Высшая Школа Управления

Негосударственное образовательное частное учреждение высшего образования «Высшая школа управления» (ЦКО)
(НОЧУ ВО «Высшая школа управления» (ЦКО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДЭ.01.01 Правовая защита информации

Направление подготовки
38.03.05
«Бизнес-информатика»

Направленность (профиль) подготовки
Информационные системы в бизнесе

Квалификация выпускника
«Бакалавр»
Форма обучения
заочная

Рабочая программа рассмотрена
на заседании кафедры
цифровой экономики и управления и
государственного администрирования
«20» марта 2025 г. протокол №8

Заведующий кафедрой д.э.н., доцент
Н.Р. Куркина

г. Москва, 2025

Рабочая программа дисциплины «Правовая защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации № 838 от 20 июля 2020 года (зарегистрирован в Минюсте России 19 августа 2020 г. № 59325).

Организация-разработчик: НОЧУ ВО «Высшая школа управления» (ЦКО)

Разработчики: к.ю.н., доц. Д.В. Синьков, к.ю.н., доц. Федоров П.Ю., к.ю.н., доц. Федорова И.А.

Содержание

1. Цели и задачи освоения дисциплины 4
2. Место дисциплины в структуре образовательной программы 4
3. Планируемые результаты обучения 5
4. Структура и содержание дисциплины (модуля) 7
4.1 Объем дисциплины и виды учебной работы 7
4.2 Тематический план дисциплины 8
4.3 Содержание дисциплины 10
4.4. Практическая подготовка 13
5. Учебно-методическое, информационное и материально-техническое обеспечение дисциплины 13
5.1 Основная литература 13
5.2 Дополнительная литература 14
5.3 Профессиональные базы данных и информационные справочные системы 14
5.4 Материально-техническое и программное обеспечение (лицензионное и свободно распространяемое) 14
6. Методические указания для обучающихся по освоению дисциплины 15
6.1 Занятия лекционного и семинарского (практического) типов 15
6.2. Самостоятельная работа студентов 16
7. Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов 17
Приложение 1. Фонд оценочных средств 19
1. Паспорт фонда оценочных средств 20
2. Оценочные средства 21
2.1 Текущий контроль 21
2.2 Промежуточная аттестация 24

1. Цели и задачи освоения дисциплины

Целью освоения дисциплины является усвоение законодательно-правовых основ правового обеспечения информационной безопасности, принципов построения систем обеспечения информационной безопасности, анализа и оценки угроз информационной безопасности объектов, средств и методов физической защиты объектов, изучение лицензионной и сертификационной деятельности в области защиты информации.

Задачи дисциплины:

- формирование теоретических знаний в области правовых и организационных основ защиты информации, средств и методов защиты информации, построения и организации функционирования систем защиты информации в компьютерных системах, методов несанкционированного доступа и взлома;
- освоение приемов программной реализации известных криптоалгоритмов и алгоритмов сокрытия информации, защиты системного программного обеспечения;
- изучение вопросов политики безопасности, стандартов безопасности России и развитых стран; тенденций и перспектив развития средств защиты информации;
- выработка умения разрабатывать политику безопасности организации, организовать защиту рабочего места, локальной сети.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Правовая зашита информации» относится к элективным дисциплинам части, формируемой участниками образовательных отношений, блока Б1 «Дисциплины (модули)» учебного плана, согласно ФГОС ВО для направления подготовки 38.03.05 Бизнес-информатика.

3. Планируемые результаты обучения

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Планируемые результаты обучения
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.1.Формулирует совокупность задач в рамках поставленной цели проекта, решение которых обеспечивает ее достижение ИУК-2.2. Определяет связи между поставленными задачами, основными компонентами проекта и ожидаемыми результатами его реализации ИУК-2.3. Выбирает оптимальные способы планирования, распределения зон ответственности, решения задач, анализа результатов с учетом действующих правовых норм, имеющихся условий, ресурсов и ограничений, возможностей использования	**Знать** ● Основные принципы и методы правовой защиты информации, включая действующие правовые нормы в области защиты данных, интеллектуальной собственности, конфиденциальности и безопасности информации. ● Основы бизнес-ориентированных языков программирования, их преимущества и недостатки, а также области применения, которые могут быть полезны при разработке приложений для защиты информации.

ПК-4 Способен разрабатывать приложения на бизнес-ориентированных языках программирования	ИПК-4.1 Знать: основы бизнес-ориентированных языков программирования с учетом их преимуществ, недостатков, сфер применения ИПК-4.2 Уметь: разрабатывать прикладные приложения для профессиональной деятельности ИПК-4.3 Владеть: навыками выбора оптимальных технологий и инструментальных средств разработки оригинального приложения	● Принципы и подходы к выбору технологий и инструментов для разработки приложений, соответствующих правовым требованиям и стандартам защиты данных. **Уметь** ● Формулировать задачи и цели проектов в области правовой защиты информации, используя подходы, которые обеспечивают достижение поставленных целей с учётом правовых норм и условий. ● Определять взаимосвязи между задачами, компонентами проекта и результатами его реализации, учитывая требования законодательства и практики защиты данных. ● Планировать, распределять зоны ответственности, решать задачи и анализировать результаты проектов с учётом ресурсов, ограничений и возможностей, гарантируя соблюдение правовых норм и стандартов защиты информации. **Владеть** ● Навыками выбора и применения технологий для разработки приложений, соответствующих правовым требованиям по защите информации. ● Навыками выбора оптимальных инструментов для разработки приложений, которые обеспечивают защиту данных в соответствии с актуальными правовыми стандартами и нормами. ● Навыками планирования и реализации проектов с учетом правовых аспектов защиты информации, а также анализа результатов, чтобы обеспечить соответствие законодательным требованиям.

4. Структура и содержание дисциплины (модуля)

4.1 Объем дисциплины и виды учебной работы

Виды учебной работы	Объем в часах
Общая трудоемкость дисциплины	**108 (3 зачетные единицы)**
Контактная работа обучающихся с преподавателем (всего)	10
Аудиторная работа (всего), в том числе:	10
Лекции	4
Семинары, практические занятия	6
Лабораторные работы	
Внеаудиторная работа (всего):	98
в том числе: консультация по дисциплине	
Самостоятельная работа обучающихся (всего)	98
Вид промежуточной аттестации обучающегося	**Зачет с оценкой**

4.2 Тематический план дисциплины

Наименование разделов и тем	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)							Компетенции
		Всего	Из них аудиторные занятия			Самостоятельная работа	Курсовая работа	Контрольная работа	
			Лекции	Лабораторные работы	Практические/ семинарские занятия				
Тема 1. Основные понятия в области охраны и защиты информации	9	10	2		2	6			УК-2, ПК-4
Тема 2. Регламентация деятельности по информационной безопасности РФ	9	10	2		2	6			УК-2, ПК-4
Тема 3. Правовое регулирование вопросов в области государственной тайны	9	10			2	8			УК-2, ПК-4
Тема 4. Правовое регулирование вопросов в области остальных видов информации ограниченного доступа	9	10				10			УК-2, ПК-4
Тема 5. Правовое регулирование вопросов в области конфиденциальной информации	9	10				10			УК-2, ПК-4

Тема 6. Правовое обеспечение защиты информационных ресурсов	9	10				10			УК-2, ПК-4
Тема 7. Режим защиты государственных информационных систем	9	10				10			УК-2, ПК-4
Тема 8. Защита критической информационной инфраструктуры	9	10				10			УК-2, ПК-4
Тема 9. Аттестация объектов информатизации по требованиям безопасности информации	9	10				10			УК-2, ПК-4
Тема 10. Лицензирование и система сертификации средств защиты информации	9	10				10			УК-2, ПК-4
Тема 11. Ответственность за правонарушения в области информационной безопасности РФ	9	8				8			УК-2, ПК-4
Итого		**108**	**4**		**6**	**98**			

4.3 Содержание дисциплины

Тема 1. Основные понятия в области охраны и защиты информации

Понятие системы права. Понятие и виды защищаемой информации по российскому законодательству. Информация как объект гражданских прав. Виды информации, подлежащие защите в процессе обычного гражданского оборота. Четыре уровня правового обеспечения защиты информации. Характеристика уровней правового обеспечения защиты информации. Категории информации с ограниченным доступом.

Тема 2. Регламентация деятельности по информационной безопасности РФ

Органы законодательства, регламентирующие деятельность по информационной безопасности. Структура органов власти по защите информации в Российской Федерации. Совет Безопасности Российской Федерации. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ). Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ). Комитет по вопросам информационной безопасности. Анализ законодательства РФ в области информационной безопасности РФ. Конституционные основы правового обеспечения информационной безопасности РФ. Доктрина информационной безопасности РФ.

Тема 3. Правовое регулирование вопросов в области государственной тайны

Перечень сведений, отнесенных законодателем к категории: государственная тайна по сферам жизнедеятельности общества и государства. Правовой режим защиты государственной тайны. Степени секретности сведений и грифы секретности носителей этих сведений. Органы защиты государственной тайны. Три формы допуска к секретным сведениям. Организация допуска должностных лиц и граждан к государственной тайне. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности. Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Тема 4. Правовое регулирование вопросов в области остальных видов информации ограниченного доступа

Понятие коммерческой тайны. Правовой режим защиты коммерческой тайны. Требования для классификации сведений категории коммерческой тайны. Понятие банковской тайны. Объекты банковской тайны. Правовой режим защиты банковской тайны. Понятие профессиональной тайны. Требования для классификации сведений категории профессиональной тайны. Объекты профессиональной тайны.

Тема 5. Правовое регулирование вопросов в области конфиденциальной информации

Правовой режим защиты конфиденциальной информации. Понятие служебной тайны. Требования для классификации сведений категории служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне. Понятие персональных данных. Регуляторы в области защиты персональных данных. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Основные объекты интеллектуальной собственности. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области защиты интеллектуальной собственности в области конфиденциальной информации. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Тема 6. Правовое обеспечение защиты информационных ресурсов

Информационные ресурсы как объект защиты. Классификация информационных ресурсов. Государственные и негосударственные информационные ресурсы. Пользование информационными ресурсами. Системы защиты информационных ресурсов.

Тема 7. Режим защиты государственных информационных систем

Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем. Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Стадии и этапы создания системы

защиты государственных информационных систем (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации). Разработка эксплуатационной документации на систему защиты информации.

Тема 8. Защита критической информационной инфраструктуры

Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ. Меры по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и ее защищенности от компьютерных атак. Правила категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак.

Тема 9. Аттестация объектов информатизации по требованиям безопасности информации

Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее – система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная). Участники аттестации и их полномочия (компетенции). Задачи, функции права и обязанности органов по аттестации. Деятельность аттестационных комиссий.

Тема 10. Лицензирование и система сертификации средств защиты информации

Организационно-правовые основы лицензирования деятельности по защите информации. Лицензирование деятельности технической и криптографической защите информации. Порядок и методы проведения сертификационных испытаний средств защиты информации основных классов: технических средств защиты информации, защищенных технических средств обработки; информации, технических средств контроля защищенности информации, программных, аппаратных; средств защиты информации,

программных средств контроля защищенности информации. Особенности сертификации средств защиты информации от утечки по техническим каналам. Особенности сертификации средств защиты информации от НСД.

Тема 11. Ответственность за правонарушения в области информационной безопасности РФ

Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области конфиденциальной информации.

4.4. Практическая подготовка

Практическая подготовка реализуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Объем занятий в форме практической подготовки составляет 6 часов.

5. Учебно-методическое, информационное и материально-техническое обеспечение дисциплины

5.1 Основная литература

1. Алексеева, М. В. Защита конфиденциальной информации в российском праве / М. В. Алексеева. — СПб.: Питер, 2021. — 380 с.
2. Данилова, Н. И. Правовая защита информации в России: теория и практика / Н. И. Данилова. — М.: Юрайт, 2021. — 350 с.
3. Кабак, В. М. Охрана и защита информации в России: правовые основы / В. М. Кабак. — М.: Эксмо, 2021. — 290 с.
4. Климентьев, П. А. Ответственность за правонарушения в сфере информационной безопасности / П. А. Климентьев. — М.: Юридическая литература, 2021. — 310 с.
5. Смирнов, В. В. Правовое обеспечение защиты информации: Учебник для вузов / В. В. Смирнов. — М.: Инфра-М, 2022. — 420 с.

5.2 Дополнительная литература

1. Горбунова, Е. И. Охрана и защита информации в цифровую эпоху: современные подходы / Е. И. Горбунова. — М.: Аспект Пресс, 2022. — 312 с.

2. Кудрявцев, О. С. Лицензирование и сертификация средств защиты информации в России / О. С. Кудрявцев. — СПб.: Научный мир, 2021. — 360 с.
3. Москвин, А. В. Правовое регулирование вопросов конфиденциальной и государственной тайны в РФ / А. В. Москвин. — М.: Статут, 2020. — 280 с.
4. Седов, Р. А. Защита государственной тайны и информационная безопасность: правовые аспекты / Р. А. Седов. — М.: Вершина, 2022. — 350 с.
5. Федоров, А. А. Законодательство РФ в области информационной безопасности / А. А. Федоров. — М.: Норма, 2020. — 250 с.

5.3 Профессиональные базы данных и информационные справочные системы

1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа)
2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа)
3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)
4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)

5.4 Материально-техническое и программное обеспечение (лицензионное и свободно распространяемое)

Наименование дисциплины (модуля), практик в соответствии с учебным планом	**Наименование специальных помещений и помещений для самостоятельной работы**	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения.**
Б1.В.ДЭ.01.01 Правовая защита информации	Кабинет информационной безопасности	Учебные места, оборудованные блочной мебелью, компьютерами с выходом в сеть интернет, рабочее место преподавателя в составе стол, стул, тумба, компьютер преподавателя с выходом в сеть интернет, экран, мультимедийный проектор, телевизор, тематические стенды, презентационный	Microsoft Windows XP Professional Microsoft Office 2010 Kaspersky Endpoint для бизнеса КонсультантПлюс AdobeReader Cisco WebEx Информационно-коммуникационная платформа «Сферум»

		материал	
	Аудитория для самостоятельной работы	Учебные места, оборудованные блочной мебелью, компьютерами с выходом в сеть интернет, многофункциональное устройство	

6. Методические указания для обучающихся по освоению дисциплины

6.1 Занятия лекционного и семинарского (практического) типов

Методические указания для занятий лекционного типа. В ходе лекционных занятий обучающемуся необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из основной и дополнительной литературы, рекомендованной преподавателем и предусмотренной учебной программой дисциплины.

Методические указания для занятий семинарского (практического) типа. Практические занятия позволяют развивать у обучающегося творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Подготовка к практическому занятию включает два этапа. На первом этапе обучающийся планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор основной и дополнительной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку к занятию, которая начинается с изучения основной и дополнительной литературы. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. Далее

следует подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие или по теме, вынесенной на дискуссию (круглый стол), продумать примеры с целью обеспечения тесной связи изучаемой темы с реальной жизнью. Готовясь к докладу или выступлению в рамках интерактивной формы (дискуссия, круглый стол), при необходимости следует обратиться за помощью к преподавателю.

6.2. Самостоятельная работа студентов

Самостоятельная работа студентов предусмотрена учебным планом по дисциплине в объеме 98 часов. Самостоятельная работа реализуется в рамках программы освоения дисциплины в следующих формах:

- работа с конспектом занятия (обработка текста);
- проработка тематики самостоятельной работы;
- написание контрольной работы;
- поиск информации в сети «Интернет» и литературе;
- выполнение индивидуальных заданий;
- подготовка к сдаче зачета с оценкой.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний студентов;
- формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу;
- развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации;
- развитию исследовательских умений студентов.

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов: библиотека с читальным залом, компьютерные классы с возможностью работы в Интернет, аудитории для самостоятельной работы.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки.

Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся.

Контроль самостоятельной работы студентов предусматривает:

-соотнесение содержания контроля с целями обучения;

-объективность контроля;

-валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);

-дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы:

-просмотр и проверка выполнения самостоятельной работы преподавателем;

-организация самопроверки, взаимопроверки выполненного задания в группе;

-обсуждение результатов выполненной работы на занятии;

-проведение письменного опроса;

-проведение устного опроса; организация и проведение индивидуального собеседования;

-организация и проведение собеседования с группой.

7. Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Обучение по дисциплине обучающихся с ограниченными возможностями здоровья (далее – ОВЗ) осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Содержание образования и условия организации обучения, обучающихся с ОВЗ определяются адаптированной образовательной программой, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Освоение дисциплины обучающимися с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ОВЗ.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ОВЗ, индивидуальными программами реабилитации инвалидов (при наличии).

В курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании

комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий как оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).
- при необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

Фонд оценочных средств
для текущего контроля и промежуточной аттестации
при изучении дисциплины
Б1.В.ДЭ.01.01 Правовая защита информации

г. Москва, 2025

1. Паспорт фонда оценочных средств

Код и наименование компетенции	Индикатор достижения компетенции	Наименование оценочного средства
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	ИУК-2.1.Формулирует совокупность задач в рамках поставленной цели проекта, решение которых обеспечивает ее достижение ИУК-2.2. Определяет связи между поставленными задачами, основными компонентами проекта и ожидаемыми результатами его реализации ИУК-2.3. Выбирает оптимальные способы планирования, распределения зон ответственности, решения задач, анализа результатов с учетом действующих правовых норм, имеющихся условий, ресурсов и ограничений, возможностей использования	Текущий контроль: тестовое задание, контрольная работа Промежуточная аттестация: зачет с оценкой
ПК-4 Способен разрабатывать приложения на бизнес-ориентированных языках программирования	ИПК-4.1 Знать: основы бизнес-ориентированных языков программирования с учетом их преимуществ, недостатков, сфер применения ИПК-4.2 Уметь: разрабатывать прикладные приложения для профессиональной деятельности ИПК-4.3 Владеть: навыками выбора оптимальных технологий и инструментальных средств разработки оригинального приложения	

Этапы формирования компетенций в процессе освоения ООП прямо связаны с местом дисциплин в образовательной программе. Каждый этап формирования компетенций, характеризуется определенными знаниями, умениями и навыками и (или) опытом профессиональной деятельности, которые оцениваются в процессе текущего контроля успеваемости, промежуточной аттестации по дисциплине (практике) и в процессе итоговой аттестации. Дисциплина «Правовая защита информации» является промежуточным этапом формирования компетенций УК-2, ПК-4 в процессе освоения ООП.

Для оценки уровня сформированности компетенций в процессе изучения дисциплины предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачет с оценкой.

2. Оценочные средства

2.1 Текущий контроль

Типовое тестовое задание

Вопрос №1 . Совокупность всех работников предприятия, обеспечивающих реализацию его функций, работающие за вознаграждение, обладающий качественными характеристиками и имеющий трудовые отношения с работодателем — это...

Варианты ответов:

1. персонал предприятия
2. личный состав
3. трудовые кадры
4. трудовые реервы

Вопрос №2 . Необходимые и устойчивые взаимосвязи экономических отношений — это сущность...

Варианты ответов:

1. Экономических законов
2. Экономических институтов
3. Экономических формаций
4. Экономических наук

Вопрос №3 . Персонал предприятия - это:

Варианты ответов:

1. совокупность всех работников предприятия, обеспечивающих реализацию его функций, работающие за вознаграждение, обладающий качественными характеристиками и имеющий трудовые отношения с работодателем
2. личный состав, работающий по принуждению, обладающий качественными характеристиками и имеющий трудовые отношения с работодателем
3. личный состав, работающий по найму, обладающий качественными характеристиками и имеющий трудовые отношения с работодателем

Вопрос №4 . Экономические законы отражают:

Варианты ответов:

1. необходимые и устойчивые взаимосвязи экономических отношений
2. случайные и неповторяющиеся экономические взаимосвязи
3. количественные оценки экономических явлений и процессов
4. переходные состояния экономических процессов

Вопрос №5 .

По доступности информация классифицируется на

Варианты ответов:

1. открытую информацию и государственную тайну
2. конфиденциальную информацию и информацию свободного доступа
3. информацию с ограниченным доступом и общедоступную информацию
4. виды информации, указанные в остальных пунктах

Вопрос №6 .

К конфиденциальной информации относятся документы,

содержащие *Варианты ответов:*

1. сведения ограниченного доступа
2. законодательные акты
3. сведения о золотом запасе страны

Вопрос №7 .

Интеллектуальная собственность включает права, относящиеся к

Варианты ответов:

1. литературным, художественным и научным произведениям, изобретениям и
2. исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
3. промышленным образцам, товарным знакам, знакам обслуживания, фирменным
4. всему, указанному в остальных пунктах

Вопрос №8.

Формой правовой защиты литературных, художественных и научных произведений является (...) право

Варианты ответов:

1. литературное
2. художественное
3. авторское
4. патентное

Вопрос №9 .

Формой правовой защиты изобретений является

Варианты ответов:

1. институт коммерческой тайны
2. патентное право
3. авторское право
4. все, перечисленное в остальных пунктах

Вопрос №10 .

К коммерческой тайне могут быть отнесены

Варианты ответов:

1. сведения не являющиеся государственными секретами
2. сведения, связанные с производством и технологической информацией
3. сведения, связанные с управлением и финансами
4. сведения, перечисленные в остальных пунктах

Шкала оценивания тестового задания

% верных решений (ответов)	**Шкала оценивания**
85-100%	*«отлично»*
70-84%	*«хорошо»*
51-69%	*«удовлетворительно»*
50% и менее	*«неудовлетворительно»*

Примерные задания для контрольных работ

Задание 1

Определите, соответствуют ли ситуация принципам правового регулирования отношений

в сфере информации, информационных технологий и защиты информации: после проведения аудиторской проверки в государственной организации было выявлено нецелевое использование бюджетных средств. Местные средства массовой информации подготовили публикацию об использовании бюджетных средств, однако руководитель организации запретил публиковать данную информацию.

Задание 2
Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в ситуации: государственный фонд данных государственного экологического мониторинга включает в себя: информацию, содержащуюся в базах данных подсистем единой системы государственного экологического мониторинга; результаты производственного контроля в области охраны окружающей среды и государственного экологического надзора; данные государственного учета объектов, оказывающих негативное воздействие на окружающую среду.

Задание 3
Проведите анализ информационно-правовой нормы и определите вид формы предписания: Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах

Задание 4
Проведите анализ информационно-правовой нормы и определите вид формы предписания:

Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и осуществления эффективных мероприятий, направленных на защиту информации на объект информатизации.

Задание 5
Проведите анализ информационно-правовой нормы и определите вид формы предписания: организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям системы менеджмента информационной безопасности, с целью предотвратить их повторное появление.

Задание 6
Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в ситуации: юридическое лицо заключило с таможенным представителем договор представлять свои интересы при оформлении таможенной декларации и помещении товаров под определённую таможенную процедуру при перемещении товаров через таможенную границу Таможенного союза, и предоставил ему информацию о себе, товаре и его назначении.

Задание 7
Центральный банк РФ для анализа экономической ситуации запросил у АО «Тюмень Нефть» информацию о количестве полученной прибыли за прошедший год и о прогнозах объёма добычи нефти на текущий год. Однако АО не предоставило

истребуемой информации, мотивировав тем, что информация отнесена к коммерческой тайне. Имеет ли право Банк России получать данную информацию, и несёт ли ответственность Банк России, а также его должностные лица и работники за разглашение коммерческой тайны.

Задание 8
Вы – начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?
2. Какое наказание должен понести нарушитель?

Шкала и критерии оценивания контрольных работ

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся глубоко и содержательно раскрывает тему контрольной работы, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер.
«хорошо»	Обучающийся в целом раскрывает тему контрольной работы, однако ответ не носит развернутого и исчерпывающего характера.
«удовлетворительно»	Обучающийся в целом раскрывает тему контрольной работы и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.
«*неудовлетворительно*»	Обучающийся не владеет выбранной темой контрольной работы. Тема контрольной работы не раскрыта

2.2 Промежуточная аттестация

Примерные вопросы к зачету с оценкой

Тема 1. Основные понятия в области охраны и защиты информации

1. Понятие системы права.
2. Понятие и виды защищаемой информации по российскому законодательству.
3. Информация как объект гражданских прав.
4. Виды информации, подлежащие защите в процессе обычного гражданского оборота.
5. Четыре уровня правового обеспечения защиты информации.
6. Характеристика уровней правового обеспечения защиты информации.
7. Категории информации с ограниченным доступом.

Тема 2. Регламентация деятельности по информационной безопасности РФ

8. Органы законодательства, регламентирующие деятельность по информационной безопасности.
9. Структура органов власти по защите информации в Российской Федерации.
10. Совет Безопасности Российской Федерации.
11. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ).

12. Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ).
13. Комитет по вопросам информационной безопасности.
14. Анализ законодательства РФ в области информационной безопасности РФ.
15. Конституционные основы правового обеспечения информационной безопасности РФ.
16. Доктрина информационной безопасности РФ.

Тема 3. Правовое регулирование вопросов в области государственной тайны

17. Перечень сведений, отнесенных законодателем к категории: государственная тайна по сферам жизнедеятельности общества и государства.
18. Правовой режим защиты государственной тайны.
19. Степени секретности сведений и грифы секретности носителей этих сведений.
20. Органы защиты государственной тайны.
21. Три формы допуска к секретным сведениям.
22. Организация допуска должностных лиц и граждан к государственной тайне.
23. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.
24. Межведомственная комиссия по защите государственной тайны.
25. Полномочия.
26. Обеспечение деятельности.
27. Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны.
28. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Тема 4. Правовое регулирование вопросов в области остальных видов информации ограниченного доступа

29. Понятие коммерческой тайны.
30. Правовой режим защиты коммерческой тайны.
31. Требования для классификации сведений категории коммерческой тайны.
32. Понятие банковской тайны.
33. Объекты банковской тайны.
34. Правовой режим защиты банковской тайны.
35. Понятие профессиональной тайны.
36. Требования для классификации сведений категории профессиональной тайны. Объекты профессиональной тайны.

Тема 5. Правовое регулирование вопросов в области конфиденциальной информации

37. Правовой режим защиты конфиденциальной информации.
38. Понятие служебной тайны. Требования для классификации сведений категории служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне.
39. Понятие персональных данных. Регуляторы в области защиты персональных данных.
40. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

41. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных.
42. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
43. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.
44. Основные объекты интеллектуальной собственности.
45. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области защиты интеллектуальной собственности в области конфиденциальной информации. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Тема 6. Правовое обеспечение защиты информационных ресурсов

46. Информационные ресурсы как объект защиты.
47. Классификация информационных ресурсов.
48. Государственные и негосударственные информационные ресурсы.
49. Пользование информационными ресурсами.
50. Системы защиты информационных ресурсов.

Тема 7. Режим защиты государственных информационных систем

51. Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем.
52. Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.
53. Стадии и этапы создания системы защиты государственных информационных систем
(формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).
54. Разработка эксплуатационной документации на систему защиты информации.

Тема 8. Защита критической информационной инфраструктуры

55. Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ.
56. Меры по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и ее защищенности от компьютерных атак.
57. Правила категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений.
58. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов
КИИ РФ.
59. Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

60. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак.

Тема 9. Аттестация объектов информатизации по требованиям безопасности информации

61. Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее – система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.
62. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная).
63. Участники аттестации и их полномочия (компетенции). Задачи, функции права и обязанности органов по аттестации. Деятельность аттестационных комиссий.

Тема 10. Лицензирование и система сертификации средств защиты информации

64. Организационно-правовые основы лицензирования деятельности по защите информации.
65. Лицензирование деятельности технической и криптографической защите информации.
66. Порядок и методы проведения сертификационных испытаний средств защиты информации основных классов: технических средств защиты информации, защищенных технических средств обработки; информации, технических средств контроля защищенности информации, программных, аппаратных; средств защиты информации, программных средств контроля защищенности информации.
67. Особенности сертификации средств защиты информации от утечки по техническим каналам.
68. Особенности сертификации средств защиты информации от НСД.

Тема 11. Ответственность за правонарушения в области информационной безопасности РФ

69. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.
70. Меры дисциплинарной ответственности.
71. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности.
72. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Шкала и критерии оценивания зачета с оценкой

Шкала оценивания	Критерии оценивания
«отлично»	оценка соответствует повышенному уровню и выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«хорошо»	оценка соответствует повышенному уровню и выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос или выполнении заданий, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	оценка соответствует пороговому уровню и выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
«неудовлетворительно»	оценка выставляется обучающемуся, который не достигает порогового уровня, демонстрирует непонимание проблемы, не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.