Образовательное учреждение профсоюзов
высшего образования
«Академия труда и социальных отношений»
Курганский филиал

Кафедра математики и прикладной информатики

Утверждаю:
Председатель Ученого Совета
Курганского филиала
ОУП ВО «АТиСО»
_____ В.Г.Роговая
Протокол № 2 от 04.10. 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки: 09.03.03«Прикладная информатика»;
Форма обучения: заочная
Цикл дисциплин: Б1.В.15
Трудоёмкость дисциплины (з.е./ч.) – 4/144

Вид учебной работы	Часы	Курсы			
		1	2	3	4
Аудиторные занятия (всего), в том числе:	16				16
Лекции	6				6
Лабораторные работы	-				-
Практические занятия: Из них: текущий контроль (тестирование, коллоквиум) (ТК)	10				10
Процент интерактивных форм обучения от аудиторных занятий по дисциплине, %	25				25
Самостоятельная работа (всего),в том числе:	119				119
Курсовая работа (КР):	-				-
Курсовой проект (КП):	-				-
Контрольная работа (аудиторная)	-				-
Вид промежуточной аттестации (зачет, экзамен)	Экз/9				Экз/9
Общая трудоемкость дисциплины	144/4				144/4

Курган - 2019

СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ В РАБОЧЕЙ ПРОГРАММЕ

Рабочая программа утверждена на 2019 20 20 учебный год со следующими изменениями:

Программа актуализирована в связи с переходом на ФГОС ВО (3++) 09.03.03 Прикладная информатика, утвержденный приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 922

Протокол заседания кафедры № 1 от «06» сентября 2019 г.
Заведующий кафедрой
_____ /С.В. Ковбасюк/

Рабочая программа утверждена на 20__/ 20__ учебный год со следующими изменениями:

Протокол заседания кафедры № _____ от «_____»_____ 20_ г.
Заведующий кафедрой
_____/_____/

Рабочая программа утверждена на 20__/ 20__ учебный год со следующими изменениями:

Протокол заседания кафедры № _____ от «_____»_____ 20_ г.

Рабочая программа составлена:

- НА ОСНОВАНИИ И С УЧЁТОМ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ - ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.03.03 «ПРИКЛАДНАЯ ИНФОРМАТИКА» (КВАЛИФИКАЦИЯ «БАКАЛАВР») ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «Информационная безопасность» ОУП ВО «АТ и СО» и с учетом требований профессионального стандарта 06.015 "Специалист по информационным системам", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. N 896н (зарегистрирован Министерством юстицииРоссийскойФедерации 24 декабря 2014 г., регистрационный N 35361)

- на основании учебного плана подготовки бакалавров по данному направлению.

Рабочую программу разработал:

нач. отдела ИТ (должность) _____ (подпись) / Михайленко В.С. (расшифровка)

Программа утверждена на заседании
Кафедры математики и прикладной информатики

Протокол № 1 «06» сентября 2019 г.

Заведующий кафедрой: _____ / С.В. Косовская

1 Место дисциплины (модуля) в структуре ООП ВО

Дисциплина входит в состав вариативной части формируемая участниками образовательных отношений дисциплин ООП (Б1.В.15).

Для изучения дисциплины студент должен обладать знаниями, полученными при изучении учебных предметов «Теория вероятностей и математическая статистика» математического и естественнонаучного цикла, «Операционные системы», «Управление информационными ресурсами в экономике», «Управление экономическими информационными системами», «Базы данных», «Системная архитектура информационных систем», «Интернет – технологии в экономической деятельности»профессионального цикла.

По завершении изучения дисциплины «Информационная безопасность» студент должен

Знать:

- виды обеспечения информационных систем;

- методологию оценки видов обеспечения информационных систем с точки зрения их информационной безопасности;

- методологию обследования организаций с целью выявления ихпотребностей в информационной защите;

- требования к информационным системам с точки зрения их информационной безопасности;

- особенности реинжиниринга прикладных и информационных процессов с точки зрения их информационной безопасности;

- содержание основных нормативно-правовых документов, регулирующих обеспечение информационной безопасности;

- методологию моделирования и проектирования структур данных и знаний, прикладных и информационных процессов с точки зрения их информационной безопасности;

- условия информационной безопасности при создании и управлении ИС на всех этапах жизненного цикла;

- методы и средства обеспечения информационной безопасности;

Уметь:

- обосновывать выбор проектных решений по видам обеспечения информационных систем с точки зрения их информационной безопасности;

- применять методологию обследования организаций с целью выявления ихпотребностей в информационной защите;

- анализировать и оценивать информационные системы с точки зрения их информационной безопасности;

- осуществлять реинжиниринг прикладных и информационных процессов с учётом их информационной безопасности;

- применять основные нормативно-правовые документы, регулирующие обеспечение информационной безопасности;

- моделировать и проектировать структуры данных и знаний, прикладные и информационные процессы с учётом их информационной безопасности;

- обеспечивать информационную безопасность при создании и управлении ИС на всех этапах жизненного цикла;

- анализировать и выбирать методы и средства обеспечения информационной безопасности;

Владеть:

- навыками применения методов и средств оценки степени информационной безопасности видов обеспечения информационных систем;

- навыками применения методологии обследования организаций с целью выявления их потребностей в информационной защите;

- способностью анализировать и оценивать информационные системы с точки зрения их информационной безопасности;

- основными методологическими подходами реинжиниринга прикладных и информационных процессов с учётом их информационной безопасности;

- навыками анализа и применения нормативно-правовых документов, относящихся к обеспечению информационной безопасности;

- навыками моделирования и проектирования систем комплексной защиты информации в предпринимательских структурах;

- способностью обеспечивать информационную безопасность при создании и управлении ИС на всех этапах жизненного цикла;

- навыками анализа и выбора методов и средств обеспечения информационной безопасности.

2 Цели и задачи освоения дисциплины

Целью освоения дисциплины является изучение студентами современной концепции и задач защиты информации, основных тенденций и направлений формирования и функционирования комплексных систем защиты информации в различных типах предпринимательских структур и организационно-правовых аспектов безопасности информационных ресурсов.

Задачами освоения дисциплины являются:

1.Изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем обеспечения информационной безопасности в предпринимательской деятельности;

2.Изучение нормативно-правовых актов в области обеспечения информационной безопасности различных предпринимательских структур;

3.Изучение научно-технической информации, отечественного и зарубежного опыта в области обеспечения информационной безопасности;

4. Выработка навыков применения методов, способов и средств обеспечения информационной безопасности в предпринимательской деятельности.

3 Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности;

ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;

ПКО-1 Способность моделировать прикладные (бизнес) процессы и предметную область;

ПКО-3 Способность принимать участие в организации ИТ инфраструктуры и управлении информационной безопасностью.

4 Образовательные результаты освоения дисциплины, соответствующие определенным компетенциям

1) знать:

Образовательный результат (указываются формируемые образовательные результаты в рамках соответствующих компетенций)
- методологию обследования организаций с целью выявления их информационных потребностей; - требования к информационным системам с точки зрения их информационной безопасности; - особенности реинжиниринга прикладных и информационных процессовс точки зрения их информационной безопасности; - содержание основных нормативно-правовых документов, регулирующих обеспечение информационной безопасности.
- методологию моделирования и проектирования структур данных и знаний, прикладных и информационных процессовс точки зрения их информационной безопасности.
- условия информационной безопасности при создании и управлении ИС на всех этапах жизненного цикла.
- виды обеспечения информационных систем; - методологию оценки видов обеспечения информационных систем с точки зрения их информационной безопасности.
- методы и средства обеспечения информационной безопасности.

2) уметь:

Образовательный результат (указываются формируемые образовательные результаты в рамках соответствующих компетенций)
- применять методологию обследования организаций с целью выявления их информационных потребностей; - анализировать и оценивать информационные системы с точки зрения их информационной безопасности; - применять основные нормативно-правовые документы, регулирующие обеспечение информационной безопасности.
- моделировать и проектировать структуры данных и знаний, прикладные и информационные процессыс учётом их информационной безопасности.
- обеспечивать информационную безопасность при создании и управлении ИС на всех этапах жизненного цикла.
- обосновывать выбор проектных решений по видам обеспечения информационных системс точки зрения их информационной безопасности.
- анализировать и выбирать методы и средства обеспечения информационной безопасности.

3) владеть:

Образовательный результат (указываются формируемые образовательные результаты в рамках соответствующих компетенций)
- навыками применения методологии обследования организаций с целью выявления их потребностей в информационной защите; - способностью анализировать и оценивать информационные системы с точки зрения их информационной безопасности; - основными методологическими подходами реинжиниринга прикладных и информационных процессов с учётом их информационной безопасности; - навыками анализа и применения нормативно-правовых документов, относящихся к обеспечению информационной безопасности.
- навыками моделирования и проектирования систем комплексной защиты информации в предпринимательских структурах.
- способностью обеспечивать информационную безопасность при создании и управлении ИС на всех этапах жизненного цикла.
- навыками применения методов и средств оценки степени информационной безопасности видов обеспечения информационных систем.
- навыками анализа и выбора методов и средств обеспечения информационной безопасности.

5 Матрица соотнесения тем/разделов учебной дисциплины и формируемых в них компетенций

Шифр раздела,	Наименование раздела, темы дисциплины	Количество часов	Компетенции	
			Общепрофессиональные (ОПК),профессиональные (ПКО)	зачётные единицы
Р1	**Основы теории информационной безопасности**	26	ОПК – 3, ОПК – 4, ПКО – 1, ПКО – 3	0,7
Р2	**Особенности защиты информации в предпринимательской деятельности**	118	ОПК – 3, ОПК – 4, ПКО – 1, ПКО – 3	3,3
Итого:		144		4

6 Тематическое планирование

6.1 Распределение учебных занятий по разделам

Шифр раздела, темы дисциплины	Наименование раздела, темы дисциплины	Количество часов по видам учебных занятий		
		лекции	практические занятия	самостоятельная работа
Р1	**Основы теории информационной безопасности**	4	-	22
1	Информационная безопасность как составная часть экономической безопасностипредпринимательской деятельности	1	-	1
2	Основы информационной безопасности и защиты информации	1	-	5
3	Информационные ресурсы. Защита открытых и закрытых информационных ресурсов	1	-	8
4	Источники конфиденциальной информации и каналы ее утраты	1	-	8

Р2	**Особенности защиты информации в предпринимательской деятельности**	2	10	106
5	Системы защиты информации: назначение, принципы и структура	1	1	8
6	Регламентация работы систем защиты информации	1	1	10
7	Защищённый документооборот	-	2	22
8	Защита информации в процессе публикаторской, рекламной и выставочной деятельности	-	2	22
9	Защита информации в компьютерах, локальных сетях и средствах связи	-	2	22
10	Охрана территорий, зданий, помещений, транспорта и персонала фирмы	-	2	22
Итого:		6	10	128

6.2 Содержание лекционных занятий

Раздел 1.Основы теории информационной безопасности

Тема 1.Информационная безопасность как составная часть экономической безопасности предпринимательской деятельности

Понятие безопасности. Цели экономической безопасности. Концепция информационной безопасности России. Международные доктрины в области информационной безопасности. Соперничество в информационной сфере. Законодательство в области информационных ресурсов, продуктов и услуг (защита государственной, коммерческой и персональной информации). Безопасность функционирования предпринимательской структуры.

Тема 2. Основы информационной безопасности и защиты информации

Цели, задачи и практическая реализация информационной безопасности. Концепция защиты информации.

Тема 3.Информационные ресурсы. Защита открытых и закрытых информационных ресурсов

Понятие информационных ресурсов и информационных систем. Критерии оценки информационных ресурсов и классификация. Классификационные группы ценной предпринимательской информации. Понятие уязвимости. Классификация информационных продуктов и услуг. Документирование информации.

Тема 4. Источники конфиденциальной информации и каналы её утраты

Понятие и классификация источников конфиденциальной информации. Каналы распространения конфиденциальной информации. Понятие угрозы информации. Уязвимость информации и механизм реализации угроз. Классификация технических каналов утечки конфиденциальной информации.

Раздел 2.Особенности защиты информации в предпринимательской деятельности

Тема 5.Системы защиты информации: назначение, принципы и структура

Понятие, цели и задачи системы конфиденциальной информации. Принципы построения системы, её технологичность, иерархичность и факторы эффективности. Надежность системы. Вопросы применения компьютерных технологий. Сертификация средств защиты.

Тема 6. Регламентация работы систем защиты информации

Разработка и внедрение перечня сведений, составляющих предпринимательскую тайну. Ведение перечня на ЭВМ. Определение правил доступа к конфиденциальной информации. Цели и задачи разрешительной (разграничительной) системы. Протоколирование фактов доступа.

Виды служб безопасности (аналитические подразделения, подразделения пропускного режима, подразделение инженерно-технической защиты информации). Руководство и подчиненность. Менеджер по безопасности. Взаимодействие службы безопасности и службы персонала.

6.3 Содержание практических занятий

Раздел 2. Особенности защиты информации в предпринимательской деятельности

Тема 5. Системы защиты информации: назначение, принципы и структура

Понятие, цели и задачи системы конфиденциальной информации. Принципы построения системы, её технологичность, иерархичность и факторы эффективности. Надежность системы. Вопросы применения компьютерных технологий. Сертификация средств защиты.

Тема 6. Регламентация работы систем защиты информации

Разработка и внедрение перечня сведений, составляющих предпринимательскую тайну. Ведение перечня на ЭВМ. Определение правил доступа к конфиденциальной информации. Цели и задачи разрешительной (разграничительной) системы. Протоколирование фактов доступа.

Виды служб безопасности (аналитические подразделения, подразделения пропускного режима, подразделение инженерно-технической защиты информации). Руководство и подчиненность. Менеджер по безопасности. Взаимодействие службы безопасности и службы персонала.

Тема 7. Защищённый документооборот

Виды угроз и задачи защиты документопотоков. Критерии безопасности документооборота. Взаимосвязь документопотока и технологической системы обработки и хранения документов. Виды угроз со стороны технологической системы. Процедура изготовления конфиденциальных документов и ликвидация черновиков. Виды грифов и ограничительных отметок. Порядок работы персонала с конфиденциальными документами.

Тема 8. Защита информации в процессе публикаторской, рекламной и выставочной деятельности

Угрозы безопасности информации в процессе публикаторской, рекламной и выставочной деятельности. Анализ ценности информации.

Оформление разрешения на публикацию, издание рекламной продукции и демонстрацию технической документации и моделей.

Тема 9. Защита информации в компьютерах, локальных сетях и средствах связи

Состав действующих руководящих документов по защите информации в компьютерах, локальных сетях и средствах связи. Разграничение прав доступа. Сертификация оборудования. Технические средства пассивной и активной защиты. Программные продукты защиты информационных ресурсов. Криптография. Защита информации в Интернете.

Тема 10.Охрана территорий, зданий, помещений, транспорта и персонала фирмы

Угрозы безопасности собственности фирм и персоналу. Виды охраняемых объектов, категории защищаемых помещений. Построение систем охраны объектов. Технические средства охраны. Сигнализация, оповещение, идентификация и ограничения. Правила охраны транспортных средств и транспортируемой продукции. Действия персонала в типовых и чрезвычайных ситуациях.

6.4 Содержание самостоятельной работы студентов

Шифр СРС	Виды самостоятельной работы студентов (СРС)	Наименование и содержание	Трудоёмкость (часы)	Виды контроля СРС
С1	Углубленное изучение разделов, тем лекционного курса дисциплины	С1Р1 **Основы теории информационной безопасности** Т1 Информационная безопасность как составная часть экономической безопасности предпринимательской деятельности Т2 Основы информационной безопасности и защиты информации	5 5	Письменное домашнее задание Письменное домашнее задание

		Т3 Информационные ресурсы. Защита открытых и закрытых информационных ресурсов	9	Письменное домашнее задание
		Т4 Источники конфиденциальной информации и каналы её утраты	10	Письменное домашнее задание
		С1Р2**Особенности защиты информации в предпринимательской деятельности**		
		Т5 Системы защиты информации: назначение, принципы и структура	10	Письменное домашнее задание
		Т6 Регламентация работы систем защиты информации	10	Письменное домашнее задание
		Т7 Защищённый документооборот	10	Письменное домашнее задание
		Т8 Защита информации в процессе публикаторской, рекламной и выставочной деятельности	10	Письменное домашнее задание
		Т9Защита информации в компьютерах, локальных сетях и средствах связи	10	Письменное домашнее задание
		Т10 Охрана территорий, зданий, помещений, транспорта и персонала фирмы	10	Письменное домашнее задание
С3	Подготовка к аудиторным занятиям (семинарские занятия, текущий и рубежный контроль)	С3Р2 **Особенности защиты информации в предпринимательской деятельности**		
		Т5 Системы защиты информации: назначение, принципы и структура	5	Выступления в ходе семинарских занятий
		Т6 Регламентация работы систем защиты информации	5	Выступления в ходе семинарских занятий
		Т7Защищённый документооборот	5	Выступления в ходе семинарских занятий
		Т8 Защита информации в процессе публикаторской, рекламной и выставочной деятельности	5	Выступления в ходе семинарских занятий
		Т9Защита информации в компьютерах, локальных сетях и средствах связи	5	Выступления в ходе семинарских

		Т10 Охрана территорий, зданий, помещений, транспорта и персонала фирмы	5	занятий Выступления в ходе семинарских занятий
С5	Подготовка к промежуточной аттестации по дисциплине (экзамен)	С5Р1**Основы теории информационной безопасности** С5Р2**Особенности защиты информации в предпринимательской деятельности**	2 7	Компьютерное тестирование или устный экзамен
		Итого:	128	

7 Фонд оценочных средств

7.1 Оценочные средства

Темы рефератов:

1. Необходимость обеспечения безопасности в информационных системах.
2. Прогресс информационных технологий и информационная безопасность.
3. Нормативно-правовые аспекты информационной безопасности.
4. Классификация угроз безопасности информационных объектов.
5. Основные виды каналов утечки информации.
6. Умышленные и неумышленные угрозы информационной безопасности.
7. Внешние угрозы информационной безопасности.
8. Мотивы и цели компьютерных преступлений.
9. Статьи уголовного кодекса о компьютерных преступлениях.
10. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.
11. Объекты информационной безопасности на предприятии.
12. Организационные методы обеспечения информационной безопасности.
13. Физическая защита информационных систем.
14. Программно - технические методы обеспечения ИБ.
15. Идентификация и аутентификация.
16. Доктрина информационной безопасности Российской Федерации.

17. Государственное регулирование информационной безопасности в России.
18. Несанкционированный доступ и защита от него.
19. Проблема информационной безопасности в историческом аспекте.
20. Предупреждение компьютерных преступлений.
21. Типы компьютерных вирусов и защита от них.
22. Человеческие факторы, обуславливающие информационные угрозы.
23. Способы воздействия угроз на информационный объект.
24. Признаки воздействия вирусов на компьютерную систему.
25. Фрагментарный и системный подходы к защите информации.
26. Уголовно-правовая характеристика компьютерных преступлений.
27. Субъективная сторона компьютерных преступлений.
28. Объективная сторона компьютерных преступлений.
29. Способы совершения компьютерных преступлений («за хвост», «маскарад» и др.).
30. Причины и условия, способствующие совершению компьютерных преступлений.
31. Меры предупреждения преступлений в сфере компьютерной информации.
32. История вредоносных программ.
33. Защита учетной информации коммерческих фирм.
34. Свойства экономической информации, нарушаемые при несанкционированном доступе.
35. Исторические аспекты компьютерных преступлений.
36. Экономическая информация как объект безопасности.
37. Перечень сведений, которые не могут составлять коммерческую тайну.
38. Виды тайн и как их сохранить.
39. Причины разглашения конфиденциальной информации.
40. Разглашение и утечка информации.
41. Стратегия злоумышленника при несанкционированном доступе.

42. Организация конфиденциального делопроизводства.
43. Структура службы безопасности компании.
44. Теоретические аспекты информационной безопасности экономических систем.
45. Основные понятия информационной безопасности экономических систем.
46. Экономическая информация как товар и объект безопасности.
47. Понятия информационных угроз и их виды.
48. Вредоносные программы.
49. Компьютерные преступления и наказания.
50. Принципы построения системы информационной безопасности.
51. Подходы, принципы, методы и средства обеспечения безопасности.
52. Организационно-техническое обеспечение компьютерной безопасности.
53. Электронная цифровая подпись и особенности ее применения.
54. Защита информации в Интернете.
55. Организация системы защиты информации экономических систем.
56. Этапы построения системы защиты информации.
57. Политика безопасности.
58. Оценка эффективности инвестиций в информационную безопасность.
59. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).
60. Информационная безопасность электронной коммерции (ЭК).
61. Обеспечение компьютерной безопасности учетной информации.
62. Сущность криптографических методов.
63. Организационно-административные мероприятия обеспечения компьютерной безопасности.
64. Организация конфиденциального делопроизводства.
65. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения.
66. Типы и субъекты информационных угроз.

7.2 Контрольно-оценочные средства

Вопросы к экзамену:

1. Необходимость обеспечения безопасности в информационных системах.
2. Прогресс информационных технологий и информационная безопасность.
3. Нормативно-правовые аспекты информационной безопасности.
4. Классификация угроз безопасности информационных объектов.
5. Основные виды каналов утечки информации.
6. Умышленные и неумышленные угрозы информационной безопасности.
7. Внешние угрозы информационной безопасности.
8. Мотивы и цели компьютерных преступлений.
9. Статьи уголовного кодекса о компьютерных преступлениях.
10. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.
11. Объекты информационной безопасности на предприятии.
12. Организационные методы обеспечения информационной безопасности.
13. Физическая защита информационных систем.
14. Программно - технические методы обеспечения информационной безопасности.
15. Идентификация и аутентификация.
16. Доктрина информационной безопасности Российской Федерации.
17. Государственное регулирование информационной безопасности в России.
18. Несанкционированный доступ и защита от него.
19. Проблема информационной безопасности в историческом аспекте.
20. Предупреждение компьютерных преступлений.
21. Типы компьютерных вирусов и защита от них.
22. Человеческие факторы, обуславливающие информационные угрозы.
23. Способы воздействия угроз на информационный объект.
24. Признаки воздействия вирусов на компьютерную систему.
25. Фрагментарный и системный подходы к защите информации.
26. Уголовно-правовая характеристика компьютерных преступлений.

27. Субъективная сторона компьютерных преступлений.
28. Объективная сторона компьютерных преступлений.
29. Способы совершения компьютерных преступлений («за хвост», «маскарад» и др.).
30. Причины и условия, способствующие совершению компьютерных преступлений.
31. Меры предупреждения преступлений в сфере компьютерной информации.
32. История вредоносных программ.
33. Защита учетной информации коммерческих фирм.
34. Свойства экономической информации, нарушаемые при несанкционированном доступе.
35. Исторические аспекты компьютерных преступлений.
36. Экономическая информация как объект безопасности.
37. Перечень сведений, которые не могут составлять коммерческую тайну.
38. Виды тайн и как их сохранить.
39. Причины разглашения конфиденциальной информации.
40. Разглашение и утечка информации.
41. Стратегия злоумышленника при несанкционированном доступе.
42. Организация конфиденциального делопроизводства.
43. Структура службы безопасности компании.
44. Теоретические аспекты информационной безопасности экономических систем.
45. Основные понятия информационной безопасности экономических систем.
46. Экономическая информация как товар и объект безопасности.
47. Понятия информационных угроз и их виды.
48. Вредоносные программы.
49. Компьютерные преступления и наказания.

50. Принципы построения системы информационной безопасности.
51. Подходы, принципы, методы и средства обеспечения безопасности.
52. Организационно - техническое обеспечение компьютерной безопасности.
53. Электронная цифровая подпись и особенности ее применения.
54. Защита информации в Интернете.
55. Организация системы защиты информации экономических систем.
56. Этапы построения системы защиты информации.
57. Политика безопасности.
58. Оценка эффективности инвестиций в информационную безопасность.
59. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).
60. Информационная безопасность электронной коммерции (ЭК).
61. Обеспечение компьютерной безопасности учетной информации.
62. Сущность криптографических методов.
63. Организационно-административные мероприятия обеспечения компьютерной безопасности.
64. Организация конфиденциального делопроизводства.
65. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения.
66. Типы и субъекты информационных угроз.

Критерии определения оценок на экзаменах (зачётах).

1. Оценка «отлично».

Оценка «отлично» ставится студенту, ответ которого содержит:

- глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
- знание концептуально-понятийного аппарата всего курса;
- знание монографической литературы по курсу свидетельствует о способности: самостоятельно критически оценивать основные положения курса и увязывать теорию с практикой.

Оценка «отлично» не ставится в случаях систематических пропусков студентом семинарских и лекционных занятий по неуважительным причинам, отсутствия активного участия на семинарских занятиях, а также неправильных ответов на дополнительные вопросы преподавателя.

2. Оценка «хорошо».

Оценка «хорошо» ставится студенту, ответ которого свидетельствует:

- о полном знании материала по программе;
- о знании рекомендованной литературы, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «хорошо» не ставится в случаях пропусков студентом семинарских и лекционных занятий по неуважительным причинам.

3. Оценка «удовлетворительно» ставится студенту, ответ которого содержит:

- поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии курса;
- стремление логически чётко построить ответ, свидетельствует о возможности последующего обучения.

4. Оценки «неудовлетворительно» и «не зачтено» ставятся студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

8 Образовательные технологии

Шифр раздела, темы дисциплины	Наименование раздела, темы дисциплины	Активные и интерактивные методы и формы обучения	Трудоёмкость, часы (кол-во часов по разделу (теме), отводимое на занятия в интерактивной форме
Р2	**Особенная часть** Т7Защищённый документооборот Т8Защита информации в процессе публикаторской, рекламной и выставочной деятельности Т9Защита информации в компьютерах, локальных сетях и средствах связи	Оформление необходимой документации в соответствии с действующими нормативными требованиями Работа в компьютерных классах	1 1 2
Интерактивных занятий от объёма аудиторных занятий			25%

9 Учебно-методическое обеспечение дисциплины

9.1Учебные издания:

1. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — Электрон.текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 c. — 978-5-238-02857-6. — Режим доступа: http://www.iprbookshop.ru/72444.html

9.2Программное обеспечение, Интернет-ресурсы, электронные библиотечные системы

1. Электронная библиотечная система «Университетская библиотека online»: www.biblioclub.ru.

2. Электронный учебник «Информационное право»/ О.А. Городов. М.: КНОРУС, 2009 г.

3. Справочные правовые системы «Консультант плюс» и «Гарант».

4. www.info-protect.ru;

5. http://portal.tusur.ru;

6. http://www.sduto.ru;

7. http://www.radiostancii.ru;

8. http://www.intuit.ru;

9. www.securitylab.ru;

10. http://runtex.ru;

11.www.wired.com;

12. http://virusov-net.info.

10 Материально-техническое обеспечение дисциплины

1. Электронные учебники.

2. Аудиовизуальные средства: презентации на цифровых носителях.

3. Компьютеры.

4. Мультимедиапроектор.