КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОРГАНИЗАЦИЯ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Рабочая программа по дисциплине «Организация и правовое обеспечение информационной безопасности» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Цели определены государственным образовательным стандартом высшего профессионального образования и соотнесены с общими целями ООП ВО по специальности 10.05.01 Компьютерная безопасность, в рамках которой преподается дисциплина «Организация и правовое обеспечение информационной безопасности».

Целью освоения учебной дисциплины «Компьютерные преступления в компьютерных системах и сетях» является формирование у студентов современных знаний, навыков и компетенций в области уголовного права, посвященного компьютерным преступлениям, обеспечение усвоения поведенческих мотивов, целей, условий и механизмов совершения компьютерных преступлений, а также законодательных основ их предотвращения, предупреждения и расследования.

Задачи дисциплины

– привить навыки формирования требований по защите информации в различных КС;

– ознакомить с требованиями к защите автоматизированных информационных систем (ИС) от несанкционированного доступа (НСД) на территории Российской Федерации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Организация и правовое обеспечение информационной безопасности» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» учебного плана.

Дисциплина «Организация и правовое обеспечение информационной безопасности» занимает одно из ключевых мест в этом блоке программы, являясь основой для изучения других курсов. Ее изучение формирует теоретические знания, базовые компетенции и прикладные навыки в квалификации компьютерных преступлений, уголовного законодательства в указанной области, изучении поведенческих навыков и мотивов совершения компьютерных преступлений, предотвращения и предупреждения их совершения, а также расследования.

Для ее успешного освоения слушатель должен владеть знаниями таких дисциплин как компьютерные сети, основы информационной безопасности, операционные системы, сети и системы передачи информации и т.д.

В свою очередь, данный курс служит фундаментом для успешного освоения таких дисциплин, как защита информации от утечки по техническим каналам, методы и средства криптографической защиты информации, проведения НИР, подготовки и защите ВКР, практической деятельности специалистов.

3. Перечень планируемых результатов обучения по дисциплине

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.2 Демонстрирует умение решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	Знать основные принципы работы с данными, современные инструменты анализа данных на базовом уровне, в том числе навыки программирования, алгоритмизации и математические методы при решении задач анализа данных Уметь: выбирать и применять средства защиты информационных систем, компьютерных сетей, баз данных, операционных систем, технических каналов утечки информации Владеть: нормативно-правовой информацией, регламентирующей вопросы защиты информации, и применение её в профессиональной деятельности.
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.3 Демонстрирует умения разработки криптографических протоколов и исследования их стойкости к различным атакам в составе средств защиты компьютерных систем	Знать основные типы криптографических протоколов и принципы их построения с использованием шифрсистем, основные стандарты, протоколы и интерфейса, необходимые при сертификации средств защиты информации. Уметь проводить анализ криптографических протоколов, применять криптографические средства и системы информационной безопасности Владеть математическими методами при использовании криптографических протоколов, государственными стандартами

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся:

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			7
1. Контактная работа обучающихся с преподавателем:		69	69
Аудиторные занятия, часов всего, в том числе:		68	68
• занятия лекционного типа		34	34
• занятия семинарского типа:		34	34
практические занятия		-	-
лабораторные занятия		34	34
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		39	39
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		20	20
- выполнение домашних заданий по практическим занятиям		19	19
- подготовка к зачету		-	-
Промежуточная аттестация: зкзамен		36	36
ИТОГО:	часов	144	72
общая трудоемкость	Зач.ед.	4	2

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Характеристика правоотношений в сфере защиты информации.

Информация и окружающий мир. Свойства информации. Влияние информации на общество. Информация и право. Правовое определение понятия «информация». Документирование информации. Понятие информационных ресурсов. Виды информации по категориям доступа. Общедоступная информация. Информация ограниченного доступа. Информационные технологии. Правовое закрепление необходимости принятия мер по защите информации. Составление правовых понятий информационной безопасности и защиты информации. Объекты и субъекты сферы защиты информации. Цели защиты информации.

Тема 2. Структура системы организационно- правового обеспечения

информационной безопасности.

Определение понятия «Комплексная система защиты информации» и элементы этой системы. Понятие «Организационная защита информации». Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией. Особенности нормативно- правового регулирования современных отношений в сфере защиты информации.

Тема 3. Нормативно-правовая база обеспечения защиты информации в России.

Особенности нормативно-правового регулирования современных отношений в сфере защиты информации. Конституционное законодательство о защите информации. Доктрина информационной безопасности Российской Федерации. Обзор законодательных актов общего характера, содержащих положения о защите информации. Специальное законодательство по защите информации. Особая роль законов «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О государственной тайне», «О персональных данных», «Об электронной подписи», «Об оперативно-розыскной деятельности», «О техническом регулировании», «О безопасности критической информационной инфраструктуры Российской Федерации». Законы субъектов РФ, регламентирующие вопросы защиты информации. Подзаконные правовые акты, регулирующие процессы защиты информации. Роль подзаконных нормативных документов ФСТЭК РФ и ФСБ РФ. Основные документы ФСТЭК России определяющие требования по защите информации. Нормативно-правовые акты, устанавливающие юридическую ответственность за правонарушения в сфере защиты информации

Тема 4. Угрозы информационной безопасности.

Основные понятия. Классификация угроз. Источники и каналы утечки информации.

Тема 5. Силы и средства организационной защиты информации.

Служба информационной безопасности предприятия. Состав, задачи, основные направления деятельности службы информационной безопасности предприятия.

Основные направления деятельности по взаимодействию с правоохранительными органами и службами обеспечения информационной безопасности. Политика информационной безопасности предприятия.

Тема 6. Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа.

Особенности правовой защиты сведений, составляющих государственную тайну. Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих

государственную тайну, к различным степеням секретности. Присвоение грифа и изменение грифа секретности работам, документам и изделиям. Особенности правовой защиты коммерческой тайны. Режим коммерческой тайны Учёт, хранение и уничтожение носителей, содержащих информацию, ограниченного доступа.

Тема 7. Подбор персонала на должности, связанные с работой с конфиденциальной информацией.

Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Порядок подбора персонала на должности, связанные с работой с конфиденциальной информацией. Особенности документирования трудовых отношений с персоналом, обладающим конфиденциальной информацией.

Тема 8. Организация доступа и допуска к информации ограниченного доступа. Понятие допуск.

Понятие допуск. Формы допусков, их назначение и классификация. Основные принципы допускной работы. Понятие доступ к защищаемой информации. Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа. Понятие разрешительной системы доступа, основные требования, предъявляемые к ней.

Тема 9. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов.

Понятие служебное расследование по фактам разглашения информации. Цели и задачи служебного расследования. Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.

Тема 10. Организация защиты информации при взаимодействии со сторонними организациями.

Отражение вопросов защиты информации в гражданско-правовых договорах о взаимодействии. Организация защиты информации при подготовке материалов к открытому опубликованию. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Подготовка помещений для проведения конфиденциальных мероприятий, организация их аттестации. Организация защиты информации при приеме в организации посетителей и командированных лиц.

Тема 11. Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.

Виды деятельности в сфере защиты информации, подлежащие лицензированию. Подзаконные правовые акты, определяющие порядок лицензирования. Органы государственной власти, наделенные полномочиями

лицензирования в сфере защиты информации. Сертификация. Нормативно-правовые акты, определяющие порядок сертификации средств защиты информации. Ответственность за нарушение порядка лицензирования и сертификации.

Тема 12. Правовая защита информации, составляющей интеллектуальную собственность.

Понятие интеллектуальной собственности. Общие положения по регулированию отношений в области защиты интеллектуальной собственности. Особенности правовой защиты объектов патентного права. Защита авторских прав на программы для ЭВМ и базы данных. Правовая защита секретов производства (ноу-хау). Ответственность за правонарушения в сфере интеллектуальной собственности.

Тема 13. Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Определение понятия «Критическая информационная инфраструктура. Объекты КИИ. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Тема 14. Правовая защита информации, составляющей персональные данные.

Принципы и условия обработки персональных данных. Особенности обработки и защиты персональных данных в информационных системах. Ответственность за правонарушения.

Тема 15. Особенности правовой защиты сведений, составляющих различные виды тайн.

Личная и семейная тайна. Тайна голосования. Тайна исповеди. Тайна усыновления. Служебная тайна. Защита сведений, составляющих тайну следствия и судопроизводства. Налоговая тайна. Таможенная тайна. Защита профессиональной тайны. Журналистская тайна. Нотариальная тайна. Страховая тайна. Врачебная тайна. Тайна аудита. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Банковская тайна.

Тема 16. Правовое обеспечение безопасности информации в информационных системах.

Доктрина информационной безопасности России об угрозах безопасности информационным системам. Особенности правовой защиты информационных и телекоммуникационных систем. Гражданско-правовые, уголовно-правовые и административно-правовые нормы защиты информации в информационных и телекоммуникационных системах.

Тема 17. Контроль функционирования системы организационной защиты информации

Сущность контроля, как функции управления. Формы контроля. Аудит информационной безопасности.

По итогам изучаемой дисциплины обучающиеся сдают экзамен.

Дисциплина изучается на 4 курсе, в 7 семестре по учебному плану очной формы обучения.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование разделов (тем)	Количество часов					Индикаторы достижения компетенций
		Всего	Аудиторная работа			Внеаудиторная работа	
			занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки	лабораторные занятия	самостоятельная работа	
	2		4	5		7	8
1.	Характеристика правоотношений в сфере защиты информации.	6	2	–	2	2	ОПК-9.2; ОПК-10.3
2.	Структура системы организационно-правового обеспечения информационной безопасности.	6	2	–	2	2	ОПК-9.2; ОПК-10.3
3.	Нормативно-правовая база обеспечения защиты информации в России.	6	2	–	2	2	ОПК-9.2; ОПК-10.3
4.	Угрозы информационной безопасности.	6	2	–	2	2	ОПК-9.2; ОПК-10.3
5.	Силы и средства организационной защиты информации.	6	2	–	2	2	ОПК-9.2; ОПК-10.3
6.	Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа.	6	2	–	2	2	ОПК-9.2; ОПК-10.3

7.	Подбор персонала на должности, связанные с работой с конфиденциальной информацией.	6	2	–	2	2	ОПК-9.2; ОПК-10.3
8.	Организация доступа и допуска к информации ограниченного доступа. Понятие допуск.	6	2	-	2	2	ОПК-9.2; ОПК-10.3
9.	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов.	6	2	-	2	2	ОПК-9.2; ОПК-10.3
10.	Организация защиты информации при взаимодействии со сторонними организациями.	6	2	-	2	2	ОПК-9.2; ОПК-10.3
11.	Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.	6	2	-	2	2	ОПК-9.2; ОПК-10.3
12.	Правовая защита информации, составляющей интеллектуальную собственность.	7	2	-	2	3	ОПК-9.2; ОПК-10.3
13.	Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации.	6	2	-	2	2	ОПК-9.2; ОПК-10.3
14.	Правовая защита информации, составляющей персональные данные.	7	2	-	2	3	ОПК-9.2; ОПК-10.3
15.	Особенности правовой защиты сведений, составляющих различные виды тайн.	8	2	-	2	4	ОПК-9.2; ОПК-10.3

16.	Правовое обеспечение безопасности информации в информационных системах.	7	2	-	2	3	ОПК-9.2; ОПК-10.3
17.	Контроль функционирования системы организационной защиты информации	6	2	-	2	2	ОПК-9.2; ОПК-10.3
18.	Консультация перед экзаменом	0,5			0,5		ОПК-9.2; ОПК-10.3
19.	Подготовка к экзамену	36					
20.	Каттэк	0,5					
21.	Общая трудоемкость по дисциплине*:*	**144**	**34**	–	**34**	**39**	

6. Лабораторные занятия

№ п/п	Наименование раздела(темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1.	Характеристика правоотношений в сфере защиты информации.	Информация и окружающий мир. Свойства информации. Влияние информации на общество. Информация и право. Правовое определение понятия «информация». Документирование информации. Понятие информационных ресурсов. Виды информации по категориям доступа. Общедоступная информация. Информация ограниченного доступа. Информационные технологии. Правовое закрепление необходимости принятия мер по защите информации. Составление правовых понятий информационной безопасности и защиты информации. Объекты и субъекты сферы защиты информации. Цели защиты информации.	ЛР
2.	Структура системы организационно-правового обеспечения информационной безопасности.	Определение понятия «Комплексная система защиты информации» и элементы этой системы. Понятие "Организационная защита информации". Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией. Особенности нормативно- правового регулирования современных отношений в	ЛР

		сфере защиты информации	
3.	Нормативно-правовая база обеспечения защиты информации в России.	Особенности нормативно-правового регулирования современных отношений в сфере защиты информации. Конституционное законодательство о защите информации. Доктрина информационной безопасности Российской Федерации. Обзор законодательных актов общего характера, содержащих положения о защите информации. Специальное законодательство по защите информации. Особая роль законов «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О государственной тайне», «О персональных данных», «Об электронной подписи», «Об оперативно-розыскной деятельности», «О техническом регулировании», «О безопасности критической информационной инфраструктуры Российской Федерации». Законы субъектов РФ, регламентирующие вопросы защиты информации. Подзаконные правовые акты, регулирующие процессы защиты информации. Роль подзаконных нормативных документов ФСТЭК РФ и ФСБ РФ. Основные документы ФСТЭК России определяющие требования по защите информации. Нормативно-правовые акты, устанавливающие юридическую ответственность за правонарушения в сфере защиты информации.	ЛР
4.	Угрозы информационной безопасности.	Основные понятия. Классификация угроз. Источники и каналы утечки информации.	ЛР
5.	Силы и средства организационной защиты информации.	Служба информационной безопасности предприятия. Состав, задачи, основные направления деятельности службы информационной безопасности предприятия. Основные направления деятельности по взаимодействию с правоохранительными органами и службами обеспечения информационной безопасности. Политика информационной безопасности предприятия.	ЛР

6.	Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа.	Особенности правовой защиты сведений, составляющих государственную тайну. Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение грифа и изменение грифа секретности работам, документам и изделиям. Особенности правовой защиты коммерческой тайны. Режим коммерческой тайны Учёт, хранение и уничтожение носителей, содержащих информацию, ограниченного доступа.	ЛР
7.	Подбор персонала на должности, связанные с работой с конфиденциальной информацией.	Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Порядок подбора персонала на должности, связанные с работой с конфиденциальной информацией. Особенности документирования трудовых отношений с персоналом, обладающим конфиденциальной информацией.	ЛР
8.	Организация доступа и допуска к информации ограниченного доступа. Понятие допуск.	Понятие допуск. Формы допусков, их назначение и классификация. Основные принципы допускной работы. Понятие доступ к защищаемой информации. Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа. Понятие разрешительной системы доступа, основные требования, предъявляемые к ней.	ЛР
9.	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов.	Понятие служебное расследование по фактам разглашения информации. Цели и задачи служебного расследования. Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.	ЛР
10.	Организация защиты информации при взаимодействии со сторонними организациями.	Отражение вопросов защиты информации в гражданско-правовых договорах о взаимодействии. Организация защиты информации при подготовке материалов к открытому опубликованию. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Подготовка помещений для проведения конфиденциальных мероприятий, организация их аттестации. Организация защиты информации при приеме в организации посетителей и командированных	ЛР

		лиц.	
11.	Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.	Виды деятельности в сфере защиты информации, подлежащие лицензированию. Подзаконные правовые акты, определяющие порядок лицензирования. Органы государственной власти, наделенные полномочиями лицензирования в сфере защиты информации. Сертификация. Нормативно-правовые акты, определяющие порядок сертификации средств защиты информации. Ответственность за нарушение порядка лицензирования и сертификации.	ЛР
12.	Правовая защита информации, составляющей интеллектуальную собственность.	Понятие интеллектуальной собственности. Общие положения по регулированию отношений в области защиты интеллектуальной собственности. Особенности правовой защиты объектов патентного права. Защита авторских прав на программы для ЭВМ и базы данных. Правовая защита секретов производства (ноу-хау). Ответственность за правонарушения в сфере интеллектуальной собственности.	ЛР
13.	Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации.	Определение понятия «Критическая информационная инфраструктура. Объекты КИИ. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	ЛР
14.	Правовая защита информации, составляющей персональные данные.	Принципы и условия обработки персональных данных. Особенности обработки и защиты персональных данных в информационных системах. Ответственность за правонарушения.	ЛР
15.	Особенности правовой защиты сведений, составляющих различные виды тайн.	Личная и семейная тайна. Тайна голосования. Тайна исповеди. Тайна усыновления. Служебная тайна. Защита сведений, составляющих тайну следствия и судопроизводства. Налоговая тайна. Таможенная тайна. Защита профессиональной тайны. Журналистская тайна. Нотариальная тайна. Страховая тайна. Врачебная тайна. Тайна аудита. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Банковская тайна.	ЛР

16.	Правовое обеспечение безопасности информации в информационных системах.	Доктрина информационной безопасности России об угрозах безопасности информационным системам. Особенности правовой защиты информационных и телекоммуникационных систем. Гражданско-правовые, уголовно-правовые и административно-правовые нормы защиты информации в информационных и телекоммуникационных системах.	ЛР
17.	Контроль функционирования системы организационной защиты информации	Сущность контроля, как функции управления. Формы контроля. Аудит информационной безопасности.	ЛР

7. Практические занятия

Учебным планом не предусмотрены

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. Составление тематического конспекта на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях

Учебно-методические материалы для самостоятельной работы обучающихся и числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их

здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,
– в форме электронного документа. Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,
– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с Фондом оценочных средств.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения ОПОП ВО

1.1. Оценочные средства для текущего контроля

Устный опрос

По теме: «Характеристика правоотношений в сфере защиты информации»

1. Дайте определение понятию «Информационная безопасность»
2. Какая информация входит в перечень сведений конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997г. № 188
3. Федеральный закон «Об информации, информационных технологиях и о защите информации». Какие отношения регулирует? Какие направления деятельности в области ИБ рассматриваются в данном законе?
4. В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», дайте определение понятиям «Информация», «Конфиденциальность информации», «Обладатель информации», «Доступ к информации», «Предоставление информации», «Распространение информации».
5. Понятие и основные признаки документированной информации?
6. Какая информация, в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», относится к общедоступной, и как регулируются отношения при использовании такой информации?
7. Права и обязанности обладателя информации, в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации».

По теме: «Структура системы организационно-правового обеспечения информационной безопасности.»

1. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
2. Какая информация запрещена к распространению, в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации»?
3. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ. Ознакомиться. Описать. Чему посвящён закон? Какие отношения регулирует?
4. В соответствии с ФЗ «О коммерческой тайне», дайте определение понятиям «Коммерческая тайна», «Информация, составляющая коммерческую тайну», «Разглашение информации, составляющей коммерческую тайну».
5. Какие сведения, не могут составлять коммерческую тайну?

По теме: «Нормативно-правовая база обеспечения защиты информации в России.»

1. Кому принадлежит право на отнесение информации к разряду коммерческой тайны?
2. Какие меры по охране конфиденциальности информации должен предпринять её обладатель, чтобы режим коммерческой тайны считался установленным?
3. Имеет ли право обладатель информации, составляющей коммерческую тайну, применять средства технической защиты конфиденциальности этой информации? Укажите статью ФЗ «О коммерческой тайне», которая регулирует этот вопрос.
4. Какие меры по охране конфиденциальности информации, составляющей коммерческую тайну, должен предпринять работодатель в рамках трудовых отношений, в соответствии с ФЗ «О коммерческой тайне»?
5. Что обязан делать работник, в целях охраны конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений, в соответствии с ФЗ «О коммерческой тайне»?
6. В каком случае будет правомерным требование работодателя о возмещении убытков, причиненных ему разглашением коммерческой тайны, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем?

По теме: «Угрозы информационной безопасности»

1. Верно ли утверждение о том, что работник, получивший доступ к коммерческой тайне, в случае разглашения этой информации, обязан возместить убытки, причиненные работодателю, даже в том случае, если меры по обеспечению режима
2. Коммерческой тайны, в отношении этой информации, работодателем не были соблюдены? Обоснуйте свой ответ.
3. Могут ли органы государственной власти требовать предоставления коммерческой тайны от обладателя этой информации? Как будут регулироваться

отношения в случае отказа в предоставлении этих сведений?

4. Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1. Ознакомиться. Описать.

5. Какие отношения регулирует? Какие направления деятельности в области ИБ рассматриваются в данном законе?

6. В соответствии с ФЗ «О государственной тайне», дайте определение понятию «Государственная тайна».

По теме: «Силы и средства организационной защиты информации.»

1. Какие сведения составляют государственную тайну?
2. Какие сведения, не могут составлять государственную тайну?
3. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений.
4. Что может послужить основанием для отказа должностному лицу или гражданину в допуске к государственной тайне?
5. Условия прекращения допуска должностного лица или гражданина к государственной тайне?

По теме: «Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа»

1. Дайте определение понятию «Интеллектуальная собственность»?
2. Кто может осуществлять защиту авторства после смерти автора?
3. Допускается ли переход исключительного права на результат интеллектуальной деятельности без заключения договора? Если да, то в каких случаях?
4. Будет ли признан автором результата интеллектуальной деятельности гражданин, организовавший работу по созданию такого результата и оказавший содействие по оформлению прав на такой результат? Обоснуйте свой ответ.
5. Чем отличается лицензионный договор от договора об отчуждении исключительного права?

По теме: «Организация доступа и допуска к информации ограниченного доступа. Понятие допуск»

1. Может ли лицензиат предоставить право использования результата интеллектуальной деятельности или средства индивидуализации другому лицу? Обоснуйте свой ответ
2. Может ли исключительное право на результат интеллектуальной деятельности принадлежать нескольким лицам совместно? Если да, то как определяются взаимоотношения между ними?
3. Какие правовые акты содержат нормы, регулирующие отношения в сфере интеллектуальной собственности?
4. Условия патентоспособности изобретений полезных моделей и промышленных образцов?

По теме: «Текущая работа с персоналом, обладающим

конфиденциальной информацией»

1. Что происходит с изобретением, полезной моделью или промышленным образом после прекращения действия исключительного права на них?
2. Основания и порядок продления срока действия исключительного права на объекты патентного права?
3. Открытая лицензия как форма распоряжения исключительным правом на изобретение, полезную модель или промышленный образец. Раскрыть суть.

По теме: «Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов»

1. В каком случае право на получение патента на служебное изобретение, служебную полезную модель или служебный промышленный образец, возвращается работнику?
2. Как решится вопрос о выдаче патента, если заявки, поданы разными заявителями на идентичные изобретения, полезные модели и промышленные образцы имеют одну и ту же дату приоритета?
3. Особенности подачи и рассмотрения заявки на выдачу патента на секретное изобретение.

По теме: «Организация защиты информации при взаимодействии со сторонними организациями»

1. Сроки действия исключительного права составителя базы данных и изготовителя базы данных?

По теме: «Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации»

1. Зависит ли наступление правовой охраны для программ ЭВМ и баз данных от государственной регистрации этих объектов?
2. Несет ли ответственность за нарушение исключительного права на секрет производства лицо, которое получило доступ к секрету производства случайно и не знало о том, что его использование незаконно?
3. Кому будет принадлежать исключительное право на секрет производства, полученный при выполнении работ по государственному контракту для государственных нужд.

По теме: «Правовая защита информации, составляющей интеллектуальную собственность»

1. Какие сведения не могут быть признаны ноу-хау? Приведите пример.
2. Дайте определение понятию «Персональные данные». Перечислите принципы обработки персональных данных

По теме: «Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации»

1. К какой категории сведений относятся персональные данные?
2. Каковы особенности обработки персональных данных в государственных или муниципальных информационных системах?
3. Классификация видов противоправных деяний в отношении компьютерной информации.
4. Способы и механизмы совершения компьютерных преступлений

По теме: «Правовая защита информации, составляющей персональные данные.»

1. Дайте понятие сертификации.
2. Основные нормативные акты в области лицензирования ЗИ.
3. Какие нормативные правовые акты по сертификации средств защиты информации?

По теме: «Особенности правовой защиты сведений, составляющих различные виды тайн»

1. Виды юридической ответственности за нарушение правовых норм по защите информации.

По теме: «Правовое обеспечение безопасности информации в информационных системах»

1. Уголовный кодекс РФ онаказаниях за правонарушения в области информационной безопасности.
2. Административные взыскания за нарушения правовых норм по защите информации.

По теме: «Контроль функционирования системы организационной защиты информации»

1. Проведение административного расследования пофактам нарушения установленного порядка защиты информации.
2. Особенности трудовых отношений при нарушении правовых норм в сфере информационной безопасности.

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

Код контролируемых компетенций ОПК-9, ОПК-10

1 «Характеристика правоотношений в сфере защиты информации»

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Указа Президента РФ от 6 марта 1997 г. № 188, ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ

2. «Структура системы организационно-правового обеспечения информационной безопасности».

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правового акта: ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ,

3. «Нормативно-правовая база обеспечения защиты информации в России».

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020), Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» Федеральный закон от 31.05.1996 N 61-ФЗ «Об обороне»

4. Угрозы информационной безопасности.

Цели выполнения лабораторной работы: Закрепление пройденного материала. Изучение документов ФСТЭК РФ: Приказ ФСТЭК России от 11 февраля 2013 г. N 17 База данных угроз (bdu.fstec.ru); Методический документ ФСТЭК РФ «Методика оценки угроз безопасности информации»

5. Силы и средства организационной защиты информации.

Цели выполнения лабораторной работы: Закрепление пройденного материала пройденного материала. Изучение документов: Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановление Правительства РФ от 15.07.2022 N 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)», «ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», «ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

6. Порядок засекречивания, рассекречивания, учёта и хранения сведений, ограниченного доступа.

Цели выполнения лабораторной работы: Закрепление пройденного материала. Изучение документов: Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1, Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ, Постановление Правительства РФ от 03.11.1994 N 1233 «Об

утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»

7. Организация доступа и допуска к информации ограниченного доступа.

Цели выполнения лабораторной работы: Закрепление пройденного материала. Изучение документов: Закон РФ «О государственной тайне» от 21.07.1993 N 5485- 1, Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98- ФЗ

8. Текущая работа с персоналом, обладающим конфиденциальной информацией.

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Трудовой кодекс РФ, ГОСТ «ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст)

9. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации и утраты конфиденциальных документов.

Цель выполнения лабораторной работы: Закрепление пройденного материала;

10. Организация защиты информации при взаимодействии со сторонними организациями.

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: «ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (утв. и введен в действие Приказом Росстандарта от 24.09.2012 N 423-ст), Гражданский кодекс РФ; Приказ ФСТЭК России от 29 апреля 2021 г. N 77

11. Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно- правовых актов: Закон «О лицензировании отдельных видов деятельности». Постановление Правительства Российской Федерации от 15 апреля 1995 г. N 333 Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, Постановление Правительства Российской Федерации от 3 февраля 2012 г. N 79, о лицензировании деятельности по технической защите конфиденциальной информации. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ О техническом регулировании.

12. Правовая защита информации, составляющей интеллектуальную

собственность.

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Гражданский кодекс РФ, «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149- ФЗ, Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ

13. Особенности обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно- правовых актов: Федеральный закон от 26 июля 2017 г. N 187-ФЗ, Приказ ФСТЭК России от 25 декабря 2017 г. N 239

14. Правовая защита информации, составляющей персональные данные.

Цели выполнения лабораторной работы: Закрепление пройденного материала; работа с нормативно-правовыми актами: Федеральный закон от 27 июля 2006 г. N 152-ФЗ, Приказ ФСТЭК России от 18 февраля 2013 г. N 21; Приказ ФСБ России от 10 июля 2014 года N 378

15. Особенности правовой защиты сведений, составляющих различные виды тайн.

Цели выполнения лабораторной работы: Закрепление пройденного материала; поиск и работа с нормативно-правовыми актами по тематике.

16. Правовое обеспечение безопасности информации винформационных системах. Цели выполнения лабораторной работы: Закрепление пройденного материала; проработка нормативно-правовых актов: Доктрина информационной безопасности России, ГК РФ, УК РФ, КОАП РФ, Приказ ФСТЭК России от 11 февраля 2013 г. N 17, Приказ ФСТЭК России от 18 февраля 2013 г. N 21

Примерные вопросы

1. Дайте определение понятию «Информационная безопасность».
2. Какая информация входит в перечень сведений конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997г. № 188.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации». Какие отношения регулирует? Какие направления деятельности в области ИБ рассматриваются в данном законе?
4. В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», дайте определение понятиям «Информация», «Конфиденциальность информации», «Обладатель информации», «Доступ к информации», «Предоставление информации», «Распространение информации».
5. Понятие и основные признаки документированной информации?
6. Какая информация, в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации», относится к общедоступной, и как регулируются отношения при использовании такой информации?
7. Права и обязанности обладателя информации, в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации».

8. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

9. Какая информация запрещена к распространению, в соответствии с ФЗ «Об информации, информационных технологиях и о защите информации»?

10. Федеральный закон «О коммерческой тайне" от 29.07.2004 N 98-ФЗ. Ознакомиться. Описать. Чему посвящён закон? Какие отношения регулирует?

11. В соответствии с ФЗ «О коммерческой тайне», дайте определение понятиям «Коммерческая тайна», «Информация, составляющая коммерческую тайну», «Разглашение информации, составляющей коммерческую тайну».

12. Какие сведения, не могут составлять коммерческую тайну?

13. Кому принадлежит право на отнесение информации к разряду коммерческой тайны?

14. Какие меры по охране конфиденциальности информации должен предпринять её обладатель, чтобы режим коммерческой тайны считался установленным?

15. Имеет ли право обладатель информации, составляющей коммерческую тайну, применять средства технической защиты конфиденциальности этой информации? Укажите статью ФЗ «О коммерческой тайне», которая регулирует этот вопрос.

16. Какие меры по охране конфиденциальности информации, составляющей коммерческую тайну, должен предпринять работодатель в рамках трудовых отношений, в соответствии с ФЗ «О коммерческой тайне»?

17. Что обязан делать работник, в целях охраны конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений, в соответствии с ФЗ «О коммерческой тайне»?

18. В каком случае будет правомерным требование работодателя о возмещении убытков, причиненных ему разглашением коммерческой тайны, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем?

19. Верно ли утверждение о том, что работник, получивший доступ к коммерческой тайне, в случае разглашения этой информации, обязан возместить убытки, причиненные работодателю, даже в том случае, если меры по обеспечению режима коммерческой тайны, в отношении этой информации, работодателем не были соблюдены? Обоснуйте свой ответ.

20. Могут ли органы государственной власти требовать предоставления коммерческой тайны от обладателя этой информации? Как будут регулироваться отношения в случае отказа в предоставлении этих сведений?

21. Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1. Ознакомиться. Описать. Какие отношения регулирует? Какие направления деятельности в области ИБ рассматриваются в данном законе?

22. В соответствии с ФЗ «О государственной тайне», дайте определение понятию «Государственная тайна».

23. Какие сведения составляют государственную тайну?

24. Какие сведения, не могут составлять государственную тайну?

25. Принципы отнесения сведений к государственной тайне и

засекречивания этих сведений.

26. Что может послужить основанием для отказа должностному лицу или гражданину в допуске к государственной тайне?

27. Условия прекращения допуска должностного лица или гражданина к государственной тайне?

28. Как осуществляется допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну?

29. Дайте определение понятию «Интеллектуальная собственность»?

30. Кто может осуществлять защиту авторства после смерти автора?

31. Допускается ли переход исключительного права на результат интеллектуальной деятельности без заключения договора? Если да, то в каких случаях?

32. Будет ли признан автором результата интеллектуальной деятельности гражданин, организовавший работу по созданию такого результата и оказавший содействие по оформлению прав на такой результат? Обоснуйте свой ответ.

33. Чем отличается лицензионный договор от договора об отчуждении исключительного права?

34. Может ли лицензиат предоставить право использования результата интеллектуальной деятельности или средства индивидуализации другому лицу? Обоснуйте свой ответ

35. Может ли исключительное право на результат интеллектуальной деятельности принадлежать нескольким лицам совместно? Если да, то как определяются взаимоотношения между ними?

36. Какие правовые акты содержат нормы, регулирующие отношения в сфере интеллектуальной собственности?

37. Условия патентоспособности изобретений полезных моделей и промышленных образцов?

38. Что происходит с изобретением, полезной моделью или промышленным образом после прекращения действия исключительного права на них?

39. Основания и порядок продления срока действия исключительного права на объекты патентного права?

40. Открытая лицензия как форма распоряжения исключительным правом на изобретение, полезную модель или промышленный образец. Раскрыть суть.

41. В каком случае право на получение патента на служебное изобретение, служебную полезную модель или служебный промышленный образец, возвращается работнику?

42. Как решится вопрос о выдаче патента, если заявки, поданы разными заявителями на идентичные изобретения, полезные модели и промышленные образцы имеют одну и ту же дату приоритета?

43. Особенности подачи и рассмотрения заявки на выдачу патента на секретное изобретение.

44. Сроки действия исключительного права составителя базы данных и изготовителя базы данных?

45. Зависит ли наступление правовой охраны для программ ЭВМ и баз данных от государственной регистрации этих объектов?

46. Несет ли ответственность за нарушение исключительного права на секрет производства лицо, которое получило доступ к секрету производства случайно и не знало о том, что его использование незаконно?

47. Кому будет принадлежать исключительное право на секрет производства, полученный при выполнении работ по государственному контракту для государственных нужд.

48. Какие сведения не могут быть признаны ноу-хау? Приведите пример.

49. Дайте определение понятию «Персональные данные».

50. Перечислите принципы обработки персональных данных.

51. К какой категории сведений относятся персональные данные?

52. Каковы особенности обработки персональных данных в государственных или муниципальных информационных системах?

53. Классификация видов противоправных деяний в отношении компьютерной информации.

54. Способы и механизмы совершения компьютерных преступлений

55. Дайте понятие сертификации.

56. Основные нормативные акты в области лицензирования ЗИ.

57. Какие нормативные правовые акты по сертификации средств защиты информации?

58. Виды юридической ответственности за нарушение правовых норм по защите информации.

59. Уголовный кодекс РФ онаказаниях за правонарушения в области информационной безопасности.

60. Административные взыскания за нарушения правовых норм по защите информации.

61. Проведение административного расследования пофактам нарушения установленного порядка защиты информации.

62. Особенности трудовых отношений при нарушении правовых норм в сфере информационной безопасности.

11. Учебно-методическое обеспечение дисциплины

Основная литература

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т.А. Поляковой, А.А. Стрельцова. — Москва: Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534- 03600-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239.

2. Правовое обеспечение национальной безопасности: учебное пособие для вузов / Ю. Н. Туганов [и др.]; под редакцией Ю. Н. Туганова. — 2-е изд., перераб. и доп.— Москва: Издательство Юрайт, 2023. — 180 с. — (Высшее образование). — ISBN 978-5-534-16244-

8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530662.

3. Бельская, Н. М. Организационное и правовое обеспечение информационной безопасности: методические указания / Н. М. Бельская, Н. И. Козырева, И. С. Макаров. — Самара: ПГУТИ, 2024. — 31 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/301040

Дополнительная литература

1. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. —URL: https://urait.ru/bcode/512269

2. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515435

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

1. Лекции по физике: Полный курс лекций по физике. http://physics-lectures.ru
2. Вся физика – познавательный портал. http://www.webviki.ru/all-fizika.com 3. Российский образовательный портал по физике – ресурсы для студентов и преподавателей.

http://window.edu.ru/resource/343/24343

4. Наука мира – образовательный портал по физике. http://www.naukamira.ru

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной системе и электронной информационно-образовательной среде.

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) – 1.

Учебная аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) – 1.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от _____ 20___г., протокол №____