

Программу составил(и):

к.т.н., доцент, Капустин С.А.

Рецензент(ы):

д.т.н., профессор, профессор кафедры информационных систем и программирования КубГТУ, Видовский Л.А.; директор ООО «ИС-КОНСОЛЬ», Суриков А.И.

Рабочая программа дисциплины

Информационная безопасность

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 38.03.02 Менеджмент (приказ Минобрнауки России от 12.08.2020 г. № 970)

составлена на основании учебного плана:

38.03.02 Менеджмент

утвержденного учёным советом вуза от 17.04.2023 протокол № 9.

Рабочая программа одобрена на заседании кафедры

Кафедра математики и вычислительной техники

Протокол от 11.12.2023 г. № 5

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 9 от 17.04.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	приобретение обучающимися знаний, навыков и умений, связанных с правовыми и программно-техническими методами защиты информации государственных и негосударственных организаций и учреждений
<p>Задачи: систематизация теоретических знаний по обеспечению безопасности информации в системах управления, использующих современные информационные технологии;</p> <p>выявление сущности, целей, задач и места методов и средств защиты информационных процессов в компьютерных системах в общей системе обеспечения безопасности информации на объектах информатизации;</p> <p>изучение основных принципов применения методов и средств защиты информации при организации защиты информационных процессов в компьютерных системах;</p> <p>изучение нормативно-руководящих документов, регламентирующих вопросы обеспечения безопасности информации в автоматизированных системах</p>	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Информатика
2.1.2	Основы национальной безопасности
2.1.3	Информационные технологии и интеллектуальные системы в менеджменте
2.1.4	Управление рисками
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Исследование систем управления
2.2.2	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ПК-5: Способен осуществлять процессы планирования, разработки перспективных планов, стандартов и других организационно-распорядительных документов организации и её подразделений	
ПК-5.1: Разрабатывает организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля	
Знать	
Уровень 1	Как разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 2	Как разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Уровень 3	Как разрабатывать перспективные годовые и оперативные планы работы
Уметь	
Уровень 1	Разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 2	Разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Уровень 3	Разрабатывать перспективные годовые и оперативные планы работы
Владеть	
Уровень 1	Умениями разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 2	Умениями разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Уровень 3	Умениями разрабатывать перспективные годовые и оперативные планы работы
ПК-5.2: Разрабатывает внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля	
Знать	
Уровень 1	Как разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Уровень 2	Как разрабатывать перспективные годовые и оперативные планы работы
Уровень 3	Как разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уметь	
Уровень 1	Разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Уровень 2	Разрабатывать перспективные годовые и оперативные планы работы

Уровень 3	Разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Владеть	
Уровень 1	Умениями разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Уровень 2	Умениями разрабатывать перспективные годовые и оперативные планы работы
Уровень 3	Умениями разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
ПК-5.3: Разрабатывает перспективные годовые и оперативные планы работы	
Знать	
Уровень 1	Как разрабатывать перспективные годовые и оперативные планы работы
Уровень 2	Как разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 3	Как разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Уметь	
Уровень 1	Разрабатывать перспективные годовые и оперативные планы работы
Уровень 2	Разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 3	Разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
Владеть	
Уровень 1	Умениями разрабатывать перспективные годовые и оперативные планы работы
Уровень 2	Умениями разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 3	Умениями разрабатывать внутренние стандарты и требования профессиональной этики, современные методики проведения внутреннего контроля
ПК-5.4: Способен использовать информационные технологии и соблюдать требования информационной безопасности при разработке перспективных планов, стандартов и других организационно-распорядительных документов организации и её подразделений	
Знать	
Уровень 1	Как использовать информационные технологии и соблюдать требования информационной безопасности при разработке перспективных планов, стандартов и других организационно-распорядительных документов организации и её подразделений
Уровень 2	Как разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 3	Как разрабатывать перспективные годовые и оперативные планы работы
Уметь	
Уровень 1	Использовать информационные технологии и соблюдать требования информационной безопасности при разработке перспективных планов, стандартов и других организационно-распорядительных документов организации и её подразделений
Уровень 2	Разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 3	Разрабатывать перспективные годовые и оперативные планы работы
Владеть	
Уровень 1	Умениями использования информационных технологий и соблюдать требования информационной безопасности при разработке перспективных планов, стандартов и других организационно-распорядительных документов организации и её подразделений
Уровень 2	Умениями разрабатывать организационно-распорядительные приказы, способствующие повышению эффективности работы структурного подразделения внутреннего контроля
Уровень 3	Умениями разрабатывать перспективные годовые и оперативные планы работы
ПК-6: Способен составлять итоговые документы по результатам деятельности подразделений организации и представлять их руководству организации	
ПК-6.1: Формирует завершающие документы в соответствии с нормативной базой экономического субъекта, с внутренними регламентами, отражающие фактически проведенную работу структурного подразделения внутреннего контроля	
Знать	
Уровень 1	Как формировать завершающие документы в соответствии с нормативной базой экономического субъекта, с внутренними регламентами, отражающие фактически проведенную работу структурного подразделения

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Информационная безопасность в системе национальной безопасности России					
1.1	Доктрина информационной безопасности Российской Федерации Основы информационной безопасности /Лек/	7	4	ПК-5.1 ПК-5.4 ПК-6.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.2	Государственная политика в области обеспечения безопасности автоматизированных систем управления Государственная политика Российской Федерации в области международной информационной безопасности Защита персональных данных Защита Государственной тайны /Пр/	7	10	ПК-5.2 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.3	Государственная политика в области обеспечения безопасности автоматизированных систем управления Государственная политика Российской Федерации в области международной информационной безопасности Защита персональных данных Защита Государственной тайны /Ср/	7	5	ПК-5.3 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 2. Информационная война, методы и средства ее ведения					
2.1	Методы и средства ведения информационной войны /Лек/	7	2	ПК-5.1 ПК-5.4 ПК-6.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.2	Сетецентрические войны Фейки /Пр/	7	4	ПК-5.2 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
2.3	Сетецентрические войны Фейки /Ср/	7	1	ПК-5.3 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
	Раздел 3. Критерии защищенности компьютерных систем					
3.1	Стандарты информационной безопасности /Лек/	7	2	ПК-5.1 ПК-5.4 ПК-6.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
3.2	Угрозы безопасности информации Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики /Пр/	7	4	ПК-5.2 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

3.3	Угрозы безопасности информации Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики /Ср/	7	4,4	ПК-5.3 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
	Раздел 4. Защита информации, обрабатываемой в информационных системах				
4.1	Защита информации в ГИС Защита информации в КИИ /Лек/	7	4	ПК-5.1 ПК-5.4 ПК-6.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
4.2	Работа со средствами защиты информации /Пр/	7	10	ПК-5.2 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
4.3	Программно-аппаратная защита информации /Ср/	7	3	ПК-5.3 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
	Раздел 5. Защита АС и СВТ от внешнего электромагнитного воздействия				
5.1	Защита АС и СВТ от внешнего электромагнитного воздействия /Лек/	7	2	ПК-5.1 ПК-5.4 ПК-6.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
5.2	Требования руководящих документов по защите от ПЭМИН /Пр/	7	4	ПК-5.2 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
5.3	Методы защиты информации от утечки через ПЭМИН /Ср/	7	8,4	ПК-5.3 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
	Раздел 6. Заключение				
6.1	DLP-системы. Заключение. /Лек/	7	2	ПК-5.1 ПК-5.4 ПК-6.1	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
6.2	DLP-системы. /Ср/	7	2	ПК-5.3 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9

6.3	Консультация /КА/	7	0,2	ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8 Л1.9 Л1.10 Л1.11 Л1.12 Л1.13 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9
-----	-------------------	---	-----	---	--

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

Контрольные вопросы для проведения текущего контроля

1. Угроза информационной безопасности Российской Федерации

совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере

совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в сфере общества и государства

2. Информационная безопасность Российской Федерации

состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

взаимувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

3. Обеспечение информационной безопасности

осуществление взаимувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

4. Силы обеспечения информационной безопасности

государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

взаимувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

5. Средства обеспечения информационной безопасности

правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

взаимувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

6. Система обеспечения информационной безопасности

совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

взаимувязанные правовые, организационные, оперативно-разыскные, разведывательные, контрразведывательные, научно-технические, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

7. Информационная инфраструктура Российской Федерации

совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации

Федерации или используемых на основании международных договоров Российской Федерации. совокупность объектов информатизации, глобальных информационных систем, государственных информационных систем, критических информационных инфраструктур, расположенных на территории Российской Федерации.

8. На каких принципах основывается деятельность государственных органов по обеспечению информационной безопасности?

законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;
 конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;
 соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;
 создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;
 продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

9. Задачи государственных органов в рамках деятельности по обеспечению информационной безопасности?

обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;
 оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
 планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;
 укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;
 повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности;

10. Свойства информации:

конфиденциальность
 целостность
 доступность
 непротиворечивость
 доказуемость
 все перечисленное

12. Информация, составляющая государственную тайну не может иметь гриф...

для служебного пользования
 секретно
 совершенно секретно
 особой важности

13. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
 соблюдение норм международного права в сфере информационной безопасности
 выявление нарушителей и привлечение их к ответственности
 соблюдение конфиденциальности информации ограниченного доступа
 разработку методов и усовершенствование средств информационной безопасности

14. Система защиты государственных секретов

основывается на Уголовном Кодексе РФ
 регулируется секретными нормативными документами
 определена Законом РФ "О государственной тайне"
 все перечисленное

15. Действие Закона "О государственной тайне" распространяется

на всех граждан и должностных лиц РФ
 только на должностных лиц
 на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне
 на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

16. К государственной тайне относится...

сведения в военной области
 сведения о внешнеполитической и внешнеэкономической деятельности государства
 сведения в области экономики, науки и техники

сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности
все перечисленное

17. Документы, содержащие государственную тайну снабжаются грифом
"секретно"
"совершенно секретно"
"особой важности"
все перечисленное

18. Гриф "ДСП" используется
для секретных документов
для документов, содержащих коммерческую тайну
как промежуточный для несекретных документов
в учебных целях

19. Порядок засекречивания состоит в установлении следующих принципов:
целесообразности и объективности
необходимости и обязательности
законности, обоснованности и своевременности
всех перечисленных

20. Предельный срок пересмотра ранее установленных грифов секретности составляет
5 лет
1 год
10 лет
15 лет
30 лет

21. Срок засекречивания сведений, составляющих государственную тайну
составляет 10 лет
ограничен 30 годами

22. Информация, составляющая государственную тайну не может иметь гриф...
«для служебного пользования»
«секретно»
«совершенно секретно»
«особой важности»

23. К государственной тайне относятся сведения о:
о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации
о размерах золотого запаса и государственных валютных резервах Российской Федерации
о состоянии здоровья высших должностных лиц Российской Федерации

24. К государственной тайне относятся сведения о:
о финансовой политике в отношении иностранных государств
о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях
о фактах нарушения законности органами государственной власти и их должностными лицами

25. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать ... лет.
30
25
15
10
50

26. Перечни сведений, подлежащих засекречиванию, подлежат пересмотру не реже, чем раз в ... лет
5
7
10
15
30

27. Информация это –
сведения, поступающие от СМИ
только документированные сведения о лицах, предметах, фактах, событиях
сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

только сведения, содержащиеся в электронных базах данных

28. Степени секретности информации
особой важности
совершенно секретно
секретно
для служебного пользования
не секретно

Примерный перечень вопросов к зачету:

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Понятие политики безопасности информационных систем. Назначение политики безопасности.
6. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
7. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
8. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
9. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
10. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
11. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
12. Идентификация пользователей.
13. Аутентификация пользователей.
14. Авторизация.
15. Средства идентификации и аутентификации пользователей.
16. Защита от НСД.
17. Требования к СВТ.
18. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
19. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
20. Защита персональных данных.
21. Защита информации в ГИС.
22. Концепция информационной безопасности.
23. Распределенные информационные системы. Удаленные атаки на информационную систему.
24. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
25. Физические средства обеспечения информационной безопасности.
26. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
27. DLP-системы.

Задания:

Выполнить классификацию объекта информатизации.

1. Дано: В организации с частной формой собственности в качестве средств идентификации внедрена система, работающая на основе распознавания человека по отпечатку пальца или сетчатке глаза. Информация для распознавания хранится на сервере, работающем на платформе с сертифицированной ФСТЭК ОС Astra Linux Special Edition. Все системное и прикладное программное обеспечение выполнено в защищенном исполнении и проверено на отсутствие недеklarированных возможностей.

В базе данных сотрудников обрабатывается менее 10000 субъектов ПДн. Выполнить классификацию ИСПДн сотрудников организации, хранящейся на сервере и используемой для проверки их личности.

2. Дано: В частной поликлинике обработка персональных данных пациентов. Обрабатывается менее 20000 записей о субъектах ПДн. Выполнить классификацию ИСПДн пациентов поликлиники при условии, что актуальны НДВ в прикладном программном обеспечении. В системном программном обеспечении угрозы не актуальны.

3. Дано: В районной управе ведется автоматизированная обработка информации о планируемой и проведенной работе по благоустройству территории. Определить класс защищенности информационной системы при условии, что невозможность работы с ней приведет к увеличению времени получения и обработки информации, снизит эффективность работы соответствующего подразделения.

4. Дано: В государственной организации на одном из компьютеров ведется обработка секретных сведений. За

компьютером, кроме администратора, работают пользователи user1 и user2. При этом они обрабатывают одну и ту же информацию, имеют одинаковый доступ к файлам друг друга. Определить класс автоматизированной системы.

5. Дано: В библиотеке ведется учет посетителей на сервере с сертифицированной ФСТЭК ОС Astra Linux Special Edition. Для регистрации в библиотеке указываются паспортные данные – ФИО, адрес, номер телефона, учитывается выбор изданий. Обрабатывается менее 30000 записей о субъектах ПДн. Выполнить классификацию ИСПДн при условии, что НДВ в системном и прикладном программном обеспечении не актуальны.

6. Дано: В государственной организации проводятся исследования в области повышения эффективности изготовления и прочности строительных материалов. Материалы исследований засекречены. На компьютере, где хранится секретная информация с итогами исследования, работают два пользователя. Они проводят опыты с разными строительными материалами и не имеют доступ к файлам друг друга. Определите класс автоматизированной системы.

7. Дано: В земельном фонде автоматизированная система ведет учет участков, находящихся в государственной и муниципальной собственности в масштабах одного региона. Обработка персональных данных в информационной системе не ведется. Нарушение достоверности обрабатываемой информации может повлечь умеренные негативные последствия для экономики региона.

8. Дано: В частной торговой организации ведется учет покупателей с целью предоставления им бонусных скидок при последующей покупке товаров. В информационной системе ведется учет фамилии, имени, отчества, номера телефона и номера водительского удостоверения клиента. В базе данных клиентов организации на момент классификации указано менее 3 тысяч человек. Потенциальный рост базы клиентов – не более 50 тысяч. Обработка ведется на АРМ, где установлено лицензионное программное обеспечение. Выполнить классификацию при условии, что:
1) НДВ в прикладном и системном ПО не актуальны.

5.2. Темы письменных работ

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
9. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
10. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
11. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
12. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
13. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
14. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.

15. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
17
16. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
17. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
18. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
19. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
20. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
21. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
22. Распределенные информационные системы. Удаленные атаки на информационную систему.
23. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
24. Физические средства обеспечения информационной безопасности.
25. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
26. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.

5.3. Фонд оценочных средств

1. В состав персонального компьютера входит?
- А) Сканер, принтер, монитор
- Б) Видеокарта, системная шина, устройство бесперебойного питания
- В) Монитор, системный блок, клавиатура, мышь *
- Г) Винчестер, мышь, монитор, клавиатура
2. Все файлы компьютера записываются на?
- А) Винчестер *
- Б) Модулятор
- В) Флоппи-диск
- Г) Генератор
3. Как включить на клавиатуре все заглавные буквы?
- А) Alt + Ctrl
- Б) Caps Lock *
- В) Shift + Ctrl
- Г) Shift + Ctrl + Alt
4. Как называется основное окно Windows, которое появляется на экране после полной загрузки операционной среды?
- А) Окно загрузки
- Б) Стол с ярлыками
- В) Рабочий стол*
- Г) Изображение монитора

5. Какую последовательность действий надо выполнить для запуска калькулятора в Windows?
- А) Стандартные → Калькулятор
 - Б) Пуск → Программы → Стандартные → Калькулятор *
 - В) Пуск → Стандартные → Калькулятор
 - Г) Пуск → Калькулятор
6. Как называется программа файловый менеджер, входящая в состав операционной среды Windows?
- А) Проводник *
 - Б) Сопровождающий
 - В) Менеджер файлов
 - Г) Windows commander
7. Для создания новой папки в программе Windows commander надо нажать на клавиатуре кнопку?
- А) F5
 - Б) F6
 - В) F7*
 - Г) F8
8. Для удаления файла в программе Windows commander следует нажать на клавиатуре кнопку?
- А) F5
 - Б) F6
 - В) F7
 - Г) F8*
9. Для запуска любой программы надо на рабочем столе Windows нажать на?
- А) Ссылку на программу
 - Б) Ярлык программы*
 - В) Кнопку запуска программы
 - Г) Рабочий стол
10. Чем отличается значок папки от ярлыка?
- А) Признак ярлыка – узелок в левом нижнем углу значка, которым он "привязывается" к объекту
 - Б) Значок ярлыка крупнее всех остальных значков
 - В) На значке ярлыка написана буква "Я"
 - Г) Признак ярлыка – маленькая стрелка в левом нижнем углу значка *
11. Для того, чтобы найти файл в компьютере надо нажать?
- А) Пуск → Найти → Файлы и папки*
 - Б) Пуск → Файлы и папки
 - В) Найти → Файл

Г) Пуск → Файл → Найти

12. Для настройки параметров работы мыши надо нажать?

А) Настройка → панель управления → мышь

Б) Пуск → панель управления → мышь

В) Пуск → настройка → мышь

Г) Пуск → настройка → панель управления → мышь*

13. Как установить время, через которое будет появляться заставка на рабочем столе Windows?

А) Свойства: экран → Заставка → Интервал *

Б) Заставка → Период времени

В) Свойства: экран → Заставка → Время

Г) Свойства: Интервал

14. Какие функции выполняет пункт Документы Главного меню Windows?

А) Пункт Документы Главного меню выводит список открытых в данный момент документов и позволяет переключаться между ними

Б) Пункт Документы Главного меню отображает список документов, с которыми работали последние 15 дней. Щелчок по названию или значку документа запускает приложение, с помощью которого он был создан и открывает документ

В) Пункт Документы Главного меню отображает список всех созданных документов и позволяет открыть любой из них

Г) Пункт Документы Главного меню выводит список последних открывавшихся документов. Щелчок по названию или значку документа запускает приложение, с помощью которого он был создан и открывает документ *

15. С какой целью производится выделение объектов?

А) С целью группировки и создания тематической группы

Б) С целью последующего изменения их внешнего вида (изменения размера, вида значка и др.

В) С целью их сортировки

Г) С тем, чтобы произвести с ними какие-либо действия (открыть, скопировать, переместить и др.) *

16. Как вызвать на экран контекстное меню?

А) Щелкнуть левой кнопкой мыши на объекте и в открывшемся списке выбрать команду "Контекстное меню"

Б) Открыть команду меню "СЕРВИС" и в ней выбрать команду "Контекстное меню"

В) Щелкнуть на объекте правой кнопкой мыши *

Г) Дважды щелкнуть левой кнопкой мыши на объекте

17. В какой программе можно создать текстовый документ (отчет по научной работе)?

А) Windows Word

Б) Microsoft Word *

В) Microsoft Excel

Г) Microsoft Power Point

18. Какое из изображений соответствует логотипу программы Microsoft Word?

А) *

- Б)
В)
Г)
19. Сколько документов можно одновременно открыть в редакторе Word?
- А) Только один
Б) Не более трех
В) Сколько необходимо
Г) Зависит от задач пользователя и ресурсов компьютера *
20. Открыть или создать новый документ в редакторе Microsoft Word можно используя панель?
- А) Стандартная *
Б) Форматирование
В) Структура
Г) Элементы управления
21. Для включения или выключения панелей инструментов в Microsoft Word следует нажать?
- А) Вид → панели инструментов
Б) Сервис → настройка → панели инструментов
В) Щелкнув правой кнопкой мыши по любой из панелей
Г) Подходят все пункты а, б и в *
22. Как создать новый документ "Стандартный отчет" из шаблонов Microsoft Word?
- А) Файл → создать → общие шаблоны → отчеты → стандартный отчет*
Б) Общие шаблоны → отчеты → стандартный отчет
В) Файл → отчеты → стандартный отчет
Г) Файл → создать → стандартный отчет
23. Для настройки параметров страницы Word надо нажать последовательность?
- А) Файл → параметры страницы *
Б) Файл → свойства → параметры страницы
В) Параметры страницы → свойства
Г) Правка → параметры страницы
24. Какая из представленных кнопок позволяет закрыть открытый документ Word?
- А)
Б)
В) *
Г)
25. Какую кнопку надо нажать для вставки скопированного текста в Microsoft Word?

А)

Б)

В) *

Г)

26. Какую последовательность операций в Microsoft Word нужно выполнить для редактирования размера кегля шрифта в выделенном абзаце?

А) Вызвать быстрое меню → шрифт → размер

Б) Формат → шрифт → размер

В) На панели Форматирование изменить размер шрифта

Г) Подходят все пункты а, б и в *

27. Какую кнопку в Microsoft Word нужно нажать для создания нумерованного списка литературы?

А) *

Б)

В)

Г)

28. Как найти в тексте документа Microsoft Word необходимое слово?

А) Ctrl + F12

Б) Правка → найти *

В) Сервис → найти

Г) Подходят все пункты а, б и в

29. Что означает, если отдельные слова в документе Word подчеркнуты красной волнистой линией?

А) Это означает, что шрифтовое оформление этих слов отличается от принятых в документе

Б) Это означает, что эти слова занесены в буфер обмена и могут использоваться при наборе текста

В) Это означает, что в этих словах необходимо изменить регистр их написания

Г) Это означает, что по мнению Word в этих словах допущены ошибки *

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей	Москва: Форум, 2021, URL: https://ibooks.ru/reading.php?short=1&productid=361273
Л1.2	Медведев В. А.	Информационная безопасность. Введение в специальность + eПриложение:Тесты: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/936335

	Авторы, составители	Заглавие	Издательство, год
Л1.3	Бабаш А. В., Баранова Е. К., Мельников Ю. Н.	Информационная безопасность. Лабораторный практикум + eПриложение: Учебное пособие	Москва: КноРус, 2021, URL: https://book.ru/book/936566
Л1.4	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/939292
Л1.5	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2020, URL: https://book.ru/book/932059
Л1.6	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность: Учебник	Москва: КноРус, 2020, URL: https://book.ru/book/932908
Л1.7	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность: Учебник	Москва: КноРус, 2022, URL: https://book.ru/book/941809
Л1.8	Озерский С.В., Попов И.В.	Информационная безопасность: Учебное пособие	Самара: Самарский юридический институт ФСИН России, 2019, URL: http://znanium.com/catalog/document? id=358668
Л1.9	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document? id=360289
Л1.10	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2021, URL: http://znanium.com/catalog/document? id=364622
Л1.11	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2021, URL: http://znanium.com/catalog/document? id=364911
Л1.12	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: http://znanium.com/catalog/document? id=366835
Л1.13	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2022, URL: http://znanium.com/catalog/document? id=388766

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Козьминых С. И.	Информационная безопасность финансово- кредитных организаций в условиях цифровой трансформации экономики: Монография	Москва: КноРус, 2021, URL: https://book.ru/book/941548
Л2.2	Бабаш А. В., Баранова Е. К., Мельников Ю. Н.	Информационная безопасность. Лабораторный практикум (для бакалавров)+ Электронные приложения на сайте www.book.ru : Учебное пособие	Москва: КноРус, 2018, URL: https://book.ru/book/926191
Л2.3	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2019, URL: https://book.ru/book/932909
Л2.4	Мельников В. П., под ред., Куприянов А. И.	Информационная безопасность: Учебник	Москва: КноРус, 2018, URL: https://book.ru/book/924214
Л2.5	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2021, URL: https://book.ru/book/938255

	Авторы, составители	Заглавие	Издательство, год
Л2.6	Мельников В. П., Куприянов А. И., Васильева Т. Ю.	Информационная безопасность: Учебник	Москва: КноРус, 2018, URL: https://book.ru/book/929884
Л2.7	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2018, URL: https://book.ru/book/931784
Л2.8	Глинская Е.В., Чичварин Н.В.	Информационная безопасность конструкций ЭВМ и систем: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, URL: https://znanium.com/catalog/document?id=362430
Л2.9	Панфилова О.А., Крюкова Д.Ю.	Информационная безопасность и защита информации: Учебное пособие	Вологда: федеральное казенное образовательное учреждение высшего образования «Вологодский институт права и экономики Федеральной службы исполнения наказаний», 2018, URL: http://znanium.com/catalog/document?id=370184
Л2.10	Баранова Е.К., Бабаш А.В., Ларин Д.А.	Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие	Москва: Издательский Центр РИО, 2022, URL: https://znanium.com/catalog/document?id=388319
6.2. Электронные учебные издания и электронные образовательные ресурсы			
Э1	Совет Безопасности Российской Федерации . - Режим доступа: http://www.scrf.gov.ru/		
Э2	Федеральная служба по техническому и экспортному контролю . - Режим доступа: https://fstec.ru/		
Э3	Информационно-правовой портал ГАРАНТ.РУ . - Режим доступа: https://www.garant.ru/		
Э4	Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» . - Режим доступа: https://docs.cntd.ru/		
Э5	Национальный Открытый Университет "ИНТУИТ". - Режим доступа: https://intuit.ru/		
Э6	Электронные ресурсы Академии ИМСИТ. - Режим доступа: http://eios.imsit.ru/		
Э7	Электронная библиотечная система Znanium. - Режим доступа: http://znanium.com		
Э8	Электронная библиотечная система Ibooks. - Режим доступа: http://www.ibooks.ru/		
Э9	Электронная библиотечная система BOOK.ru. - Режим доступа: http://www.book.ru		
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства			
6.3.1.1	Windows 10 Pro RUS Операционная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021		
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL		
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/		
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL		
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL		
6.3.1.6	Notepad++. Текстовый редактор Notepad++. Программное обеспечение по лицензии GNU GPL		
6.3.1.7	Kaspersky Endpoint Security Антивирусное ПО Kaspersky Endpoint Security для бизнеса Стандартный (350шт). Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)		
6.3.1.8	Oracle VM VirtualBox VM VirtualBox — программный продукт виртуализации для операционных систем Программное обеспечение по лицензии GNU GPL		
6.3.1.9	Adobe Reader DC Adobe Acrobat — пакет программ, предназначенный для создания и просмотра электронных публикаций в формате PDF Adobe Acrobat Reader DC and Runtime Software distribution license agreement for use on personal computers от 31.01.2017		
6.3.1.1	MS Office Standart 2010 Офисный пакет Microsoft Office Microsoft Open License 48587685 от 02.06.2011		
6.3.1.1	MS Visio Pro 2010 Интегрированная среда разработки Microsoft Visio профессиональный 2010 Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021		
6.3.1.1	Windows 7 Pro Операционная система Microsoft Windows 7 Professional Microsoft Open License 48587685 от 02.06.2011		
6.3.1.1	Консоль Kaspersky Security Center Консоль администрирования Kaspersky Security Center Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи)		
6.3.1.1	Kaspersky Endpoint Security 11 Kaspersky Endpoint Security 11 для Windows Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)		

6.3.1.1 5	Microsoft Windows 10 PRO x64 DSP OEM Операционная система Microsoft Windows 10 PRO Счет №93 от 21.05.2019, Акт передачи прав №31 от 05.06.2019.
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	Global CIO Официальный портал ИТ-директоров http://www.globalcio.ru
6.3.2.3	ARIS BPM Community https://www.ariscommunity.com
6.3.2.4	ИСО Международная организация по стандартизации https://www.iso.org/ru/home.html
6.3.2.5	РОССТАНДАРТ Федеральное агентство по техническому регулированию и метрологии https://www.gost.ru/portal/gost/
6.3.2.6	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
208	Лаборатория "Интеллектуальные системы и технологии" (Research Laboratory of Intelligent Systems and Technologies). Помещение для проведения занятий лекционного типа, семинарского типа, курсовых работ (курсовых проектов), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы.	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Diptrace Embarcadero RAD Studio XE8 Arduino Software (IDE) NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2007 NI LabVIEW Full	19 посадочных мест, рабочее место преподавателя, 10 компьютеров H97-PLU/INTEL i5-4460/DDR3-1333-16Гб/SD7SB6S-128G+ST500DM002/Radeon R7 200/Realtek PCIe GBE 9 компьютеров A320M-H-CF/AMD Ryzen 5 2600/DDR4-2666-16Гб/Apacer AS2280P4-256Gb, Toshiba HDWD110 1Tb/Nvidia GT-710/Realtek PCI-E GBE 1 компьютер P8Z77-V-LX2/INTEL I5-3570K/DDR3-1600-8Гб/ SSD SSDPR-CX400-128G2, WDC WS15EARS/AMD HD-5700 Realtek PCIe GBE 10 мониторов Philips 274E5QSB 27" 1 монитор Samsung SyncMaster E1720 11 комплектов клавиатура+мышь 1 принтер HP LaserJet 1018 1 коммутатор неуправляемый TL-SG1024D Междисциплинарная лабораторная станция NI ELVIS II и ПО Circuit Design Suit Лаборатория схемотехники (необходимо наличие лаб. станции ELVIS) Практикум по цифровым элементам вычислительной и информационно-измерительной техники (необходимо наличие лабораторной станции ELVIS) Лаборатория проектирование цифровых устройств и программирования ПЛИС (необходимо наличие лабораторной станции ELVIS) Комплект аксессуаров NI myRIO Starter Accessory Kit (опционально) Комплект аксессуаров NI myRIO Mechatronics Accessory Kit Комплект аксессуаров NI myRIO Embedded Systems Accessory Kit Лаборатория программирования встраиваемых систем Локальные вычислительные сети (необходимо наличие лабораторной станции ELVIS) Промышленные интерфейсы и протоколы (программная версия) Академическая лицензия NI LabVIEW на неограниченное кол-во рабочих мест в пределах кафедры. Arduino Robot.
113	Помещение для проведения занятий лекционного типа, семинарского типа, курсовых работ (курсовых проектов), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016	20 посадочных мест, рабочее место преподавателя 20 компьютеров P55-UD3/INTEL-i5-750/DDR3-1333-8Гб/SSD Flexis 120Gb /WD3200AAKS/Radeon HD-4600/DWL-G520 Wireles 20 мониторов Acer V193W-19" 20 комплектов клавиатура+мышь 1 коммутатор неуправляемый DES-1024D 1 беспроводная точка доступа DWL-3200AP 3 Комплект оборудования Arduino 5 учебных комплектов SDK 1.1s 1 МФУ HP LJ M1212nf MFP 12 Инструмент для сборки ПК (отвертка ph-1, плоскогубцы 150 мм, термопаста 2гр., Антистатический браслет, стяжки 150 мм)

	самостоятельной работы.	MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Diptrace Ramus Educational Micro-Cap Evaluation	
114а	Кабинет информатики. Помещение для проведения занятий лекционного типа, семинарского типа, курсовых работ (курсовых проектов), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Ramus Educational Micro-Cap Evaluation	16 посадочных мест, рабочее место преподавателя 16 компьютеров GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE 16 мониторов AOC e2243Fw 21,5” 16 комплектов клавиатура+мышь 1 Коммутатор LincSys SR224G 1 Проектор ViewSonic PJD5232 1 Проекционный экран Luma 1 Шкаф телекоммуникационный 1 ИБП SMART UPS 2000 3 Коммутатор Cisco Catalist 2960 1 Концентратор AlterPath 16 port 4 Маршрутизатор Cisco-2800 2 Маршрутизатор Cisco-2811 6 Модуль 2-port 2 Панель коммутационная 12 Шнур V.35 Cable Витая пара, Коннектор RJ-45 2 Инструмент для зачистки кабеля UTP 1 Протяжка кабельная, d=3,5 мм 10 м 1 Тестер МЕГЕОН 40060/Шт. 5 Инструмент для обжима витой пары 5 Тестер кабельный 3 Инструмент для заделки кабеля витая пара тип Krone с крючками 3 Р телефон GrandStream GXP1610 2 Комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) 2 Роутер Wi-Fi роутер Keenetic 1 Сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE
115	Помещение для проведения занятий лекционного типа, семинарского типа, курсовых работ (курсовых проектов), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community	20 посадочных мест, рабочее место преподавателя 20 компьютеров GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/DDR3-1333-4Гб/ SSD Flexis 120Gb/WD5000AAK/Radeon HD-5800/Atheros AR9287 Wireless 19 мониторов AOC e2243Fw 21,5” 1 монитор Acer V226HQL 21,5” 20 комплектов клавиатура+мышь 1 беспроводная точка доступа TP-Link TL-WA801ND

	работы.	Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL Klite Mega Codec Pack	
119	Помещение для проведения занятий лекционного типа, семинарского типа, курсовых работ (курсовых проектов), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы.	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Embarcadero RAD Studio XE8 Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express AnyLogic Klite Mega Codec Pack MS Office Standart 2007	20 посадочных мест, рабочее место преподавателя 20 компьютеров H110M-S2-C/INTEL Pentium G4400/DDR4-2133-4Гб/TOSHIBA HDWD105/Intel HD-510/Atheros AR9287 Wireless 20 мониторов 20 комплектов клавиатура+мышь 1 беспроводная точка доступа TP-Link TL-WA801ND
120	Кабинет информатики, технологий и методов программирования. Помещение для проведения занятий лекционного типа, семинарского типа, курсовых работ (курсовых	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management	20 посадочных мест, рабочее место преподавателя 20 компьютеров A320M-H-CF/AMD Ryzen 5 2600X/DDR4-2933 16Гб/SSD XPG GAMMIX S11 Pro 512Гб/NVIDIA GeForce GTX 1050 Ti/Realtek PCIe GbE Family Controller 40 мониторов Samsung S24R350FHI 23.8" 20 ИБП CyberPower UT650EG 20 комплектов клавиатура+мышь 20 гарнитур Defenfer G-320 1 управляемый коммутатор TP-LINK TL-SG1024D 1 Интерактивная панель EliteBoard LR-75UT40i7

проектов), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы.	Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL SMath Studio Klite Mega Codec Pack	
---	---	--

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой. В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Системное программное обеспечение» разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).

Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.

Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.

Методические указания и материалы по видам учебных занятий по дисциплине:

Вид учебных занятий, работ - Организация деятельности обучающегося

Лекция - написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа студентов в ходе семестра является важной составной частью учебного процесса и необходима для закрепления и углубления знаний, полученных в период сессии на лекциях, практических и интерактивных занятиях, а также для индивидуального изучения дисциплины «Информационная безопасность» в соответствии с программой и рекомендованной литературой.

Самостоятельная работа выполняется в виде подготовки домашнего задания или сообщения по отдельным вопросам, написание и защита научно-исследовательского проекта.

Контроль качества выполнения самостоятельной (домашней) работы может осуществляться с помощью устного опроса на лекциях или практических занятиях, обсуждения подготовленных научно-исследовательских проектов, проведения тестирования.

Устные формы контроля помогут оценить владение студентами жанрами научной речи (дискуссия, диспут, сообщение, доклад и др.), в которых раскрывается умение студентов передать нужную информацию, грамотно использовать языковые средства, а также ораторские приемы для контакта с аудиторией.

Письменные работы позволяют оценить владение источниками, научным стилем изложения, для которого характерны: логичность, точность терминологии, обобщенность и отвлеченность, насыщенность фактической информацией.