МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.09
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Международные и российские нормативные акты и стандарты по информационной безопасности

(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость:4 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	**8**	**Итого**
Форма контроля **Вид занятий**	**зачет**	
Лекции	16	16
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,25	0,25
Контактная работа	48,25	48,25
Самостоятельная работа	95,75	95,75
Контроль		
Итого	**144**	**144**

Рабочую программу составил(и):

Басацкий Василий Васильевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☒ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Цель освоения дисциплины – изучение международного и российского законодательства в области информации и информационной безопасности. Слушатели курса познакомятся с международными и российскими нормативными актами, и стандартами по информационной безопасности, изучат структуру законодательства, основы стандартизации и метрологии в ИБ, сертификация в области защиты информации.

Для достижения указанной цели предлагается решение следующих задач:

- изучить международную и отечественную нормативно-правовую базу,
- усвоить стандарты и требования сертификации в области обеспечения информационной безопасности;
- изучить структуру законодательства, основы стандартизации и метрологии в ИБ;
- получить практические навыки участия в анализе и разработке стандартов, норм и правил, а также технической документации, связанной с ИБ
-

.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Основы информационной безопасности;
- Комплексная безопасность

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:

- Обеспечение безопасности критической информационной инфраструктуры;
- Аудит защищенности информационных систем

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-10 Способен осуществлять моделирование решений по реализации программного обеспечения и управлению БД	ПК-10.1 Использует знания стандартов ИБ и НПА	Знать: - роль стандартов и спецификаций; - основные понятия и идеи, изложенные в стандартах в области информационной безопасности
		Уметь: - применять основные требования международных и российских нормативных правовых актов в области обеспечения информационной безопасности - использовать утвержденные в нормативных правовых актах и методических документах формы документации
		Владеть: - основами ИБ:

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		- навыками работы с нормативными правовыми актами
	ПК-10.2 Умеет применить рекомендации стандартов в практической деятельности	Знать: - Госты, стандарты по ИБ; - технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами
		Уметь: - применить рекомендации стандартов в практической деятельности; - проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов
		Владеть: - профессиональной терминологией
	ПК-10.3 Владеет методами управления ИБ в соответствии с лучшими практиками	Знать: - основы управления ИБ
		Уметь: - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
		Владеть: - методами управления ИБ в соответствии с лучшими практиками

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности. Раздел 1 Международная нормативно-правовая база	Лек,	Тема 1. Международная нормативно-правовая база в области обеспечения информационной безопасности. 1.1 Информационная безопасность. Нормативные определения 1.2. Международные нормативные правовые акты 1.3. Конвенция Совета Европы 1.4. Окинавская «Хартия глобального информационного общества»	8	2 ч (л)		-	
Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности. Раздел 1 Международная нормативно-правовая база	Пр,	Тема 2 Стратегии развития информационного общества (мировое пространство) 2.1. Определите цели, задачи и меры по реализации внутренней и внешней политики стран в сфере применения информационных и коммуникационных технологий.		2			Отчет по практическому занятию №1

Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности. Раздел 1 Международная нормативно-правовая база	Лекция	Тема 3 Основные угрозы международной кибербезопасности 3.1.Использование ИКТ в военно-политических и иных сферах 3.2. Использование ИКТ в террористических и экстремистских целях 3.3 Использование ИКТ в преступных целях для проведения компьютерных атак на информационные ресурсы государства. 3.4.Использование государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка ИКТ		2			
Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности. Раздел 1 Международная нормативно-правовая база	Практич	Тема 4. Основные угрозы международной кибербезопасности. Меры профилактики и защиты. 4.1. Проанализировать основные угрозы и риски международной кибербезопасности. 4.2. Разработать рекомендации и предложения по преодолению рисков и угроз международной кибербезопасности		2			Отчет по практическому занятию №2

Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности. Раздел 1 Международная нормативно-правовая база	Практич	Тема 5. Основы государственной политики в сфере международной информационной безопасности 4.1. Проанализировать российские подходы к формированию системы обеспечения международной информационной безопасности 4.2. Продумать инициативы в сфере международной ИБ, содействующие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве		2			Отчет по практическому занятию №3
Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности. Раздел 1 Международная нормативно-правовая база	Практич	Тема 6 Уголовная и административная ответственность за нарушения в области кибербезопасности и нарушении требований по защите информации 6.1. Определить вид ответственности за нарушение требований по защите информации (уголовная, гражданско-правовая, административная, дисциплинарная (решение кейсов) Например, Кейс: Работая в должности системного администратора, работник имел доступ к программе 1С Трудовой договор предусматривал обязанность не разглашать сведения, касающиеся системы, условий и размеров оплаты труда в компании. Работник был ознакомлен с локальными		2			Отчет по практическому занятию №4

		нормативными правовыми актами работодателя, в частности, касающимися обработки персональных данных. Системный администратор стал распространять среди других сотрудников информацию о повышении заработной платы одного из менеджеров компании, полученную из 1С 6.2 Директива по безопасности информационных систем и сетей ОЭСР 2002 г. «К культуре безопасности» ОЭСР и принципы операционного риска Банка международных расчетов (Basel II)		18 (4л+8пр+6ср)			
Модуль 1 Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности Раздел 2 Национальная нормативная база РФ в области информационной безопасности. Законодательство Российской Федерации в области информации и информационной безопасности	Лек,	Тема 7. Структура и состав информационного законодательства РФ. 7.1.Нормативное регулирование в сфере ИБ 7.2.Состав законодательства по обеспечению ИБ (федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации 7.3. Наиболее значимых нормативных правовые актов в области обеспечения ИБ Тема 8. Международные договоры	8	2 2		-	

	Лек	РФ по обеспечению ИБ 8.1. Билатеральные международные договоры в сфере ИБ (Республика Беларусь, Республика Куба, Китайская Народная Республоика,) 8.2. Екатеринбургское Соглашение ШОС, Соглашение Россия-Китай		2			
	Лек	Тема 9 Законодательство в области ИБ 9.1.Конституция РФ, федеральные законы и кодексы в области информационной безопасности. 9.2.Указы Президента РФ, 9.3.Постановления Правительства РФ об информационной безопасности.		2			
	Практич	Тема 10.. ИБ и правовая защита информации 10.1. Составление классификационной схемы понятий в области «Защита информации» 10.2. Определить источники правовой информации:сайты органов власти, справочно-правовые системы		2			Отчет по практическому занятию № 5
	Практич	Тема 11. Система нормативно-правового регулирования ИБ: Конституция РФ и международные акты. 11.1 Определите баланс между тайной частной жизни и свободой информации, опираясь на систему нормативно-правового					Отчет по практическому занятию № 6

		регулирования ИБ (эссе) В КоАП					
	Практич	Тема 12 Система нормативно-правового регулирования ИБ: федеральное законодательство 12.1.Положения о защите информации в ГК (гражданском кодексе) 12.2. Положения о защите информации в ТК (трудовом кодексе) 12.3. Положения о защите информации в КоАП РФ(кодекс об административных правонарушениях). 12.4 Положения о защите информации в УК РФ 12.5.Основные федеральные законы в области защиты информации Решение кейсов: какие положения нарушены в данной ситуации?		4			Отчет по практическому занятию № 7
	Практич	Тема 13.Нормативно-правовая база Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по информационной безопасности. 13.1. Стратегия национальной безопасности РФ Перечислите факторы, влияющие на ИБ (в рамках стратегии ИБ РФ)		2			Отчет по практическому занятию № 8

	Практич	13.2. Каковы задачи в области ИБ 13.3. Сертификация в рамках ФСБ Тема 14. Нормативно-правовая база других Министерств, ведомств и служб РФ в области защиты информации (МО РФ, ФСО России, МВД РФ 14.1. Составьте список нормативно- правовых документов Министерств и ведомств, служб РФ в области защиты информации(МО РФ, ФСО России, МВД РФ)		2 26 (6л+12пр+8ср)			Отчет по практическому занятию № 9
Модуль 1 Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности Раздел 3 Общие сведения о стандартизации, сертификации и метрологии	Лек, Практич	Тема 15. Лицензирование деятельности в области защиты информации 15.1 Основные нормативные правовые акты в области Лицензирования 15.2. Лицензия. Действие лицензии. Субъекты лицензирования. Лицензионные требования. 15.3. Виды работ и услуг, подлежащих лицензированию в ТЗКИ Тема 16. Сертификация средств защиты информации 16.1.Составьте табоицу, в которой перечислите федеральные законы в области сертификации, Постановления правительства и Ведомственные нормативные акты 16.2. Обязательная и добровольная	8	2 2			Отчет по практическому занятию №10

	Практич	сертификация СЗИ. Когда нужно сертифицировать СЗИ? Назовите средства, подлежащие сертификации 16.3. Сертификация в рамках ФСТЭК Назовите реестры ФСТЭК Опишите программу и методику сертификационных испытаний. Тема 17. Аттестация объектов информатизации по требованиям безопасности информации. 17.1. Действующие ГОСТы в области аттестации объектов информатизации (анализ действующих ГОСТов) 17.2. Обязательность аттестации. Требования документов. Перечислите и охарактеризуйте перечень работ по аттестации, основные этапы аттестации объектов информатизации. 17.3 Продумайте мероприятия и работы в рамках аттестационных испытаний: оценка документов. 17.4. Продумайте мероприятия и работы в рамках аттестационных испытаний: оценка работников 17.5. Продумайте мероприятия и работы в рамках аттестационных испытаний:защита от НСД		2 10 (2+4+4)			Отчет по практическому занятию №11
			Итого:	**54**			

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 2 Международные и национальные стандарты по информационной безопасности	Лек,	Тема 18 Международные стандарты в сфере ИБ: 18.1. Стандарты BS 7799-1:2005, BS 7799-2:2005, BS 7799- 3:2006 (построения СУИБ). 18.2.Стандарты ISO/IEC 17799:2005, ISO/IEC 27000, ISO/IEC 27001:2005, ISO/IEC 27002, ISO/IEC 27005. DOD, TCSEC (оранжевая книга) США, GreenBook Германия, WhiteBook (ITSEC) и другие стандарты по информационной безопасности.	8	4		-	
	Практич	Тема 18 Международные стандарты в сфере ИБ 18.3. Проанализируйте набор стандартов PCI DSS (Payment Card Industry Data Security Standard) — стандарты безопасности данных индустрии платежных карт. Разработайте на их основе рекомендации пользователю платежных карт 18.4. Проанализируйте стандарт PA-DSS – стандарт безопасности данных платежных приложений. Разработайте на их основе рекомендации пользователю		4			Отчет по практическому занятию №12

		платежных приложений		18 (4 л+4пр+10 ср)			
Модуль 2 Тема 2.2. Национальные стандарты по информационной безопасности.	Лек, Практич Лекция	Тема 19..Национальные стандарты РФ (ГОСТы) информационной безопасности. 19.1. Защита информации (ГОСТ Р 56103-2014 ГОСТ Р 58189-2018) 19.2 Безопасность финансовых (банковских операций (ГОСТ Р 57580.1-2017) 19.3.Мониторинг и прогнозирование поведения людей (ГОСТ Р 58776-2019) Тема 20. .Национальные стандарты РФ ГОСТ Р ИСО/МЭК по информационной безопасности. 20.1.Осуществить анализ ГОСТов на аналогичность международным стандартам Р ИСО/МЭК Тема 21 Обновление национальных стандартов ИСО/МЭК 21.1. ГОСТы в области информационных технологий. Анализ ГОСТов (ГОСТ Р 59343-2021 ГОСТ Р 59346-2021 ГОСТ Р 59352-2021 ГОСТ Р 59356-2021 ГОСТ Р 59381-2021 ГОСТ Р 59382-2021 ГОСТ Р 59383-2021) 21.2. Анализ ГОСТов (ГОСТ Р 59407-2021 ГОСТ	8	4 2 2		-	Отчет по практическому занятию №13

		Р 59494-2021 ГОСТ Р 59502-2021 ГОСТ Р 59503-2021 ГОСТ Р 59515-2021 ГОСТ Р 59516-2021)					
	Лекция	Тема 22. Система нормативно-правового регулирования ИБ: локальные акты. 22.1 Локальные нормативные правовые акты организации в области защиты детей от информации, причиняющей вред их здоровью и (или) развитию (ФЗ от 29.12.2010 N 436-ФЗ). 22.2. Анализ квалификационного справочника должностей руководителей, специалистов и других служащих		2			
	Практич	22.3.Подготовьте примерный перечень локальных нормативных правовых актов организации в сфере информационной безопасности: обязательных и факультативных		2			Отчет по практическому занятию №14
	Практич	22.4.Квалификационные характеристики должностей по ИБ Подготовьте квалификационные характеристики должностей руководителей (специалистов) по обеспечению безопасности информации, в ключевых системах информационной инфраструктуры		4			Отчет по практическому занятию №15

	Практич	противодействию техническим разведкам и технической защите информации 22.5 Профстандарты и должностные обязанности-На основании профстандартов подготовьте квалификационные характеристики и должностные обязанности: - специалиста по автоматизации информационно-аналитической деятельности в сфере ИБ; - специалиста по безопасности компьютерных систем и сетей; - специалиста по защите информации в автоматизированных системах; - специалист по защите информации в телекоммуникационных системах и сетях; - специалист по технической защите информации		6			Отчет по практическому занятию №16
	Практич.	Тема 23.Стандарт Центробанка России «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения». 23.1.Департамент безопасности ЦБ 23.2.Профиль защиты ЦБ 23.3.Проанализируйте		6 36 (8л+20пр+8ср)			Отчет по практическому занятию №17

		требования к ИБ банка. Подготовьте свои рекомендации к ИБ банка					
	ПА		8	0,25		-	Вопросы к зачету Итоговый тест
			Итого:	**90**			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
8	ПК-10.1 , ПК-10.2 ПК-10.3	Протоколы практических заданий №1-17
		Вопросы к зачету №№1-80 Банк тестовых заданий 1-350

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

Типовые тестовые задания

При изучении дисциплины используются 4 теста (3 теста в Модуле 1, 1 тест – в Модуле 2); тестовые задания – открытого и закрытого типа. Каждое тестовое задание включает вопрос и несколько вариантов ответов к нему либо предполагает вписывание правильного словосочетания, термина, даты и т.п. в текст тестового вопроса

Тестирование выполняется в письменной форме или в виде on-line-тестирования во время практических занятий по результату изучения теоретического материала. Критерии оценки каждого теста различны (баллы за тесты приводятся в конце каждого теста ниже).

Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности

Тест 1. «Правовое нормативное регулирование деятельности в области информационной безопасности и защиты информации РФ» Внесите информацию в пустые поля (заполните пропуски данными, словами или фразами):

1. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О _____ отдельных видов деятельности».
2. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об _____подписи».
3. Федеральный закон от 28 декабря 2010 г. № _____ФЗ «О безопасности».
4. Федеральный закон от 27 июля _____г. № 152-ФЗ «О персональных данных».
5. Федеральный закон от 27 июля _____г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Критерий оценивания Теста № 1: 30 вопросов – до 9 баллов (1 правильно сделанный вопрос теста = 0,3 балла)

Тест 2. Нормативная международная и отечественная база по защите информации

Внесите информацию в пустые поля в названиях нормативных документов:.

1. «_____ требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по _____ каналам». Гостехкомиссия России. - М., 2002.

3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические _____. Госстандарт России. - М., 1995.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие _____. Госстандарт России. - М., 2006.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и _____. - М., 2006. 18 и т.д.

Критерий оценивания Теста № 2: 40 вопросов – до 12 баллов (1 правильно сделанный вопрос теста = 0,3 балла)

Тест 3. Отечественные нормативные документы в области криптографической защиты

1. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № ____ «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

2. Приказ ФСБ России от _____ июля _____ г. № _____ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

3. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки _____ . Защита криптографическая. Алгоритм криптографического преобразования.

4. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. _____ защита информации. Процессы формирования и проверки электронной цифровой подписи.

5. ГОСТ Р 34.10-_____ Государственный стандарт Российской Федерации. Информационная технология. _____ защита информации. Процессы формирования и проверки электронной цифровой подписи. и т.д.

Критерий оценивания Теста № 3: 10 вопросов – до 4 баллов (1 правильно сделанный вопрос теста = 0,4 балла)

Модуль 2. Международные и национальные стандарты по информационной безопасности

Итоговый тест № 4

1 Уровень безопасности С, согласно "Оранжевой книге", характеризуется:

а. произвольным управлением доступом

б. принудительным управлением доступом

в. верифицируемой безопасностью

2. Согласно стандарту Х.700, в число функций управления безопасностью входят:

а. создание инцидентов

б. реагирование на инциденты в. устранение инцидентов

3. Согласно рекомендациям Х.800, выделяются следующие сервисы безопасности:

а. аутентификация

б. идентификация

в. туннелирование

4 Т.н. стандарт информационной безопасности «Общие критерии» содержит следующие виды требований:

а. функциональные

б. доверия безопасности

в. экономической целесообразности

5. В число классов функциональных требований "Общих критериев" входят:

а. анонимность

б. приватность

в. связь и т.д.

Критерий оценивания Теста № 4: 20 вопросов – до 5 баллов (1 правильно сделанный вопрос теста = 0,25 балла).

7.2.3. Выполнение практических заданий

Темы Практических и семинарских занятий

№	Тема
1	Стратегии развития информационного общества (мировое пространство)
2	Основные угрозы международной кибербезопасности. Меры профилактики и защиты.
3	Основы государственной политики в сфере международной информационной безопасности
4	Уголовная и административная ответственность за нарушения в области кибербезопасности и нарушении требований по защите информации
5	ИБ и правовая защита информации
6	Система нормативно-правового регулирования ИБ: Конституция РФ и международные акты.
7	Система нрмативно-правового регулирования ИБ: федеральное законодательство
8	Нормативно-правовая база Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по информационной

	безопасности.
9	Нормативно-правовая база других Министерств, ведомств и служб РФ в области защиты информации (МО РФ, ФСО России, МВД РФ
10	Сертификация средств защиты информации
11	Аттестация объектов информатизации по требованиям безопасности информации.
12	Международные стандарты в сфере ИБ
13	Национальные стандарты РФ (ГОСТы) информационной безопасности.
14	Система нормативно-правового регулирования ИБ: локальные акты.
15	Квалификационные характеристики должностей руководителей (специалистов) по обеспечению безопасности информации
16	Профстандарты и должностные обязанности
17	Стандарт Центробанка России «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения

Методические указания по выполнению итоговой практической работы

Для предприятия, выбранного согласно вашему варианту (вариант определяется по последней цифре зачетной книжки студента), следует составить список нормативных правовых актов и стандартов, которыми необходимо руководствоваться при построении комплексной системы защиты информации предприятия.

К каждому документу представить комментарий, указывающий обязательный или рекомендательный характер документа, основное содержание документа, область применения документа для рассматриваемого вами предприятия.

Примерные варианты тем самостоятельной контрольной работы (КСР)

1. факультет университета;
2. филиал банка;
3. небольшое торговое предприятие;
4. поликлиника;
5. больница;
6. железнодорожная станция;
7. школа;
8. библиотека;
9. юридическая фирма;
10. фирма по разработке программного обеспечения.

Отчет оформите с титульным листом по принятым в России ГОСТам оформления научно-исследовательских работ, с указанием вуза, кафедры, специальности, дисциплины, варианта, года и т.д.

Приложите Оглавление (2-й лист отчета), Введение (с постановкой задач и описанием заданий), Вывод и Список использованных источников. Отчет должен быть зарегистрирован в учебной части и сдан для проверки преподавателю на кафедру ……. за несколько недель или дней до сессии.

Критерии и методика оценивания самостоятельной контрольной работы:

- 5 баллов студент получает, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение прикладными программами.

- 4 балла студент получает за самостоятельную контрольную работу, если она выполнена в полном объеме, но имеет один из недостатков:

- в работе допущены один-два недочета при освещении основного содержания ответа;

- нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла и менее студент получает, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков (пропорционально количеству недочетов, ошибок, пробелов в знаниях).

Оценочные баллы выставляются по результату защиты КСР на предпоследнем практическом занятии.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

№ п/п	Вопросы к зачету
1.	Определение информационной безопасности
2.	Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
3.	Порядок проведения лицензирования и контроля за деятельностью лицензиатов
4.	Получение информации из открытых источников
5.	Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
6.	Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
7.	Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.
8.	Сертификат соответствия. Опишите документ. Какие признаки в СС указывают на его подлинность или нед
9.	Маркировка сертифицированной продукции.
10.	Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов».
11.	Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно- розыскной деятельности».
12.	Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».
13.	Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
14.	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

15.	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
16.	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
17.	Доктрина информационной безопасности Российской Федерации
18.	Понятие и виды информации, защищаемой законодательством Российской Федерации
19.	Международная нормативно-правовая база в области обеспечения информационной безопасности.
20.	Нормативно-правовая база Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по информационной безопасности
21.	Нормативно-правовая база ФСБ, других Министерств, ведомств и служб РФ в области защиты информации (МО РФ, ФСО России, МВД РФ, Минкомсвязи РФ, Роскомнадзора и др.
22.	Стандарт Центробанка России от 01.06.2014 г. «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения» (СТО БР ИББС-1.0–2014)
23.	Использование грифов секретности.
24.	Окинавская «Хартия глобального информационного общества»;
25.	Директива по безопасности информационных систем и сетей ОЭСР 2002 г. «К культуре безопасности» ОЭСР и принципы операционного риска Банка междун
26.	Стандарты ISO/IEC 17799:2005, ISO/IEC 27000, ISO/IEC 27001:2005, ISO/IEC 27002, ISO/IEC 27005;
27.	Стандарты DOD , TCSEC (оранжевая книга) США, GreenBook Германия, WhiteBook (ITSEC).
28.	Закон о «О техническом регулировании»
29.	Сертификация в области защиты информации (обязательная и добровольная)
30.	Закон о «О лицензировании отдельных видов деятельности
31.	Структура и состав информационного законодательства РФ
32.	Международные договоры РФ,
33.	Основы стандартизации и метрологии в ИБ.
34.	Сертификация в области защиты информации
35.	Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
36.	Получение информации из открытых источников
37.	Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
38.	Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?

39.	Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.
40.	Сертификат соответствия. Опишите документ. Какие признаки в СС указывают на его подлинность или нед
41.	Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
42.	Порядок проведения лицензирования и контроля за деятельностью лицензиатов
43.	Получение информации из открытых источников
44.	Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
45.	Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
46.	Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.
47.	Сертификат соответствия. Опишите документ. Какие признаки в СС указывают на его подлинность или нед
48.	Маркировка сертифицированной продукции.
49.	Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
50.	Порядок проведения лицензирования и контроля за деятельностью лицензиатов
51.	Получение информации из открытых источников
52.	Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
53.	Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
54.	Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.
55.	Сертификат соответствия. Опишите документ. Какие признаки в СС указывают на его подлинность или нед
56.	Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
57.	Порядок проведения лицензирования и контроля за деятельностью лицензиатов
58.	Получение информации из открытых источников
59.	Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
60.	Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
61.	Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных

	(криптографических) средств.
62.	Сертификат соответствия. Опишите документ. Какие признаки в СС указывают на его подлинность или нед
63.	Маркировка сертифицированной продукции.
64.	Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
65.	Порядок проведения лицензирования и контроля за деятельностью лицензиатов
66.	Получение информации из открытых источников
67.	Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
68.	Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
69.	Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
70	Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.
71.	Сертификат соответствия. Опишите документ. Какие признаки в СС указывают на его подлинность или нед
72.	Маркировка сертифицированной продукции.
73	РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»
74	Классы защищенности АС от НСД к информации. Требования по защите информации от НСД для АС.
75	Классы защищенности СВТ и МЭ. Показатели защищенности СВТ;
76	Национальные стандарты РФ ГОСТ-ИСО/МЭК по информационной безопасности
77	ГОСТ Р ИСО/МЭК 15408-2002. Профиль защиты и задание по безопасности
78	ГОСТ Р ИСО/МЭК 15408-2002. Функциональные требования безопасности
79	ГОСТ Р ИСО/МЭК 15408-2002. Оценочные уровни доверия.
80	ГОСТ Р ИСО/МЭК 15408-2002. Область применения документа, краткий обзор

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
8	Зачет (письменно/по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Фот Ю.Д.	Стандарты информационной безопасности	Учебное пособие	2020	https://e.lanbook.com/book/159804
2	Прохорова Ю.В.	Информационная безопасность и защита информации	**Учебник**	2023	https://e.lanbook.com/book/293009

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Моргунов, А. В.	Информационная безопасность : учебно-методическое пособие : [16+] /	учебно-методическое пособие	2019	URL: https://biblioclub.ru/index.php?

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
					page=book&id=576726 (дата обращения: 18.08.2022)

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. www.fstec.ru –сайт ФСТЭК России
5. www.fsb.ru – сайт ФСБ России
6. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
7. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
8. www.newlibrary.ru – Новая электронная библиотека;
9. www. edu.ru – Федеральный портал российского образования;
10. www.elibrary.ru – Научная электронная библиотека;
11. www.nehudlit.ru – Электронная библиотека учебных материалов.
12. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
13. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

8.3. Перечень профессиональных баз данных и информационных справочных систем

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

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

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. УЛК -310	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф