МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2023

Рабочая программа дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Иванова А.В., старший преподаватель, Кафедра информационной безопасности, Ivanova.A@vvsu.ru

Шумик Е.Г., кандидат экономических наук, доцент, Кафедра математики и моделирования, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 18.05.2023 , протокол № 7

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000BBEDB4
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Организационное и правовое обеспечение информационной безопасности» является сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;.формирование у обучаемых профессиональных компетенций в эксплуатационно-технической и научно-исследовательской областях профессиональной деятельности.

Задачи дисциплины дать основы:

1. законодательства РФ в области информационной безопасности, защиты
2. понятий и видов защищаемой информации по законодательству РФ;
3. правовых основ защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);
4. организации и обеспечения режима конфиденциальности.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-5 : Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.2к : использует нормативные документы, регламентирующих работу по защите информации, а также положения, инструкции и другие организационно-распорядительных документы для решения поставленных задач	РД1	Знание	нормативные правовые акты по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем
	ОПК-5.1 : Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	ОПК-5.1.1к : определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД2	Умение	осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач с учетом требований нормативных правовых актов

			РД3	Знание	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах
			РД4	Умение	эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем
	ОПК-6 : Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1к : Применяет нормативно-правовые механизмы лицензирования, сертификации и аттестации; основные руководящие документы по обеспечению режима и конфиденциальности на объекте; основные документы, регламентирующие организационную безопасность на объекте	РД5	Навык	анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
			РД6	Знание	права и обязанности субъектов, осуществляющих деятельность в информационной сфере
			РД8	Навык	эффективной работы с электронными базами правовой информации, анализа нормативных правовых актов

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к базовой части дисциплин учебного плана направления «Информационная безопасность автоматизированных систем». Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Основы информационной безопасности». На данную дисциплину опираются «Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты», «Производственная преддипломная практика».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	6	5	91	36	36	0	1	18	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Место информационной безопасности в системе информационного права	РД1, РД2, РД3, РД8	6	6	0	17	
2	Правовое обеспечение информационной безопасности	РД1, РД5, РД8	6	6	0	18	
3	Лицензирование и сертификация в области защиты информации	РД5, РД8	8	8	0	18	
4	Правовые основы защиты конфиденциальной информации	РД1, РД2, РД4, РД6	8	8	0	18	
5	Юридическая ответственность за правонарушения в области информационной безопасности	РД2, РД5, РД7	8	8	0	18	
Итого по таблице			**36**	**36**	**0**	**89**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Место информационной безопасности в системе информационного права.

Содержание темы: Информационное право, как отрасль права. Понятие информации. Виды информации. Правовая информация как вид социальной информации. Классификация информации по уровню доступа (общедоступная информации, информация ограниченного доступа). Предмет информационно-правового регулирования. Международный характер информационного права. Комплексный характер информационного права. Соотношение информационного права со смежными отраслями права. Особенности формирования информационного права. Становление и развитие информационного права в России и в мире Право и его роль в регулировании комплекса отношений в информационной сфере. Понятие об информационном объекте и его элементах. Правовая информация, Официальная правовая информация, информация индивидуально правовая, неофициальная правовая информация. Юридические особенности и свойства информации. Информационно-правовые нормы и отношения. Система и источники информационного права. Информационные правоотношения. Объекты и субъекты информационных правоотношений. Информационно-правовые отношения: понятие, соотношение с правовой нормой, защита информационно-правовых отношений. Понятие и виды источников информационного права. Принципы информационного права. Информационные правоотношения. Объекты и субъекты информационных правоотношений. Виды информационно-правовых норм: по содержанию, по масштабу действия. Система нформационного права: общая часть; особенная часть. Принципы информационного права.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 2 Правовое обеспечение информационной безопасности.

Содержание темы: Понятие, предмет информационной безопасности. Понятие информационной безопасности, ее место в системе обеспечения национальной безопасности. Информационная безопасность личности, общества и государства. Основные задачи и методы обеспечения информационной безопасности. Понятие информационной безопасности личности. Соблюдение конституционных прав и свобод человека и гражданина в области информационных правоотношений. Запрет цезуры. Ограничения использования информации о частной жизни. Гарантии информационных прав граждан. Право на судебную защиту. Информационная безопасность общества Понятие информационной безопасности общества. Правовое регулирование средств информатизации, телекоммуникации и связи. Правовое регулирование единого информационного пространства. Информационная безопасность государства. Понятие информационной безопасности государства. Обеспечение защиты информационных ресурсов от несанкционированного доступа. Обеспечение безопасности информационных и телекоммуникационных систем Правовой режим защиты государственной тайны Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.

Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Перечень и содержание мер, направленных на защиту государственной тайны. Система контроля за состоянием защиты государственной тайны.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 3 Лицензирование и сертификация в области защиты информации.

Содержание темы: Лицензирование в области защиты информации Понятие лицензирования. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. Правовая регламентация лицензионной деятельности в области защиты информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Контроль за соблюдением лицензиатами условий ведения деятельности Сертификация в области защиты информации Понятие сертификации. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия. Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.).

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 4 Правовые основы защиты конфиденциальной информации.

Содержание темы: Защита интеллектуальной собственности Понятие интеллектуальной собственности. Нормативные правовые акты Российской Федерации, определяющие требования к защите авторских и смежных прав. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Законодательство РФ об интеллектуальная собственности. Понятие интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Защита авторских и смежных прав. Основы патентных правоотношений Условия патентоспособности. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Правовые режимы защиты конфиденциальной информации Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной

литературы.

Тема 5 Юридическая ответственность за правонарушения в области информационной безопасности.

Содержание темы: Ответственность за правонарушения в информационной сфере Особенности юридической ответственности в информационной сфере: понятие, виды, субъекты. Общая характеристика и виды ответственности за правонарушения в информационной сфере. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная). Компьютерные преступления и правовая защита от них. Преступления в сфере компьютерной информации. Преступления в сфере компьютерной информации. Правовые режимы защиты информации ведущих мировых держав.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 5 настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 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 (дата обращения: 12.04.2024).

2. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. - Воронеж : Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999941 (дата обращения: 11.04.2024).

7.2 Дополнительная литература

1. Актуальные проблемы информационного права : учебник / И. Л. Бачило, М. А. Лапина, Л. А. Букалерова [и др.] ; под ред. И. Л. Бачило, М. А. Лапиной. — Москва : Юстиция, 2019. — 592 с. — (Магистратура). — ISBN 978-5-4365-2987-5. — URL: https://book.ru/book/931052 (дата обращения: 26.02.2024). — Текст : электронный.

2. Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1359091 (дата обращения: 11.04.2024).

3. Торба, О. И., Правовое нормативное обеспечение защиты от информационных войн в области информационной безопасности : монография / О. И. Торба, Д. О. Торба, Ю. И. Коваленко, М. М. Тараскин. — Москва : Русайнс, 2021. — 582 с. — ISBN 978-5-4365-8828-5. — URL: https://book.ru/book/942308 (дата обращения: 26.02.2024). — Текст : электронный.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет",

включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "BOOK.ru"
3. Электронно-библиотечная система "ZNANIUM.COM"
4. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
5. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
6. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

· Проектор

· Доска аудиторная ДА-8МЦ

Программное обеспечение:

· СПС КонсультантПлюс: Версия Проф

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность и специализация

10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2023

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-5 : Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.2к : использует нормативные документы, регламентирующих работу по защите информации, а также положения, инструкции и другие организационно-распорядительных документы для решения поставленных задач
	ОПК-5.1 : Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	ОПК-5.1.1к : определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности
	ОПК-6 : Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1к : Применяет нормативно-правовые механизмы лицензирования, сертификации и аттестации; основные руководящие документы по обеспечению режима и конфиденциальности на объекте; основные документы, регламентирующие организационную безопасность на объекте

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.2к : использует нормативные документы, регламентирующих работу по защите информации, а также положения, инструкции и другие организационно-распорядительных документы для решения поставленных задач	РД1	Знание	нормативные правовые акты по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	перечисляет нормативные правовые акты по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем

Компетенция ОПК-6 «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-6.1к : Применяет нормативно-правовые механизмы лицензирования, сертификации и аттестации; основные руководящие документы по обеспечению режима и конфиденциальности на объекте; основные документы, регламентирующие организационную безопасность на объекте	РД 5	Навык	анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем	анализирует информационную инфраструктуры автоматизированной системы и ее безопасности с учетом специфики объекта; выбирает и обосновывает критериев эффективности функционирования защищенных автоматизированных информационных систем при разработке политики информационной безопасности
	РД 6	Знание	права и обязанности субъектов, осуществляющих деятельность в информационной сфере	Отвечает на вопросы по правам и обязанностям субъектов, осуществляющих деятельность в информационной сфере
	РД 8	Навык	эффективной работы с электронными базами правовой информации, анализа нормативных правовых актов	работает с электронными базами правовой информации, анализирует нормативные правовые акты в области защиты информации с учетом особенностей объекта исследования

Компетенция ОПК-5.1 «Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;»

Таблица 2.3 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.1.1к : определяет источники информации, регламентирующие деятельность, связанную с организацией политики безопасности	РД 2	Умение	осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач с учетом требований нормативных правовых актов	планирует организацию работы рабочего коллектива при выполнении поставленных задач

	РД3	Знание	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах	перечисляет угрозы безопасности информации и модели нарушителя в автоматизированных системах и принципы формирования политики информационной безопасности в автоматизированных системах
	РД4	Умение	эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем	использует криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывает частные политики информационной безопасности информационной безопасности автоматизированных систем

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : нормативные правовые акты по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	1.1. Место информационной безопасности в системе информационного права	Тест	Опрос
		1.2. Правовое обеспечение информационной безопасности	Тест	Опрос
		1.4. Правовые основы защиты конфиденциальной информации	Тест	Опрос
РД2	Умение : осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач с учетом требований нормативных правовых актов	1.1. Место информационной безопасности в системе информационного права	Практическая работа	Опрос
		1.4. Правовые основы защиты конфиденциальной информации	Практическая работа	Опрос
		1.5. Юридическая ответственность за правонарушения в области информационной безопасности	Практическая работа	Опрос

РД3	Знание : основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах	1.1. Место информационной безопасности в системе информационного права	Тест	Опрос
РД4	Умение : эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем	1.4. Правовые основы защиты конфиденциальной информации	Тест	Опрос
РД5	Навык : анализа информационной инфраструктуры автоматизированной системы и ее безопасности; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем	1.2. Правовое обеспечение информационной безопасности	Практическая работа	Опрос
		1.3. Лицензирование и сертификация в области защиты информации	Практическая работа	Опрос
		1.5. Юридическая ответственность за правонарушения в области информационной безопасности	Практическая работа	Опрос
РД6	Знание : права и обязанности субъектов, осуществляющих деятельность в информационной сфере	1.4. Правовые основы защиты конфиденциальной информации	Тест	Опрос
РД7	Умение : защищать информацию, в том числе обеспечивать ее конфиденциальность, с использованием правовых знаний в различных сферах деятельности; не нарушать права на информацию иных субъектов; содействовать нераспространению запрещенной законом информации	1.5. Юридическая ответственность за правонарушения в области информационной безопасности	Тест	Опрос
РД8	Навык : эффективной работы с электронными базами правовой информации, анализа нормативных правовых актов	1.1. Место информационной безопасности в системе информационного права	Практическая работа	Опрос
		1.2. Правовое обеспечение информационной безопасности	Практическая работа	Опрос
		1.3. Лицензирование и сертификация в области защиты информации	Практическая работа	Опрос

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Дифференцированный зачет	Итого
Лекционные занятия	50			50
Практические занятия		30		30
Промежуточная аттестация			20	20
Итого			20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, нет очности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры тестовых заданий

1. Термином «право» обозначается:

а) обоснованная, оправданная свобода или возможность поведения человека в его взаимоотношениях с другими людьми, которая признана и поддерживается обществом;

б) отрасль науки, которая изучает уголовный кодекс;

в) отрасль науки, которая изучает уголовный кодекс;

г) нет верного ответа.

2.В зависимости от формы проявления общественного признания этой свободы и способа ее поддержки со стороны общества различают следующие виды права:

а) обычное право, моральное право, корпоративное право;

б) обычное право, моральное право, корпоративное право, естественное право,

юридическое право;

в) естественное право, юридическое право;

г) корпоративное право, естественное право.

3. Юридическое право представляет собой:

а) систему общеобязательных норм, выраженных в только в уставах организаций;

б) свободу, или возможность поведения, основанную на принципах добра, справедливости (заботливое отношение детей к родителям, уважение к женщине);

в) свободу, или возможность поведения, основанную на уставных и иных положениях, которые действуют внутри общественных, негосударственных объединений, организаций, партий (право избирать и быть избранным в руководящие органы, право руководящих органов налагать взыскания);

г) систему общеобязательных норм, выраженных в законах, иных признаваемых государством источниках права и являющихся общеобязательным основанием для определения правомерно-дозволенного, запрещенного и предписанного поведения.

4. Наиболее известными в настоящее время правовыми системами являются:

а) религиозная, базирующаяся на священной для мусульман книге — Коране (мусульманское право характерно, например, для Ирана);

б) романо-германская, основанная на праве законодателя (континентальная Европа);

в) прецедентная, основанная на праве судей (Великобритания и США);

г) верны все варианты.

5. Предмет правового обеспечения информационной безопасности представляет собой:

а) совокупность общественных отношений, на которые направлено правовое воздействие в целях недопущения, выявления и пресечения проявлений угроз объектам национальных интересов в информационной сфере, а также минимизации негативных последствий проявления этих угроз;

б) совокупность общественных отношений, на которые направлено правовое воздействие только в целях недопущения проявлений угроз объектам национальных интересов в информационной сфере;

в) нет верного ответа.

6. Правовое обеспечение безопасности информации в форме сведений образуется:

а) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - сведений, обладателем которых является субъект права;

б) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;

в) совокупностью норм и институтов, регулирующих отношения по поводу только объекта - свобода мысли.

7. Правовое обеспечение безопасности информации в форме сообщений определяется:

а) совокупностью норм и институтов, регулирующих отношения по поводу следующих объектов: сведения, обладателем которых является субъект права; свобода мысли; субъективная значимость национальных культурных ценностей;

б) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются сообщения, передаваемые по каналам связи, данные, накапливаемые и обрабатываемые в информационных системах, автоматизированных системах управления, а также документы как входящие, так и не входящие в информационные системы;

в) совокупностью правовых норм и институтов, регулирующих отношения, объектами которых являются средства связи, автоматизации обработки информации, информационно-телекоммуникационные системы и средства массовой информации;

г) совокупностью правовых норм и институтов.

8. Содержание и структура законодательства в области информационной безопасности включает:

а) Конституция Российской Федерации - Нормативно-правовые акты (Указы)

Президента Российской Федерации - Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;

б) Конституция Российской Федерации - Нормативно-правовые акты (Указы) Президента Российской Федерации;

в) Подзаконные акты Правительства Российской Федерации - Федеральные законы - Кодексы;

г) нет верного ответа.

9. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации состоит из:

а) Федерального закона «Об информации, информационных технологиях и о защите информации» и других федеральных законов, регулирующих отношения в области использования информации;

б) Федерального закона «О персональных данных» и других федеральных законов, регулирующих отношения в области использования информации;

в) Федерального закона «О коммерческой тайне» и других федеральных законов, регулирующих отношения в области использования информации;

г) Федерального закона «О государственной тайне» и других федеральных законов, регулирующих отношения в области использования информации.

10. Предметом правового регулирования в области информации, информационных технологий и защиты информации являются:

а) отношения, возникающие только при осуществлении права на поиск, получение, передачу, производство и распространение информации;

б) отношения, возникающие только при применении информационных технологий; в) отношения, возникающие только при обеспечении защиты информации;

г) отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации.

11. Документированной информацией называют:

а) Информацию, зафиксированную на материальном носителе путем документирования, с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

б) Информацию, зафиксированную на материальном носителе путем документирования, без реквизитов;

в) нет верного ответа.

12. К общедоступной информации относятся:

а) общеизвестные сведения и иная информация, доступ к которой не ограничен после достижения определенного возраста;

б) общеизвестные сведения и иная информация, доступ к которой не ограничен;

в) нет верного ответа.

13. Различают следующие виды информационных систем:

а) государственные информационные системы, муниципальные информационные системы, иные информационные системы;

б) государственные информационные системы;

в) муниципальные информационные системы;

г) нет верного ответа.

14. Правовой режим информационных технологий включает:

а) порядок регулирования использования информационно коммуникационных сетей;

б) перечень областей государственного регулирования в сфере применения информационных технологий;

в) требования к государственным информационным системам;

г) верны все варианты.

15. Защита информации представляет собой принятие правовых, организационных и

технических мер, направленных:

а) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

б) соблюдение конфиденциальности информации ограниченного доступа;

в) реализацию права на доступ к информации;

г) верны все варианты.

16. В структуру государственной системы защиты информации РФ входят:

а) ФСБ РФ;

б) МВД РФ;

в) ФСТЭК;

г) ФСИН

17. Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:

а) отнесенные к государственной тайне;

б) отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн);

в) отнесенные к информации о прогнозах погоды; г) все верны ответы.

18. Как называется закон, регулирующий деятельность государственной тайны на территории РФ?

а) «О коммерческой тайне»;

б) «О государственной тайне»;

в) «О служебной тайне»;

г) «О врачебной тайне».

19. Нормативно-правовой акт - это:

а) правовой акт, принятый полномочным на то органом и содержащий правовые нормы, т. е. предписания общего характера и постоянного действия, рассчитанные на многократное применение;

б) правовой акт, принятый полномочным на то органом и содержащий правовые нормы, т. е. предписания общего характера и постоянного действия, рассчитанные на однократное применение;

в) нет верного ответа.

20. К информации ограниченного доступа относятся:

а) государственная тайна;

б) конфиденциальная информация;

в) персональные данные;

г) все ответы верны.

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, помнению студента, вариант ответа. В течение семестра проводится 5 тестов по 5 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Студент допустил не более 2х ошибок
4	5-7	Студент совершил от 3 до 6 ошибок в ответах на тест
3	3-4	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-2	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Задание.

1. Проанализировать информационные процессы выбранной Вами организации и

выявить критически важную информацию, которую необходимо защищать.

2. Разработать политику безопасности 1-го уровня организации в соответствии с требованиями нормативных документов.

3. Разработать частную политику безопасности. Объект политики выбирается исходя из специфики деятельности организации.

4. Подготовить презентацию выполненного проекта. Результат проекта. Результаты проекта представляют собой проекты Политики безопасности организации 1-го уровня и частной политики безопасности, а также презентация, отражающая основные этапы выполнения задания.

Краткие методические указания

Цель выполнения проекта заключается в формировании профессиональных компетенций обучаемых, выражающихся в способности участвовать в работах по разработке и реализации политики информационной безопасности. Примерный перечень организаций 1. Банк 2. УФМС 3. УКЦ 4. Аэропорт 5. Больница 6. Казначейство 7. Страховая компания 8. Фирма по разработке ПО 9. Юридическая фирма 10. Радиозавод 11. Дата-центр (ЦОД) 12. Аптека 13.Фирма, занимающаяся маркетинговыми исследованиями 14. Контора по ремонту и обслуживанию ПК 15. Интернет-провайдер 16. Система складских помещений 17. Психологическая клиника 18. Налоговая инспекция 19. Сотовый оператор 20. Железнодорожный вокзал 21. ЗАГС 22. ВУЗ 23. Магазин бытовой техники 24. Электростанция

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный ма териал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по суще ству излагает его, не допуская существенных неточностей в ответе на вопрос, правильно при меняет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные форму лировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной част и программного материала, допускает существенные ошибки.

5.3 Примерные вопросы

1. Понятие, предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.

2. Основные положения Концепции национальной безопасности Российской Федерации и Доктрины информационной безопасности Российской Федерации.

3. Определение понятия «государственная тайна». Перечень сведений, составляющих государственную тайну.

4. Правовые механизмы отнесения сведений к государственной тайне, рассекречивания сведений и их носителей.

5. Защита государственной тайны. Субъекты защиты государственной тайны, их функции в данной сфере. Контроль и надзор за обеспечением защиты государственной тайны.

6. Особенности правовой защиты сведений, составляющих государственную тайну.

7. Основные объекты института коммерческой тайны.

8. Субъекты информационных правоотношений, возникающих по поводу коммерческой тайны.

9. Правовой режим коммерческой тайны.

10. Защита прав на коммерческую тайну. Ответственность за нарушения при работе с коммерческой тайной.

11. Институты профессиональных тайн и их значение для обеспечения защиты прав и

свобод человека и гражданина, коммерческих интересов организаций и учреждений.

12. Основные категории сведений, защищаемых в режиме профессиональной тайны.

13. Система правового регулирования отдельных институтов профессиональных тайн.

14. Понятие и характеристика правонарушений в информационной сфере.

15. Криминалистическая характеристика преступлений в сфере компьютерной информации.

16. Ответственность за правонарушения в сфере компьютерной информации.

Контрольные работы целесообразно провести по окончании разделов дисциплины.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.