлично» (8-10 баллов)	Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция. Выводы сформулированы. Тема раскрыта полностью. Работа выполнена творчески, самостоятельно. Соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны правильные ответы на дополнительные вопросы
		«Хорошо» (5-7 баллов)	Основные требования к докладу (сообщению) и его представлению в целом выполнены, но при этом допущены отдельные недочеты. Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему, однако не изложена собственная позиция. Выводы сформулированы. Работа выполнена самостоятельно. В целом соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны неточные ответы на дополнительные вопросы
		«Удовлетворительно» (2-4 балла)	Имеются существенные отступления от требований к докладам (сообщениям). Тема освещена частично. Имеются неточности в изложении материала. Отсутствует логическая последовательность в суждениях. Допущены фактические ошибки в содержании доклада (сообщения) или при ответе на дополнительные вопросы. Отсутствуют выводы. Имеются недостатки в оформлении работы. Представление доклада (сообщения) было без мультимедийного сопровождения
		«Неудовлетворительно» (0-1 балл)	Тема доклада (сообщения) не раскрыта. Обнаруживается существенное непонимание проблемы. Работа выполнена несамостоятельно. Представление доклада (сообщения) было без мультимедийного сопровождения
			Доклад (сообщение) не представлен
	лабораторн	«Отлично»	Полные ответы. Точное раскрытие поставленных вопросов. Свободное владение понятийно-

	ая работа	(8-10 баллов)	категориальным аппаратом и терминологией соответствующего раздела. Логически корректное и убедительное изложение ответа
		«Хорошо» (5-7 баллов)	Неполные ответы на поставленные вопросы, но большая часть материала изложена (отражена). Умение пользоваться понятийно-категориальным аппаратом и терминологией соответствующего раздела. В целом логически корректное, но не всегда точное и аргументированное изложение ответа
		«Удовлетворительно» (1-4 балла)	Неточное раскрытие поставленных вопросов. Затруднения с использованием понятийно-категориального аппарата и терминологии соответствующего раздела. Присутствует стремление логически определенно и последовательно изложить ответ
		«Неудовлетворительно» (0 баллов)	Поставленные вопросы не раскрыты либо содержание ответа не соответствует сути вопроса. Неумение использовать понятийно-категориальный аппарат и терминологию соответствующего раздела. Отсутствие логической связи в ответе
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия			
Управление информационными рисками	Доклад (сообщение)	«Отлично» (8-10 баллов)	Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция. Выводы сформулированы. Тема раскрыта полностью. Работа выполнена творчески, самостоятельно. Соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны правильные ответы на дополнительные вопросы
		«Хорошо» (5-7 баллов)	Основные требования к докладу (сообщению) и его представлению в целом выполнены, но при этом допущены отдельные недочеты. Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему, однако не изложена собственная позиция. Выводы сформулированы. Работа выполнена самостоятельно. В целом соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны неточные ответы на дополнительные вопросы
		«Удовлетворительно» (2-4 балла)	Имеются существенные отступления от требований к докладам (сообщениям). Тема освещена частично. Имеются неточности в изложении материала. Отсутствует логическая последовательность в суждениях. Допущены фактические ошибки в содержании доклада (сообщения) или при ответе на дополнительные вопросы. Отсутствуют выводы. Имеются недостатки в оформлении работы. Представление доклада (сообщения) было без мультимедийного сопровождения
		«Неудовлетворительно» (0-1 балл)	Тема доклада (сообщения) не раскрыта. Обнаруживается существенное непонимание проблемы. Работа выполнена несамостоятельно. Представление доклада (сообщения) было без мультимедийного сопровождения

			Доклад (сообщение) не представлен
	лабораторная работа	«Отлично» (8-10 баллов)	Полные ответы. Точное раскрытие поставленных вопросов. Свободное владение понятийно-категориальным аппаратом и терминологией соответствующего раздела. Логически корректное и убедительное изложение ответа
		«Хорошо» (5-7 баллов)	Неполные ответы на поставленные вопросы, но большая часть материала изложена (отражена). Умение пользоваться понятийно-категориальным аппаратом и терминологией соответствующего раздела. В целом логически корректное, но не всегда точное и аргументированное изложение ответа
		«Удовлетворительно» (1-4 балла)	Неточное раскрытие поставленных вопросов. Затруднения с использованием понятийно-категориального аппарата и терминологии соответствующего раздела. Присутствует стремление логически определенно и последовательно изложить ответ
		«Неудовлетворительно» (0 баллов)	Поставленные вопросы не раскрыты либо содержание ответа не соответствует сути вопроса. Неумение использовать понятийно-категориальный аппарат и терминологию соответствующего раздела. Отсутствие логической связи в ответе
Математические модели систем и процессов защиты информации.	Доклад (сообщение)	«Отлично» (8-10 баллов)	Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция. Выводы сформулированы. Тема раскрыта полностью. Работа выполнена творчески, самостоятельно. Соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны правильные ответы на дополнительные вопросы
		«Хорошо» (5-7 баллов)	Основные требования к докладу (сообщению) и его представлению в целом выполнены, но при этом допущены отдельные недочеты. Обозначена проблема и обоснована ее актуальность. Сделан краткий анализ различных точек зрения на рассматриваемую проблему, однако не изложена собственная позиция. Выводы сформулированы. Работа выполнена самостоятельно. В целом соблюдены требования к оформлению работы. Представление доклада (сообщения) имело мультимедийное сопровождение. Даны неточные ответы на дополнительные вопросы
		«Удовлетворительно» (2-4 балла)	Имеются существенные отступления от требований к докладам (сообщениям). Тема освещена частично. Имеются неточности в изложении материала. Отсутствует логическая последовательность в суждениях. Допущены фактические ошибки в содержании доклада (сообщения) или при ответе на дополнительные вопросы. Отсутствуют выводы. Имеются недостатки в оформлении работы. Представление доклада (сообщения) было без мультимедийного сопровождения
		«Неудовлетворительно» (0-1 балл)	Тема доклада (сообщения) не раскрыта. Обнаруживается существенное непонимание проблемы. Работа выполнена несамостоятельно. Представление доклада (сообщения) было без мультимедийного сопровождения

			Доклад (сообщение) не представлен
	лабораторная работа	«Отлично» (8-10 баллов)	Полные ответы. Точное раскрытие поставленных вопросов. Свободное владение понятийно-категориальным аппаратом и терминологией соответствующего раздела. Логически корректное и убедительное изложение ответа
		«Хорошо» (5-7 баллов)	Неполные ответы на поставленные вопросы, но большая часть материала изложена (отражена). Умение пользоваться понятийно-категориальным аппаратом и терминологией соответствующего раздела. В целом логически корректное, но не всегда точное и аргументированное изложение ответа
		«Удовлетворительно» (1-4 балла)	Неточное раскрытие поставленных вопросов. Затруднения с использованием понятийно-категориального аппарата и терминологии соответствующего раздела. Присутствует стремление логически определенно и последовательно изложить ответ
		«Неудовлетворительно» (0 баллов)	Поставленные вопросы не раскрыты либо содержание ответа не соответствует сути вопроса. Неумение использовать понятийно-категориальный аппарат и терминологию соответствующего раздела. Отсутствие логической связи в ответе

6.2.2 Промежуточная аттестация

Показатели оценивания компетенций в результате изучения дисциплины

в процессе освоения образовательной программы

Показатели оценивания компетенций	
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях	
Знает	Основные приемы первой помощи, методы защиты в чрезвычайных ситуациях
Умеет	применять приемы первой помощи, методы защиты в чрезвычайных ситуациях
Владеет	знаниями первой помощи, методы защиты в чрезвычайных ситуациях
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия	
Знает	Основы по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия
Умеет	применять знания по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия
Владеет	знаниями разработки и совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия

Шкала и критерии оценивания формируемых компетенций
в результате изучения дисциплины в процессе освоения
образовательной программы

Шкала оценивания	Критерии оценки
экзамен	
«Отлично» (91-100 баллов)	Обучающийся обнаруживает всестороннее и глубокое знание учебного материала. Демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной дисциплины, так и смежных дисциплин. Усвоил основную и дополнительную литературу, рекомендованную для изучения дисциплины. Проявляет творческие способности в понимании, изложении и использовании учебного материала. Грамотно излагает свои мысли. В результате следует считать

	компетенцию сформированной на более высоком (продвинутом) уровне. Присутствие сформированной компетенции на продвинутом уровне свидетельствует о высоких результатах освоения дисциплины
«Хорошо» (78-90 баллов)	Обучающийся обнаруживает знание учебного материала. Демонстрирует самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель. Усвоил основную литературу, рекомендованную для изучения дисциплины. Показывает систематический характер знаний учебного материала. Грамотно излагает свои мысли. В результате это подтверждает наличие сформированной компетенции на высоком (повышенном) уровне. Присутствие сформированной компетенции на повышенном уровне следует оценить как положительное и устойчиво закрепленное в практическом навыке
«Удовлетворительно» (61-77 баллов)	Обучающийся обнаруживает отдельные пробелы в знаниях основного учебного материала. Понимает и умеет определить основные категории дисциплины. Демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем (решение было показано преподавателем). Знаком с основной литературой, рекомендованной для изучения дисциплины. В результате следует считать, что компетенция сформирована, но ее уровень недостаточно высок (пороговый уровень). Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне
«Неудовлетворительно» (менее 61 балла)	Обучающийся обнаруживает существенные пробелы в знаниях основного учебного материала. Допускает принципиальные ошибки в трактовке основных понятий и категорий дисциплины. Неспособен самостоятельно продемонстрировать наличие знаний, умений и навыков при решении заданий, которые были представлены преподавателем вместе с образцом их решения. В результате это свидетельствует об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения дисциплины

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

6.3.1 Текущий контроль

Типовые контрольные задания
для оценки сформированности компетенций в процессе изучения
дисциплины, соотнесенные с этапами их формирования

Контролируемые модули / разделы / темы дисциплины	Форма оценочного средства	№ задания
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях		
Управление информационными рисками	Отчет по лабораторной работе	Вопросы 1,13
Математические модели систем и процессов защиты информации	Отчет по лабораторной работе	Вопросы 1,14,33
Виды защищаемой информации.	Отчет по лабораторной работе	Вопросы 1-3,15,32
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия		
Математические модели систем и процессов защиты информации.	Отчет по лабораторной работе	Вопросы 1-6,17,30
Модель угроз и модель информационной безопасности	Отчет по лабораторной работе	Вопросы 1-12,23,24
Понятие защищенной информационной системы. Программа информационной безопасности	Отчет по лабораторной работе	Вопросы 1-12,23,24

Контрольные вопросы к лабораторной работе:

1. Подготовка предварительного варианта концепции информационной безопасности компании
2. Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права.
3. Подготовка описания охраняемой информации, «портрета» нарушителя, модели угроз, построение модели информационной безопасности
4. Разработка параметров защищенности программных и информационных систем компании и программы ИБ
5. Разработка модели общей и частных политик информационной безопасности компании. Подготовка нормативного документа для введения в действия политики ИБ.
6. Описание структуры информационных рисков, построение модели процесса оценки рисков, составление списка мероприятий для уменьшения рисков. Обзор программных продуктов для оценки информационных рисков.
7. Формирование опорной системы стандартов для реализации информационной безопасности предприятия.

8. Подготовка базовой совокупности сервисов информационной защиты. Выбор и внедрение средств криптографической защиты информации.
9. Формирование программно-аппаратных и технических средств защиты информационных ресурсов от внешних атак и вирусной опасности. Построение комплексной системы информационной защиты.

6.3.2 Промежуточная аттестация

Типовые контрольные задания
для оценки сформированности компетенций в результате изучения дисциплины в процессе освоения образовательной программы, соотнесенные с этапами их формирования

Контролируемые модули / разделы / темы дисциплины	№ вопроса / задания для проверки уровня обученности		
	Знать	Уметь	Владеть
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях			
Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности	Вопросы 1-10	Задание 1-10	Задание 1-10
Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности	Вопросы 1-10	Задание 1-15	Задание 1-15
Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности	Вопросы 1-15	Задание 1-15	Задание 1-25
Понятие защищенной информационной системы. Программа информационной безопасности	Вопросы 1-17	Задание 1-20	Задание 1-28
Стандартизация в сфере информационной безопасности	Вопросы 1-20	Задание 1-25	Задание 1-30
Криптографические методы защиты информации	Вопросы 1-30	Задание 1-48	Задание 1-38
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия			

Вопросы для проверки уровня обученности ЗНАТЬ (ответьте на теоретические вопросы)

1. Информационная безопасность в системе национальной безопасности
2. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
3. Виды национальной безопасности и их краткая характеристика.
4. Системные связи информационной безопасности с другими видами национальной безопасности.
5. Информационные уязвимости объектов.
6. Антропогенные информационные уязвимости.
7. Техногенные информационные уязвимости.
8. Организационно-правовые информационные уязвимости.
9. Комбинированные информационные уязвимости
10. Угрозы информационной безопасности и их источники.
11. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
12. Эндогенные и экзогенные, угрозы информационной безопасности, их классификация.
13. Антропогенные и техногенные угрозы информационной безопасности, их классификация.
14. Системная классификация угроз информационной безопасности.
15. Угрозы конфиденциальности, целостности и доступности информации.
16. Информационная война как высшая форма угрозы информационной безопасности.
17. Допуск к информационным ресурсам.
18. Основные принципы защиты информации от несанкционированного доступа.
19. Средства обеспечения информационной безопасности.
20. Аппаратные средства обеспечения информационной безопасности.
21. Программные средства обеспечения информационной безопасности.
22. Криптографические средства обеспечения информационной безопасности.
23. Стеганографические средства обеспечения информационной безопасности.
24. Организационно-правовые средства обеспечения информационной безопасности,
25. Государственная политика в области информационной безопасности.
26. Государственные органы обеспечения информационной безопасности.
27. Приоритетные направления обеспечения информационной безопасности в условиях информационного общества.
28. Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества.
29. Технические каналы утечки конфиденциальной информации. Основные методы защиты.
30. Пассивные средства противодействия техническим разведкам.
31. Активные средства противодействия техническим разведкам.
32. Базовые стратегии организации защиты информации.
33. Полное множество функций защиты информации.
34. Задачи защиты информации. Репрезентативное множество задач защиты.
35. Формирование политики обеспечения информационной безопасности объекта.
36. Проектирование оптимальных систем защиты информации.
37. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.

38. Риски информационной безопасности
39. Статистика инцидентов информационной безопасности.

Вопросы / Задания для проверки уровня обученности УМЕТЬ (решите практическую (ситуационную) задачу)

1. Были ли в вашей практике случаи попыток несанкционированного получения информации, обрабатываемой в АС? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.

2. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.

3. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.

4. Рассмотрите возможности несанкционированного получения информации в следующем случае:
- в рассматриваемой АС возможны нарушители двух категорий: внеш-ние, не имеющие отношения к системе, и внутренние, входящие в состав пер-сонала, обслуживающего АС;
- в качестве компонентов, являющихся объектами несанкционированных действий, рассматриваются магнитные носители информации (дискеты), видео-терминалы ввода-вывода информации и принтеры;
- каналами несанкционированного получения информации являются непосредственное хищение носителей, просмотр информации на экране дис-плея и выдача ее на печать.
Каковы, с вашей точки зрения, в этом случае вероятности несанкциони-рованного получения информации?
5. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?
6. Каковы основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?

7. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

8. Сравните различные известные вам модели защиты от несанкционированного доступа к информации.

9. Что можно сказать о взаимодействии уровней безопасности субъектов и объектов доступа для различных видов доступа, с которыми оперирует модель Белла – Ла Падула?

10. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями?

11. Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

12. Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере?

13. Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик.

14. Какие основные методы контроля доступа используются в современных автоматизированных системах? Охарактеризуйте эти методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.

Задания для проверки уровня обученности ВЛАДЕТЬ (предложить решение)

1. Охарактеризуйте процесс развития проблемы защиты информации в современных системах ее обработки.
2. Раскройте содержание разграничения доступа к информации с помощью монитора обращений.
3. Охарактеризуйте проблему определения предметной области информационной безопасности и дайте определения основным понятиям, используемым в этой сфере.
4. Раскройте содержание исторических этапов развития подходов к защите информации и обеспечению информационной безопасности.
5. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности.
6. Раскройте содержание модели разграничения доступа Лэмпсона – Грэхема – Деннинга.
7. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа.
8. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?
9. Раскройте содержание принципов чистоты повторно используемых ресурсов и целостности средств защиты как основных принципов защиты информации от несанкционированного доступа.
10. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.
11. . Рассмотрите основные методы повышения стойкости парольных систем аутентификации пользователей автоматизированных систем.
12. Что изучают криптография, криптоанализ и криптология? Дайте определения этим наукам.
13. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием?
14. Объясните, что представляет собой стеганография?

15. Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования.

16. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

17. От каких основных свойств криптографических алгоритмов зависит, на ваш взгляд, стойкость криптосистемы?

18. В чем принципиальное различие оценки стойкости криптосистемы с использованием теории информации и теории вычислительной сложности?

19. . Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

20. . Опишите наиболее известный алгоритм шифрования DES. Какие из основных методов шифрования использованы в этом алгоритме?

21. . Каковы основные особенности криптосистем с общедоступным ключом?

22. . Раскройте основное содержание алгоритма электронной цифровой подписи.

23. Какие методы распределения ключей в криптографических системах с большим числом абонентов вы знаете? Охарактеризуйте основные особенности децентрализованных и централизованных систем.

24. Опишите последовательность установления связи и передачи сообщений в централизованных системах распределения ключей шифрования с центром трансляции ключей и с центром распределения ключей.

25. В каких случаях применяются криптографические методы защиты информации непосредственно в ЭВМ?
26. Дайте определение компьютерного вируса как саморепродуцирующейся программы. Приведите примеры известных вам случаев заражения компьютеров вирусами.

27. Попробуйте изобразить структуру компьютерного вируса в виде программы, написанной на псевдоязыке.

28. Охарактеризуйте основные фазы, в которых может существовать компьютерный вирус.

29. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ?

30. Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами?

31. Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

32. Рассмотрите возможности вирусного подавления как одной из форм радиоэлектронной борьбы.

33. Каковы основные механизмы внедрения компьютерных вирусов в поражаемую систему?

34. Раскройте содержание комплексной стратегии защиты, ориентированной на противодействие возможному вирусному подавлению.

35. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов.

36. Какой, по вашему мнению, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала.

37. Дайте классификацию источников утечки информации по техническим каналам.

38. Что такое основные и вспомогательные технические средства автоматизированной системы? Приведите примеры и рассмотрите возможности их использования в качестве технических каналов утечки информации.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Методические материалы, определяющие процедуры
оценивания сформированности компетенций,
соотнесенные с этапами их формирования

Контролируемые модули / разделы / темы дисциплины	Форма оценочного средства	№ задания
ОК-9 способностью использовать приемы первой помощи, методы защиты в чрезвычайных ситуациях		
Виды защищаемой информации.	Доклад (сообщение)	Методические указания по подготовке доклада (сообщения)
	Лабораторная работа	Методические указания по подготовке к лабораторной работе
Модель угроз и модель информационной безопасности	Доклад (сообщение)	Методические указания по подготовке доклада (сообщения)
	Лабораторная работа	Методические указания по подготовке к лабораторной работе
Понятие защищенной информационной системы. Программа информационной безопасности	Доклад (сообщение)	Методические указания по подготовке доклада (сообщения)
	Лабораторная работа	Методические указания по подготовке к лабораторной работе
ПК-21 умение консультировать заказчиков по вопросам совершенствования управления информационной безапасностью ИТ- инфраструктуры предприятия		

Математические модели систем и процессов защиты информации.	Доклад (сообщение)	Методические указания по подготовке доклада (сообщения)
	Лабораторная работа	Методические указания по подготовке к лабораторной работе
Криптографические методы защиты информации	Доклад (сообщение)	Методические указания по подготовке доклада (сообщения)
	Лабораторная работа	Методические указания по подготовке к лабораторной работе

Методические указания по подготовке доклада (сообщения)

Доклад (сообщение) – продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической или научно-исследовательской темы. Цель выполнения доклада (сообщения) состоит в том, чтобы научить обучающихся связывать теорию с практикой, пользоваться литературой, статистическими данными, привить умение публично излагать сложные вопросы.

Работа обучающегося над докладом (сообщением) состоит из следующих этапов: выбор темы, накопление информационного материала, подготовка доклада (сообщения), выступление на семинаре.

Прежде чем приступить к подбору соответствующей литературы, целесообразно наметить общий предварительный план доклада (сообщения). План не следует излишне детализировать. В нем перечисляются основные (центральные) вопросы темы в логической последовательности. Перечень основных вопросов заканчивается краткими выводами, которые представляют обобщение важнейших положений, выдвинутых и рассмотренных в докладе (сообщении). При работе над докладом (сообщением) необходимо внимательно изучить соответствующую теме литературу, включая монографии, статистические сборники, а также материалы, публикуемые в журналах и сети Интернет.

Когда обучающийся в достаточной степени накопил и изучил материал по соответствующей теме, он принимается за его систематизацию. Внимательно перечитывая свой конспект, обучающийся располагает материал в той последовательности, которая представляется ему наиболее стройной и целесообразной. Одновременно обучающийся фиксирует собственные мысли, которые он считает нужным изложить в тексте доклада (сообщения).

Основному тексту в докладе (сообщении) предшествует введение. В нем необходимо показать значение, актуальность рассматриваемой проблемы, обоснованность причины выбора темы. Кроме того, следует отметить, в каких произведениях известных ученых-экономистов рассматривается изучаемая проблема. В основной части работы большое внимание следует уделить глубокому теоретическому освещению как темы в целом, так и отдельных ее вопросов, правильно увязать теоретические положения с практикой, конкретным

фактическим и цифровым материалом. Представление доклада (сообщения) должно иметь мультимедийное сопровождение.

После обсуждения доклада (сообщения) в группе работа обучающегося оценивается преподавателем.

Методические указания по подготовке к лабораторной работе

Лабораторная работа представляет собой средство контроля усвоения учебного материала темы или раздела дисциплины, организованное как учебное занятие в виде практической работы преподавателя с обучающимися. Целью лабораторной работы является формирование у обучающегося навыков работы и практической реализации теоретических знаний на основе самостоятельного изучения учебной и научной литературы. От обучающегося требуется:

- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- знание разных точек зрения, высказанных в специальной литературе по соответствующей проблеме, умение сопоставлять их между собой;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.

Однако лабораторная работа не консультация и не экзамен. Его задача добиться глубокого изучения отобранного материала путем практической реализации теоретических знаний, пробудить у обучающегося стремление к чтению дополнительной литературы. Экзамен завершает изучение определенного раздела учебного курса и должен показать умение обучающегося использовать полученные знания в ходе подготовки и сдачи лабораторных работ при ответах на экзаменационные вопросы.

7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

7.1 Основная литература

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5
2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-627-0, 1000 экз.
3. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60x90 1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8, 300 экз.

Дополнительная литература:

1. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: 60x90 1/16. - (Высшее образование) (Переплёт) ISBN 978-5-369-01450-9

2. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.setevoi.ru/
2. http://www.iso27000.ru
3. http://znanium.com/bookread.php?book=411182
4. http://www.gaap.ru/biblio/soft/art_soft026.asp
5. http://www.fd.ru/

9 Методические указания для обучающихся по освоению дисциплины

В ходе лекционных занятий обучающимся рекомендуется: 1) вести конспектирование учебного материала; 2) обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению; 3) задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций; 4) желательно оставить в рабочих конспектах поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Самостоятельная работа обучающихся осуществляется в виде изучения литературных источников и эмпирических данных по публикациям, подготовки докладов (сообщений), выполнения творческих заданий, работы с лекционным материалом, самостоятельного изучения отдельных тем дисциплины.

Подготовка к контрольным мероприятиям требует от обучающегося не только повторения пройденного материала на аудиторных занятиях, но поиска и анализа материала, выданного на самостоятельное изучение. При подготовке к лабораторным работам обучающимся необходимо повторить материал лекционных и практических (семинарских) занятий по отмеченным преподавателем темам.

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций в процессе изучения дисциплины, проводится в форме текущего контроля и промежуточной аттестации. Текущий контроль успеваемости осуществляется в течение семестра в ходе повседневной учебной работы, обеспечивая оценивание хода освоения дисциплины. В частности, текущий контроль успеваемости проводится с целью определения уровня усвоения обучающимися знаний, оценки формирования у них умений и навыков. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению дисциплины. Текущий контроль успеваемости осуществляются на практических (семинарских) занятиях, а также в ходе индивидуальных консультаций с преподавателем. К оценочным средствам для проведения текущего контроля успеваемости по дисциплине относятся доклад (сообщение).

Промежуточная аттестация обучающихся позволяет определить степень достижения запланированных результатов обучения по дисциплине и проводится в форме экзамена. Данная форма контроля включает в себя теоретические вопросы, позволяющие оценить уровень освоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и навыков. Форма проведения экзамена (устная, письменная,

тестирование) определяется преподавателем. По результатам экзамена выставляется оценка: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

10 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При осуществлении образовательного процесса по дисциплине используется следующее программное обеспечение и информационные справочные системы:

6. http://www.setevoi.ru/
7. http://www.iso27000.ru
8. http://znanium.com/bookread.php?book=411182
9. http://www.gaap.ru/biblio/soft/art_soft026.asp
10. http://www.fd.ru/

11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных аудиторий (помещений)	Перечень основного оборудования, приборов и материалов
1	Лекционная аудитория	Видеопроекционное оборудование и экран
2	Компьютерный класс	Не менее 25 персональных компьютеров, имеющих выход в локальную сеть университета и Интернет, доступ к ресурсам информационного центра вуза, интерактивная доска, проектор

12. Иные сведения и (или) материалы

12.1. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

При освоении дисциплины используется сочетание отдельных видов учебной работы с методами и формами активизации познавательной деятельности обучающихся с целью достижения запланированных результатов обучения и формирования соответствующих компетенций.

Методы активного и интерактивного обучения

при разных видах учебных занятий

№ п/п	Методы активного и интерактивного обучения	Лекции	Практические (семинарские) занятия	Лабораторные работы	Самостоятельная работа
1.	Разбор конкретных ситуаций	+	+		+
2.	Электронное тестирование знаний	+			+