Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ТЕОРИЯ И МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Уровень высшего образования: магистратура

Направление подготовки: 40.04.01 Юриспруденция

Направленность (профиль)подготовки: Правоохранительная и служебная деятельность органов внутренних дел

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 2 года

Объем: в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

г. Самара, 2026

Разработчики:
Кандидат юридических наук Петроградская А. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 40.04.01 Юриспруденция, утвержденного приказом Минобрнауки от 25.11.2020 № 1451, с учетом трудовых функций профессиональных стандартов: "Следователь-криминалист", утвержден приказом Минтруда России от 23.03.2015 № 183н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра теории права и публично-правовых дисциплин	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Ревина С. Н.	Рассмотрено	18.05.2026, № 9

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - Формирование у обучающихся системных теоретических знаний и практических методологических компетенций в области обеспечения информационной безопасности, позволяющих выявлять, оценивать и нейтрализовать угрозы информации в органах государственной власти, правоохранительной и иных профессиональных сферах с учётом действующего законодательства и современных вызовов.

Задачи изучения дисциплины:

- Изучить основы теории информационной безопасности, включая понятийно-категориальный аппарат, классификацию угроз и уязвимостей, модели нарушителя, а также методы и средства защиты информации в автоматизированных и информационно-телекоммуникационных системах.;
- Сформировать умения применять методологию комплексного подхода к обеспечению информационной безопасности — проводить анализ рисков, разрабатывать политики безопасности, выбирать организационные, правовые и технические меры защиты информации с учётом актуальных угроз и требований нормативных правовых актов.;
- Выработать владения навыками практического применения методов и средств защиты информации в профессиональной деятельности, включая мониторинг инцидентов, реагирование на утечки и управление системой информационной безопасности организации или органа власти..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

УК-2 Способен управлять проектом на всех этапах его жизненного цикла

УК-2.1 Разрабатывает концепцию проекта в условиях обозначенной проблемы

Знать:

УК-2.1/Зн1 Понимает методологию проектирования систем информационной безопасности, нормативно-правовой базы, моделей угроз и уязвимостей, принципов управления рисками.

Уметь:

УК-2.1/Ум1 Анализирует проблемную ситуацию, формулировать цели и задачи проекта, разрабатывать альтернативные варианты концепции, выбирать оптимальный с учётом ограничений (правовых, технических, бюджетных).

Владеть:

УК-2.1/Нв1 Владеет навыками разработки и защиты концепции проекта по обеспечению информационной безопасности, включая составление технического задания и обоснование выбранных мер защиты.

УК-2.3 Проводит оценку и анализ результативности проекта и корректирует процесс его осуществления

Знать:

УК-2.3/Зн1 Понимает критерии и показатели эффективности проектов в области информационной безопасности, методов мониторинга и оценки результативности

Уметь:

УК-2.3/Ум1 Собирает и анализирует данные о ходе реализации проекта, выявлять отклонения от плановых показателей, оценивать достижение целей по защите информации, разрабатывать обоснованные предложения по корректировке проектных решений

Владеть:

УК-2.3/Нв1 Владеет навыками подготовки отчётов об оценке результативности проекта, навыками внесения корректировок в проектную документацию, а также навыками оперативного реагирования на изменяющиеся угрозы и управленческие решения в рамках жизненного цикла проекта.

ПК-1 Способен организовать работу по отдельным направлениям правоохранительной и служебной деятельности органов внутренних дел, в том числе с использованием информационно-телекоммуникационных технологий, а также по предупреждению коррупционных и иных правонарушений и противодействию им

ПК-1.2 Планирует и организует мероприятия по предупреждению коррупционных и иных правонарушений

Знать:

ПК-1.2/Зн1 Знает нормативно-правовую базу противодействия коррупции, методы профилактики коррупционных проявлений и принципы организации антикоррупционной работы в органах власти и организациях.

Уметь:

ПК-1.2/Ум1 Выявляет коррупционные риски в информационных процессах, разрабатывать планы антикоррупционных мероприятий, определять перечень организационных и технических мер по их предупреждению, а также оценивать эффективность реализуемых антикоррупционных мер.

Владеть:

ПК-1.2/Нв1 Владеет навыками планирования и организации антикоррупционных проверок

ПК-3 Способен в пределах должностных полномочий организовать и проводить научные исследования в интересах органов внутренних дел

ПК-3.1 Определяет предмет, функции, методологии научного исследования в интересах органов внутренних дел, формы апробации и правила оформления его результатов

Знать:

ПК-3.1/Зн1 Понимает порядок организации научных исследований в системе МВД, требований к структуре НИР, методов научного познания, форм апробации и правил внедрения результатов в практическую деятельность органов внутренних дел.

Уметь:

ПК-3.1/Ум1 Формулирует предмет, цели и задачи исследования в сфере информационной безопасности, выбирает методологию, планирует формы апробации (публикации, конференции, отчёты) и разрабатывает предложения по внедрению результатов.

Владеть:

ПК-3.1/Нв1 Навыками подготовки программы и текста НИР, оформления отчётных документов, представления результатов на научных мероприятиях и подготовки проектов методических рекомендаций для внедрения в деятельность ОВД.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Теория и методология информационной безопасности» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 4.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-1 - Способен организовать работу по отдельным направлениям правоохранительной и служебной деятельности органов внутренних дел, в том числе с использованием информационно-телекоммуникационных технологий, а также по предупреждению коррупционных и иных правонарушений и противодействию им		
ПК-1.2 Планирует и организует мероприятия по предупреждению коррупционных и иных правонарушений	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Предупреждение преступлений и административных правонарушений органами внутренних дел, Производственная практика: преддипломная практика	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Предупреждение преступлений и административных правонарушений органами внутренних дел, Производственная практика: преддипломная практика
ПК-3 - Способен в пределах должностных полномочий организовать и проводить научные исследования в интересах органов внутренних дел		
ПК-3.1 Определяет предмет, функции, методологии научного исследования в интересах органов внутренних дел, формы апробации и правила оформления его результатов	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: научно-исследовательская работа, Производственная практика: преддипломная практика, Прокурорский надзор за деятельностью ОВД	Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика
УК-2 - Способен управлять проектом на всех этапах его жизненного цикла		
УК-2.1 Разрабатывает концепцию проекта в условиях обозначенной проблемы	Основы ОРД в ОВД, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: научно-исследовательская работа	Подготовка к процедуре защиты и защита выпускной квалификационной работы
УК-2.3 Проводит оценку и анализ результативности проекта и корректирует процесс его осуществления	Методика расследования административных правонарушений и преступлений, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: по профилю профессиональной деятельности	Подготовка к процедуре защиты и защита выпускной квалификационной работы

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Практические занятия (часы)	Групповая контактная работа (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация

Четвертый семестр	72	2	12	12	2	0,3	23,7	Экзамен
Всего	72	2	12	12	2	0,3	23,7	34

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Практические занятия	Самостоятельная работа
Раздел 1. Теоретические и методологические особенности информационной безопасности	**38**	**12**	**23,7**
Тема 1.1. Теоретические основы информационной безопасности	12	4	8
Тема 1.2. Методология обеспечения информационной безопасности	12,3	4	8
Тема 1.3. Управление информационной безопасностью и практическая деятельность	13,7	4	7,7

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	тестирование задание открытого типа
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Теоретические и методологические особенности информационной безопасности	тестирование задание открытого типа	Экзамен

6. Оценочные материалы текущего контроля

1. Теоретические и методологические особенности информационной безопасности тестирование

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	

1	Какой этап жизненного цикла проекта по созданию системы защиты информации предполагает формулирование целей, задач, ограничений и предварительную оценку ресурсов? 1. Инициация (концепция) 2. Завершение 3. Реализация Ответ: 1	УК-2
2	На каком этапе жизненного цикла проекта в области информационной безопасности осуществляется непосредственное внедрение программно-аппаратных средств защиты и обучение персонала? 1. Планирование 2. Реализация (исполнение) 3. Мониторинг и контроль Ответ: 2	УК-2
3	Какой документ фиксирует утверждённые цели, сроки, бюджет, основные этапы и ответственных за их выполнение в проекте по информационной безопасности? 1. Техническое задание 2. Акт внедрения 3. Устав проекта Ответ: 3	УК-2
4	Какой процесс управления проектом относится к этапу мониторинга и контроля жизненного цикла? 1. Разработка концепции защиты информации 2. Сопоставление плановых и фактических показателей, анализ отклонений 3. Формирование команды проекта Ответ: 2	УК-2
5	Каким документом завершается этап закрытия проекта по информационной безопасности? 1. Техническим заданием 2. Итоговым отчётом и актом приёмки-сдачи работ 3. Планом управления рисками Ответ: 2	УК-2
6	Соотнесите этап жизненного цикла проекта с его основным содержанием: Этап Содержание 1. Инициация А. Разработка календарного плана, бюджета, плана управления рисками и ресурсами 2. Планирование Б. Формулирование проблемы, целей и задач, разработка концепции, обоснование актуальности 3. Завершение В. Приёмка результатов, подготовка итогового отчёта, архивирование документации Ответ: 1 — Б 2 — А 3 — В	УК-2
7	Соотнесите действие руководителя проекта с этапом жизненного цикла, на котором оно выполняется: Действие Этап 1. Утверждение технического задания на разработку СЗИ А. Мониторинг и контроль 2. Сравнение фактических затрат с плановыми Б. Планирование 3. Подготовка отчёта о результатах внедрения системы защиты В. Завершение Ответ: 1 — Б 2 — А 3 — В	УК-2
8	Соотнесите документ проекта с этапом жизненного цикла, на котором он создаётся: Документ Этап 1. Концепция проекта по информационной безопасности А. Реализация 2. Акт о внедрении средств криптографической защиты Б. Инициация 3. План управления изменениями В. Планирование Ответ: 1 — Б 2 — А 3 — В	УК-2
9	Расположите в правильной последовательности этапы жизненного цикла проекта по созданию системы защиты информации в организации: 1. Инициация — определение проблемы, целей и задач, разработка концепции и обоснование необходимости проекта 2. Планирование — разработка календарного плана, бюджета, плана управления рисками, формирование команды 3. Реализация — непосредственное внедрение организационных и технических мер защиты, обучение персонала 4. Мониторинг и контроль — отслеживание выполнения плана, анализ отклонений, корректировка при необходимости 5. Завершение — приёмка результатов, подготовка итогового отчёта, архивирование документов, закрытие проекта Ответ: 1-2-3-4-5	УК-2

10	Расположите в правильной последовательности действия руководителя проекта при управлении изменениями на этапе реализации проекта по информационной безопасности: 1. Разработка и согласование решения — подготовка предложений по корректировке, получение одобрения от заказчика или проектного комитета 2. Мониторинг последствий — отслеживание эффективности внесённых изменений и при необходимости дальнейшая корректировка 3. Идентификация изменения — выявление факта, требующего корректировки (изменение законодательства, появление новой угрозы, срыв сроков) 4. Оценка влияния — анализ последствий изменения для сроков, бюджета, содержания и качества проекта 5. Внесение изменений — корректировка планов, документации, перераспределение ресурсов и актуализация задач для команды Ответ: 3-4-1-5-2	УК-2
11	Какой федеральный закон определяет правовые и организационные основы противодействия коррупции в Российской Федерации? 1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации…» 2. Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции» 3. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» Ответ: 2	ПК-1
12	Какое из перечисленных направлений использования ИКТ в деятельности органов внутренних дел непосредственно способствует предупреждению коррупционных правонарушений? 1. Внедрение системы «Посейдон» для автоматизированного контроля за доходами и расходами государственных служащих 2. Использование электронной почты для внутренней переписки 3. Автоматизация делопроизводства Ответ: 1	ПК-1
13	В соответствии с каким нормативным актом в системе МВД России организуется работа по противодействию коррупции с использованием информационных технологий? 1. Федеральный закон «Об оперативно-розыскной деятельности» 2. Указ Президента РФ от 25.04.2022 № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» 3. Приказ МВД России о ведении делопроизводства Ответ: 2	ПК-1
14	Какая мера относится к организационно-техническим способам предупреждения коррупционных правонарушений с использованием ИКТ? 1. Проведение бесед с личным составом о недопустимости коррупции 2. Увеличение заработной платы сотрудникам 3. Внедрение системы электронного документооборота с автоматической фиксацией всех действий пользователей Ответ: 3	ПК-1
15	Для каких целей в органах внутренних дел используются такие информационные базы данных, как ФИС ГИБДД-М, КАСБ ФМС и ИБД-Р? 1. Для обеспечения оперативно-справочной, розыскной, криминалистической и иной деятельности ОВД 2. Для ведения бухгалтерского учёта 3. Для хранения личных дел сотрудников Ответ: 1	ПК-1
16	Соотнесите направление деятельности ОВД с инструментом ИКТ, используемым для его реализации: Направление деятельности Инструмент ИКТ 1. Противодействие коррупции А. Единая информационно-телекоммуникационная система (ЕИТКС) для обмена данными 2. Оперативно-розыскная деятельность Б. Система видеофиксации и электронного документооборота в МФЦ 3. Информационное взаимодействие подразделений В. ГИС «Посейдон», автоматизированные проверки деклараций о доходах Ответ: 1 — В 2 — Б 3 — А	ПК-1

17	Соотнесите вид деятельности по предупреждению правонарушений с его содержанием: Вид деятельности Содержание 1. Профилактическая деятельность А. Использование специализированных информационных систем и межведомственного обмена 2. Информационно-аналитическое обеспечение Б. Выявление причин и условий, способствующих правонарушениям, и принятие мер по их устранению 3. Контрольная деятельность В. Мониторинг соблюдения антикоррупционных запретов и ограничений с использованием ИКТ Ответ: 1 — Б 2 — А 3 — В	ПК-1
18	Расположите в правильной последовательности алгоритм организации работы по предупреждению коррупции с использованием информационных технологий: 1. Выявление коррупционных рисков — анализ процессов, в которых наиболее вероятны коррупционные проявления (госзакупки, выдача разрешений и т.п.) 2. Внедрение мер ИКТ-контроля — перевод процессов в электронный вид, внедрение систем автоматической фиксации действий и разграничения доступа 3. Мониторинг и анализ данных — сбор и обработка информации из ИИС, выявление отклонений и аномалий, свидетельствующих о возможных нарушениях 4. Реагирование и корректировка — направление материалов в уполномоченные органы, принятие мер и совершенствование системы на основе выявленных недостатков Ответ: 1-2-3-4	ПК-1
19	Расположите в правильной последовательности действия сотрудника ОВД при организации профилактической работы с использованием ИКТ: 1. Анализ оперативной обстановки — изучение данных информационных баз (ИБД, ЕМИСС, статистики правонарушений) для определения проблемных зон 2. Разработка плана профилактических мероприятий — определение целей, задач, сроков и ответственных с учётом выявленных угроз и рисков 3. Реализация мероприятий — проведение проверок, использование систем автоматического контроля, информирование личного состава через служебные порталы 4. Оценка эффективности — сопоставление показателей правонарушений до и после проведения мероприятий, подготовка отчёта и корректировка плана Ответ: 1-2-3-4	ПК-1
20	Какой нормативный правовой акт определяет порядок организации и проведения научных исследований в системе МВД России? 1. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» 2. Приказ МВД России от 31.03.2021 № 198 «Об утверждении Наставления по организации научной деятельности в органах внутренних дел Российской Федерации» 3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации…» Ответ: 2	ПК-3
21	Какой из перечисленных методов научного исследования наиболее часто используется при изучении проблем информационной безопасности органов внутренних дел? 1. Метод исторической аналогии 2. Анализ информационных рисков и моделирование угроз 3. Герменевтический метод Ответ: 2	ПК-3
22	В каком разделе научно-исследовательской работы (НИР) содержатся конкретные практические рекомендации и предложения по совершенствованию деятельности ОВД в сфере информационной безопасности? 1. Введение 2. Основная часть (аналитический раздел) 3. Заключение и практические рекомендации Ответ: 3	ПК-3
23	Какой документ является итоговым результатом научного исследования в интересах органов внутренних дел и подлежит утверждению руководителем органа (организации) МВД? 1. Научный отчёт (отчёт о НИР) 2. Реферат 3. Докладная записка Ответ: 1	ПК-3
24	Какая форма апробации результатов научного исследования в области информационной безопасности считается основной в системе МВД России? 1. Публикация в коммерческих изданиях 2. Доклад на заседании учёного (экспертного) совета, научно-практической конференции 3. Размещение в открытом доступе в сети Интернет Ответ: 2	ПК-3

25	Соотнесите элемент структуры НИР с его содержанием: Элемент Содержание 1. Введение А. Изложение обоснованности и объективности выводов, предложения по совершенствованию деятельности ОВД 2. Основная часть (аналитическая) Б. Актуальность, объект, предмет, цели, задачи, методы исследования, обзор источников 3. Заключение и рекомендации В. Анализ состояния проблемы, оценка существующих подходов и предложение авторских решений Ответ: 1 — Б 2 — В 3 — А	ПК-3
26	Соотнесите метод научного исследования с его применением: Метод Применение 1. Анализ рисков А. Выявление тенденций в динамике правонарушений в сфере ИБ 2. Статистический анализ Б. Ранжирование угроз по вероятности и последствиям 3. Системный подход В. Рассмотрение информационной безопасности как единой системы с взаимосвязями элементов Ответ: 1 — Б 2 — А 3 — В	ПК-3
27	Соотнесите форму апробации с её назначением: Форма апробации Назначение 1. Выступление на конференции А. Проверка положений исследования в реальных условиях для выработки рекомендаций 2. Публикация в ведомственном журнале Б. Информирование научного сообщества и получение обратной связи 3. Внедрение в практическую деятельность В. Доведение результатов до сотрудников и руководства, использование в оперативной работе Ответ: 1 — Б 2 — В 3 — А	ПК-3
28	Расположите в правильной последовательности этапы организации научного исследования в интересах ОВД (согласно Наставлению): 1. Разработка программы исследования — выбор методов сбора и обработки данных, определение источников информации 2. Определение темы и актуальности — формулирование объекта, предмета, цели, задач, обоснование практической значимости 3. Сбор и анализ эмпирических материалов — изучение баз данных, нормативных актов, статистики, проведение опросов 4. Оформление результатов и подготовка отчёта — формулирование выводов, практических рекомендаций, подготовка заключительного отчёта Ответ: 2-1-3-4	ПК-3
29	Расположите в правильной последовательности этапы внедрения результатов научного исследования в практическую деятельность ОВД в сфере информационной безопасности: 1. Апробация результатов — обсуждение на научно-практических конференциях, семинарах, заседаниях экспертных советов 2. Разработка проекта нормативного или методического документа — подготовка инструкции, методических рекомендаций или приказа на основе научных выводов 3. Согласование и утверждение — прохождение процедуры согласования с заинтересованными подразделениями, утверждение руководством МВД 4. Внедрение и мониторинг — направление утверждённых документов в территориальные органы, обучение сотрудников, сбор обратной связи о результатах применения Ответ: 1-2-3-4	ПК-3

1. Теоретические и методологические особенности информационной безопасности задание открытого типа

№ п/п	Содержание вопроса Правильный ответ (ключ ответа)	Компетенция
1	Контрольный вопрос Какой документ, утверждаемый на этапе инициации проекта по информационной безопасности, содержит обоснование актуальности, цели, задачи, ожидаемые результаты и предварительную оценку ресурсов? Ответ: Концепция проекта по информационной безопасности.	УК-2
2	Контрольный вопрос На каком этапе жизненного цикла проекта создаются календарный план, бюджет, план управления рисками и формируется команда проекта? Ответ: Этап планирования.	УК-2

3	Контрольный вопрос Как называется процесс сопоставления плановых и фактических показателей проекта по защите информации с целью выявления отклонений и принятия корректирующих мер?		УК-2
	Ответ:	Мониторинг и контроль (или контроль исполнения).	
4	Контрольный вопрос При завершении проекта по информационной безопасности каким документом оформляется официальная приёмка результатов и фиксируется выполнение всех обязательств?		УК-2
	Ответ:	Акт приёмки-сдачи выполненных работ (или итоговый отчёт с актом).	
5	Контрольный вопрос Как называется заранее разработанная процедура, определяющая порядок внесения изменений в утверждённые сроки, бюджет или содержание проекта на этапе реализации?		УК-2
	Ответ:	План управления изменениями.	
6	Контрольный вопрос Какой федеральный закон является базовым нормативным правовым актом, определяющим систему мер противодействия коррупции в Российской Федерации?		ПК-1
	Ответ:	Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»	
7	Контрольный вопрос Как называется государственная информационная система, предназначенная для автоматизированного сбора, обработки и анализа сведений о доходах и расходах государственных служащих в целях профилактики коррупции?		ПК-1
	Ответ:	ГИС «Посейдон».	
8	Контрольный вопрос Какая мера организационно-технического характера, основанная на использовании ИКТ, позволяет исключить личный контакт заявителя с должностным лицом при получении государственной услуги и тем самым минимизировать коррупционные риски?		ПК-1
	Ответ:	Перевод государственных услуг в электронный вид через Единый портал госуслуг.	
9	Контрольный вопрос Какой метод контроля с использованием ИКТ обеспечивает фиксацию всех действий пользователей в информационной системе, что позволяет выявлять несанкционированные изменения и нарушителей?		ПК-1
	Ответ:	Аудиторский журнал (журнал регистрации событий безопасности).	
10	Контрольный вопрос Как называется процесс сбора и обработки информации из различных источников (баз данных, статистики, систем контроля) для выявления угроз и принятия профилактических мер в деятельности ОВД?		ПК-1
	Ответ:	Информационно-аналитическое обеспечение.	
11	Контрольный вопрос Какой нормативный документ регламентирует порядок организации и проведения научных исследований в системе Министерства внутренних дел Российской Федерации?		ПК-3
	Ответ:	Наставление по организации научной деятельности в органах внутренних дел Российской Федерации (приказ МВД России от 31.03.2021 № 198).	
12	Контрольный вопрос В каком разделе научно-исследовательской работы излагаются практические рекомендации по совершенствованию деятельности органов внутренних дел в сфере информационной безопасности?		ПК-3
	Ответ:	Заключение (или раздел практических рекомендаций).	
13	Контрольный вопрос Какой метод научного познания предполагает рассмотрение информационной безопасности как целостной системы с выделением взаимосвязей между её элементами?		ПК-3
	Ответ:	Системный подход.	
14	Контрольный вопрос Как называется форма апробации результатов исследования, предполагающая их обсуждение перед специалистами на заседании учёного или экспертного совета?		ПК-3
	Ответ:	Научный доклад (или выступление на заседании учёного совета).	
15	Контрольный вопрос Какой итоговый документ оформляется по завершении научно-исследовательской работы в системе МВД и утверждается руководителем органа (организации)?		ПК-3
	Ответ:	Отчёт о научно-исследовательской работе (НИР).	

7. Оценочные материалы промежуточной аттестации

7.1. Уровни овладения

Компетенция: УК-2 Способен управлять проектом на всех этапах его жизненного цикла.

Индикатор достижения компетенции: УК-2.1 Разрабатывает концепцию проекта в условиях обозначенной проблемы.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Индикатор достижения компетенции: УК-2.3 Проводит оценку и анализ результативности проекта и корректирует процесс его осуществления.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Компетенция: ПК-1 Способен организовать работу по отдельным направлениям правоохранительной и служебной деятельности органов внутренних дел, в том числе с использованием информационно-телекоммуникационных технологий, а также по предупреждению коррупционных и иных правонарушений и противодействию им.

Индикатор достижения компетенции: ПК-1.2 Планирует и организует мероприятия по предупреждению коррупционных и иных правонарушений.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100

Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Компетенция: ПК-3 Способен в пределах должностных полномочий организовать и проводить научные исследования в интересах органов внутренних дел.

Индикатор достижения компетенции: ПК-3.1 Определяет предмет, функции, методологии научного исследования в интересах органов внутренних дел, формы апробации и правила оформления его результатов.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Суворова, Г. М. Информационная безопасность: учебник для вузов / Г. М. Суворова. - 2-е изд. - Москва: Юрайт, 2026. - 277 с - 978-5-534-16450-3. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588515 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Щербак, А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. - 2-е изд. - Москва: Юрайт, 2026. - 252 с - 978-5-9916-4299-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589902 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. - 2-е изд. - Москва: Юрайт, 2026. - 107 с - 978-5-534-16388-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588741 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Чернова, Е. В. Информационная безопасность человека: учебник для вузов / Е. В. Чернова. - 3-е изд. - Москва: Юрайт, 2026. - 327 с - 978-5-534-16772-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/587699 (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. http://pravo.gov.ru/ - Государственная система правовой информации «Официальный интернет-портал правовой информации»
2. http://www.gov.ru/ - Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия»
3. http://www.gks.ru/ - Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики

Ресурсы «Интернет»

1. https://regulation.gov.ru - Федеральный портал проектов нормативных правовых актов
2. https://cyberleninka.ru/ - Научная электронная библиотека «КиберЛенинка»
3. https://digital.gov.ru - Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)
4. https://sudrf.ru - ГАС РФ «Правосудие»

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. Microsoft Windows XP;
2. Microsoft Word;
3. Microsoft Excel;
4. Microsoft Access;
5. 1С:Предприятие 8.3. Учебная версия;
6. Dr.Web Server Security Suite Антивирус + Центр управления, 2 серв., 12 мес.;
7. 1С:Документооборот государственного учреждения 8;
8. "Astra Linux Special Edition" РУСБ.10015-01;
9. "Антиплагиат.ВУЗ" версии 3.3;
10. Справочно-правовая система "Консультант Плюс";
11. 7-Zip;
12. Office 365;
13. Kaspersky Security для офисного 365;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

1. Справочно-правовая система "Гарант-Максимум";

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения