Компонент ОПОП **40.03.01 Юриспруденция**

«Направленность (профиль) Правоохранительная и правоприменительная деятельность»
наименование ОПОП

К.М.03.ДВ.02.02
шифр дисциплины

РАБОЧАЯ ПРОГРАММА

Дисциплины (модуля) ***Правовое регулирование информационной безопасности***

Разработчик (и):
Панкратова М.Е
ФИО

доцент,
должность

кандидат юридических наук, доцент
ученая степень, звание

Утверждено на заседании кафедры
Теории и истории государства и права
наименование кафедры

протокол № 6 от 04.02.2026 г.
заведующий кафедрой

Лобченко Л.Н.

Мурманск

2026

Пояснительная записка

Объем дисциплины 3 з.е.

1. Результаты обучения по дисциплине (модулю), соотнесенные с индикаторами достижения компетенций, установленными образовательной программой

Компетенции	Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	**1.1** Выполняет поиск необходимой информации, ее критический анализ и обобщает результаты анализа для решения поставленной задачи	*Знать:* задачу, выделяя ее базовые составляющие. *Уметь:* Определять, интерпретировать и ранжировать информацию, требуемую для решения поставленной задачи. *Владеть:* навыками анализа задач, применения системного подхода для решения поставленных задач
	1.2. Использует системный подход для решения поставленных задач, предлагает способы их решения	*Знать:* требуемые источники нормативной и иной информации *Уметь:* критически анализировать информацию *Владеть*: навыками поиска и критического анализа информации
ПК-2 Способен оценивать состояние законодательства, и вносить предложения по соблюдению и защите права и свободы человека и гражданина	**2.1** Определяет права и свободы человека как высшую ценность, основываясь на Конституции РФ и законодательстве	*Знать:* Конституционные права и гарантии человека и гражданина *Уметь:* определять права и свободы человека как высшую ценность *Владеть:* навыками оценки конституционного законодательства относительно прав и свобод
	2.2. Осуществляет профессиональную деятельность на основе уважения чести и достоинства личности, соблюдения прав и свобод человека и гражданина	*Знать:* Конституционные права и гарантии человека и гражданина, сущность их высшей ценности *Уметь* осуществлять профессиональную деятельность на основе уважения чести и достоинства личности *Владеть:* нормативными и иными навыками соблюдения прав и свобод человека и гражданина
	2.3 Обеспечивает различными способами защиту прав и свобод человека и гражданина в процессе своей профессиональной деятельности	*Знать:* Конституционные права и гарантии человека и гражданина, сущность их высшей ценности *Уметь:* обеспечивать различными способами защиту прав и свобод человека и гражданина *Владеть:* навыками защиты прав и свобод человека и гражданина в процессе своей профессиональной деятельности

	2.4. Вносит предложения по совершенствованию нормативных правовых актов, принимает участие во внесении изменений и дополнений в нормативные правовые акты	*Знать:* теоретические вопросы нормотворчества, его процедурных особенностей и юридическую технику *Уметь:* определять наиболее важные направления в нормотворчестве и вносить предложения по совершенствованию нормативных правовых актов *Владеть:* навыками внесении изменений и дополнений в нормативные правовые акты
ПК-4 Способен юридически правильно квалифицировать факты и обстоятельства	**4.1.** Определяет основания возникновения, изменения и прекращения правоотношений в рамках конкретных обстоятельств	*Знать:* современную нормативно-правовую базу с учетом изменений, происходящих в законодательстве; содержание Федеральных законов, иных нормативно-правовых актов, необходимых для реализации норм права в профессиональной деятельности; *Уметь*: пользоваться правовой информацией, анализировать ее с точки зрения поставленных задач; *Владеть:* навыками оказания юридической помощи, консультирование по частноправовым вопросам, в том числе по защите прав граждан и юридических лиц;
	4.2. Выявляет и анализирует факты, имеющие юридическое значение	*Знать:* основные этапы законодательного процесса и оформления их результатов; *Уметь:* ориентироваться в системе законодательства и нормативно-правовых актов общефедерального и регионального уровня; *Владеть:* навыками защиты прав и законных интересов граждан, юридических лиц, государственных и муниципальных образований;
	4.3. Дает правильную и обоснованную квалификацию юридическим фактам и обстоятельствам	*Знать:* порядок формирования, полномочия и основные формы работы общественных советов при федеральных и региональных органах государственной власти; *Уметь:* использовать нормативно-правовую документацию в сфере профессиональной деятельности; *Владеть:* профессиональными навыками по обеспечению конституционных прав человека;
	4.4. Правильно определяет юридические последствия квалифицируемых обстоятельств	*Знать:* основные задачи по организации работы по обеспечению законности и правопорядка, безопасности личности, общества, государства; *Уметь*: изучать развитие законодательства, регламентирующего формы взаимодействия государства и гражданского общества; *Владеть:* навыками осуществления правовой экспертизы нормативных правовых актов в целях юридически правильной квалификации фактов и обстоятельств, прежде всего, с точки зрения обеспечения соответствии действий и решений органов публичной власти Конституции и законодательству, а также - соблюдения основных прав и свобод человека и гражданина.

2. Содержание дисциплины (модуля)

Тема 1. Введение в проблематику информационной безопасности

В рамках темы рассматриваются понятие национальной безопасности и её неразрывная связь с информационной безопасностью, определяется место информационной безопасности в системе национальной безопасности Российской Федерации. Анализируется Доктрина информационной безопасности, её эволюция и ключевые положения. Освещается история становления проблемы информационной безопасности, выделяются основные этапы и предпосылки возникновения угроз. Изучается комплексный подход к обеспечению информационной безопасности, включающий организационную, правовую и техническую составляющие. Формируется понятийный аппарат защиты информации, раскрываются такие базовые категории, как объект защиты, уязвимость, угроза и способы защиты. Отдельное внимание уделяется организационно-правовому обеспечению информационной безопасности на уровне государства, системе нормативных правовых актов, регулирующих отношения в данной сфере, а также содержанию политики информационной безопасности на различных уровнях реализации.

Тема 2. Угрозы информационной безопасности

В данной теме раскрывается понятие угрозы для информации, рассматриваются источники угроз и условия их реализации. Проводится классификация угроз информационной безопасности по различным признакам: по природе возникновения, степени преднамеренности, характеру воздействия на информацию. Анализируются виды противников (нарушителей) — внешние и внутренние, их мотивы, возможности и категории. Изучаются виды возможных нарушений информационной системы, включая несанкционированный доступ, модификацию, уничтожение и блокирование информации. Особое внимание уделяется методам анализа угроз, оценке вероятности их реализации и возможного ущерба. Рассматриваются конкретные действия и события, которые могут привести к нарушению информационной безопасности, а также способы воздействия угроз на информационные объекты, будь то физические, программно-технические или организационно-правовые методы.

Тема 3. Вредоносные программы и противодействие им

Тема посвящена изучению вредоносных программ как одной из ключевых угроз информационной безопасности. Определяются обязательные условия вредоносности: несанкционированность, деструктивность и способность к распространению. Подробно рассматриваются разновидности вредоносных программ – классические вирусы, сетевые черви, троянские программы, клавиатурные перехватчики, логические бомбы, программы-шпионы, а также программы, захватывающие ресурсы компьютера. Описываются признаки заражения вредоносным программным обеспечением как технического, так и поведенческого характера. Анализируются меры ответственности за создание, распространение и использование вредоносных программ в соответствии с уголовным, административным и гражданским законодательством. Рассматриваются методы защиты корпоративной информационной среды, включая защиту интернет-подключений с применением межсетевых экранов, использование антивирусного программного обеспечения, а также защиту системы электронной почты и меры противодействия спаму.

Тема 4. Методы и средства защиты компьютерной информации

В данной теме формируется общее представление о структуре защищённой информационной системы, её уровнях и компонентах. Изучаются механизмы идентификации и аутентификации: парольные схемы, симметричные и асимметричные схемы аутентификации, аутентификация с третьей доверенной стороной на примере схемы Kerberos. Рассматриваются аппаратные средства аутентификации — токены и смарт-карты, а также использование биометрических данных. Освещаются сервисы управления доступом, включая дискреционный, мандатный и ролевой механизмы доступа, реализуемые в операционных системах и системах управления базами данных. Отдельное внимание уделяется протоколированию и аудиту: задачам и функциям аудита, структуре журналов аудита, методам активного аудита. Рассматриваются средства обеспечения защиты корпоративной информационной среды от атак на информационные сервисы, включая межсетевые экраны, организацию демилитаризованной зоны и использование виртуальных частных сетей. Изучаются

Тема 5. Криптографические методы информационной безопасности

Тема посвящена криптографическим методам защиты информации. Вводятся основные понятия криптологии, раскрываются различия между симметричными и асимметричными криптосистемами, а также принципы их построения. Рассматриваются способы создания симметричных криптосистем, понятие абсолютно стойкого шифра. Изучается криптографическая система DES и её модификации, а также отечественный алгоритм криптографического преобразования по ГОСТ 28147-89. Анализируются принципы построения асимметричных криптографических систем, их математическая основа и практическая реализация. Отдельное внимание уделяется правовому регулированию применения криптографических средств в Российской Федерации, включая вопросы лицензирования и требования со стороны уполномоченных органов. Рассматриваются основы использования электронной подписи, её правовое значение в соответствии с действующим законодательством.

Тема 6. Лицензирование и сертификация в области защиты информации. Критерии информационной безопасности, оценки рисков и управление её обеспечением

В заключительной теме изучается правовая основа лицензирования и сертификации в Российской Федерации, включая систему нормативных правовых актов, регулирующих данные отношения. Анализируются виды деятельности в информационной сфере, подлежащие лицензированию, прежде всего деятельность по технической защите информации, разработке и производству средств защиты информации, а также выявлению устройств негласного получения информации. Рассматриваются органы лицензирования, их полномочия и порядок получения лицензий. Раскрывается понятие сертификации применительно к средствам защиты информации, разграничиваются обязательная и добровольная сертификация, определяются органы сертификации и их полномочия. Освещается система государственного обеспечения информационной безопасности в Российской Федерации, структура уполномоченных органов и их взаимодействие. Изучаются оценочные стандарты и технические спецификации: «Оранжевая книга» (TCSEC) с её классами безопасности и механизмами защиты, рекомендации X.800, стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» (Common Criteria), а также руководящие документы Гостехкомиссии и ФСТЭК России. Завершается тема рассмотрением подходов к оценке рисков и управлению обеспечением информационной безопасности, включая создание системы менеджмента информационной безопасности на основе стандартов серии ISO/IEC 27000.

3. Перечень учебно-методического обеспечения дисциплины (модулю)

- Методические указания для практических занятий.
- Методические указания для самостоятельной работы.

4. Фонд оценочных средств по дисциплине (модулю)

Является отдельным компонентом образовательной программы, разработан в форме отдельного документа, представлен на официальном сайте МАУ в разделе «Информация по образовательным программам, в том числе адаптированным». ФОС включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля);
- задания текущего контроля;
- задания промежуточной аттестации;
- задания внутренней оценки качества образования.

5. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536902

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537000

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029

Дополнительная литература:

1. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5- 9765-1256-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843184

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1898839

3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290

4. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2022. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490026

6. Профессиональные базы данных и информационные справочные системы

1) Государственная система правовой информации - официальный интернет-портал правовой информации - URL: http://pravo.gov.ru

2) Информационная система «Единое окно доступа к образовательным ресурсам» - URL: http://window.edu.ru

3) Справочно-правовая система. Консультант Плюс - URL: http://www.consultant.ru/

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1) Офисный пакет Microsoft Office 2007

2) Система оптического распознавания текста ABBYY FineReader

8. Обеспечение освоения дисциплины лиц с инвалидностью и ОВЗ

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

9. Материально-техническое обеспечение дисциплины (модуля) представлено в приложении к ОПОП «Материально-технические условия реализации образовательной программы» и включает:

- учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения;

- помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде МАУ.

10. Распределение трудоемкости по видам учебной деятельности

Таблица 1 - Распределение трудоемкости

Вид учебной нагрузки	Распределение трудоемкости дисциплины по формам обучения											
	Очная				Очно-заочная				Заочная			
	Семестр			Всего часов	Семестр			Всего часов	Курс			Всего часов
		6				7				4/з		
Лекции		18		**18**		8		8		4		**4**
Практические работы		36		**36**		18		18		8		**8**
Самостоятельная работа		54		**54**		82		82		92		**92**
Подготовка к промежуточной аттестации		-		-		-		-		4		**4**
Всего часов по дисциплине		108		**108**		**108**		**108**		**108**		**108**
Экзамен		-		-		-		-		-		-
Зачет/зачет с оценкой		За		За		За		За		За		**За**
Курсовая работа (проект)		-		-						-		-
Количество расчетно-графических работ		-		-						-		-
Количество контрольных работ		-		-						-		-
Количество рефератов		-		-						-		-
Количество эссе		-		-						-		-

Перечень практических работ

№ п/п	Темы практических работ	Кол-во час		
		Очная	Очно-заочная	Заочная
1	Введение в проблематику информационной безопасности	6	3	1
2	Угрозы информационной безопасности	6	3	1
3	Вредоносные программы и противодействие им	6	3	2
4	Методы и средства защиты компьютерной информации.	6	3	2

5	Криптографические методы информационной безопасности.	6	3	-
6	Лицензирование и сертификация в области защиты информации. Критерии информационной безопасности, оценки рисков и управление её обеспечением.	6	3	2
	Итого:	**36**	**18**	**8**

Перечень примерных тем курсовой работы /проекта

№ п\п	**Темы курсовой работы /проекта**
1	**2**
1	
2	Не предусмотрены