Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 23.11.2026 20:10:22
Уникальный программный ключ:
637517d24e103c3db03

Образовательное частное учреждение высшего образования
«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»
(ИМПЭ им. А.С. Грибоедова)

ЮРИДИЧЕСКИЙ ИНСТИТУТ

УТВЕРЖДАЮ:
Директор
Юридического института
_____/И.А. Близнец/
«12» октября 2026 г.

Рабочая программа дисциплины

Правовое обеспечение информационной безопасности

Специальность:
40.05.01 Правовое обеспечение национальной безопасности
(уровень специалитет)

Специализация:
«Государственно-правовая»

Формы обучения: очная

Москва

Рабочая программа дисциплины «Правовое обеспечение информационной безопасности». Специальность 40.05.01 Правовое обеспечение национальной безопасности, специализация: «Государственно-правовая» / В.И. Ступаков – М.: ИМПЭ им. А.С. Грибоедова

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта высшего образования – специалитет по специальности 40.05.01 Правовое обеспечение национальной безопасности, утвержденного приказом от 31 августа 2020 г. № 1138 Об утверждении Федерального государственного образовательного стандарта высшего образования - специалитет по специальности 40.05.01 Правовое обеспечение национальной безопасности

Разработчики:	В.И. Ступаков, к. ю. н., доцент
	Р.В. Закомолдин, кандидат юридических наук, доцент
Ответственный рецензент:	ведущий научный сотрудник НИИ Университета прокуратуры Российской Федерации, юрист 2 класса, почетный работник высшего профессионального образования Российской Федерации
	(Ф.И.О., уч. степень, уч. звание, должность)

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры национальной безопасности и правоохранительной деятельности 12.10.2026 г., протокол № 2.

Заведующий кафедрой _____/ к.ю.н., доцент В.А. Бодренков /

Согласовано от Библиотеки _____/О.Е. Стёпкина/

Раздел 1. Цели и задачи освоения дисциплины

Целью дисциплины «Правовое обеспечение информационной безопасности» является формирование у студентов комплекса теоретических знаний, практических умений и навыков, необходимых для выполнения служебных обязанностей на высоком профессиональном уровне.

Реализация дисциплины предполагает последовательное решение следующих задач:

- сформировать систему знаний о правовом режиме информации;
- изучить правовой режим отдельных видов информации;
- освоить правовые основы защиты информации;
- научиться применять нормы об ответственности за правонарушения в информационной сфере;
- развить навыки правовой экспертизы и практического применения законодательства;

Раздел 2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
ОПК-9	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ИОПК 9.1. Знает: принципы работы современных информационных технологий и использования их для решения задач профессиональной деятельности. ИОПК.9.2. Умеет: применять современные информационные технологии и использовать их для решения задач профессиональной деятельности. ИОПК.9.3. Владеет: навыки работы современных информационных технологий и использования их для решения задач профессиональной деятельности

Раздел 3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовое обеспечение информационной безопасности» изучается в 8 семестре очной формы обучения, относится к Блоку Б.1 «Дисциплины (модули)», «Часть, формируемая участниками образовательных отношений», образовательной программы по специальности 40.05.01 Правовое обеспечение национальной безопасности (уровень специалитет), специализация: «Государственно-правовая».

Раздел 4. Объем (трудоемкость) дисциплины (общая, по видам учебной работы, видам промежуточной аттестации)

Трудоемкость дисциплины и виды учебной работы

на очной форме обучения

з.е.	Итого	Лекции	Практические занятия	Курсовое проектирование	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация
8 семестр							
4	144	32	32		44		36, экзамен

Тематический план дисциплины

Очная форма обучения

Разделы / Темы	Лекции	Практические занятия	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация	Всего часов
8 семестр						
Тема 1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации	5	5	8			18
Тема 2. Информационная безопасность как объект правового регулирования	5	5	8			18
Тема 3. Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности	5	5	7			17
Тема 4. Защита государственной тайны	5	5	7			17
Тема 5. Информационные ресурсы	4	4	7			15
Тема 6. Регламентация вопросов защиты информации в Федеральных законах общего характер	4	4	7			15
Тема 7. Система документов в области обеспечения информационной безопасности и защиты информации	4	4	7			15
Экзамен					36	36
Итого по дисциплине	**32**	**32**	**44**		**36**	**108**

Структура и содержание дисциплины

№ п/п	Наименование раздела \темы	Содержание темы
1	Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации	Законодательство Российской Федерации в области информационной безопасности, защиты государственной тайны и конфиденциальной информации представляет собой комплексную иерархическую систему нормативно-правовых актов. Она строится на основе Конституции РФ и имеет трехуровневую структуру: стратегический, законодательный и подзаконный уровни.
2	Информационная безопасность как объект правового регулирования	Информационная безопасность в правовой системе Российской Федерации представляет собой состояние защищенности личности, общества и

		государства от внутренних и внешних информационных угроз. Она является объектом комплексного правового регулирования, которое осуществляется на стыке конституционного, административного, гражданского и уголовного права. Предметом регулирования выступают общественные отношения, возникающие в процессе защиты информации, информационных ресурсов и обеспечивающей их инфраструктуры. В 2025 году вектор правового регулирования сместился в сторону обеспечения технологического суверенитета. Ключевым изменением стала реформа законодательства о критической информационной инфраструктуре: требования по импортозамещению и переходу на отечественное программное обеспечение были закреплены непосредственно в профильном законе. Это обязало субъекты инфраструктуры переходить на доверенные программно-аппаратные комплексы. Параллельно была расширена Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, в рамках которой государственные органы и субъекты инфраструктуры обязаны в течение 24 часов информировать координационный центр о компьютерных атаках. Правовое воздействие осуществляется через установление специфических правовых режимов, сочетающих запреты, обязывания и дозволения. Система правового обеспечения включает механизмы лицензирования деятельности, обязательной сертификации средств защиты информации и категорирования объектов инфраструктуры по уровню их значимости. Иерархия нормативных актов выстраивается от Конституции РФ и Доктрины информационной безопасности до профильных федеральных законов и детальных ведомственных приказов.
3	Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности	Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности в Российской Федерации представляет собой иерархический комплексный правовой институт, объединяющий нормы конституционного, административного, гражданского и уголовного права. Она сформирована для защиты национальных интересов личности, общества и государства от внутренних и внешних информационных угроз и базируется на принципе технологического суверенитета.
4	Защита государственной тайны	Защита государственной тайны в Российской Федерации — это единая система правовых, административных, организационных и технических мер, направленных на предотвращение распространения сведений, разглашение которых

		может нанести ущерб безопасности государства. Правовой основой этой системы является Конституция РФ, Закон РФ от 21.07.1993 № 5485-1 "О государственной тайне", Закон "О безопасности", а также указы Президента и постановления Правительства.
5	Информационные ресурсы	Информационные ресурсы представляют собой отдельные документы, массивы документов, а также документы и массивы документов в информационных системах, таких как библиотеки, архивы, фонды и банки данных. Обязательным условием включения информации в ресурсы является её документирование — фиксация на материальном носителе с реквизитами, позволяющими её идентифицировать. Правовой режим информационных ресурсов — это совокупность правил, определяющих порядок их формирования, использования, доступа и защиты. Содержание этого режима включает четыре ключевых элемента: порядок документирования информации, право собственности на документы и массивы, категорию доступа к информации и порядок её правовой охраны. В зависимости от категории доступа правовой режим делится на общий, предполагающий свободный доступ к общедоступной информации, и специальные режимы, установленные для информации ограниченного доступа. К информации с ограниченным доступом, составляющей предмет специальных правовых режимов, относятся государственная тайна, коммерческая тайна, служебная, профессиональная тайна и персональные данные. Владельцы информационных ресурсов обязаны соблюдать принципы достоверности, конфиденциальности и доступности, а также нести ответственность за нарушение установленных правил защиты. Особый правовой статус приобретают государственные информационные ресурсы и ресурсы критической информационной инфраструктуры. Вводится обязательная идентификация пользователей через единую систему идентификации и аутентификации при регистрации доменных имен, а также ужесточаются требования к владельцам новостных агрегаторов и провайдерам хостинга, которые должны быть российскими юридическими лицами.
6	Регламентация вопросов защиты информации в Федеральных законах общего характер	Регламентация вопросов защиты информации в федеральных законах общего характера носит рамочный, фундаментальный характер и устанавливает базовые принципы, права и обязанности субъектов информационных отношений. Основным нормативным актом в этой

		сфере является Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации". Он определяет общие принципы правового регулирования, классифицирует информацию на общедоступную и ограниченного доступа, а также закрепляет базовое определение защиты информации как совокупности правовых, организационных и технических мер. Согласно статье 16 закона № 149-ФЗ, защита информации направлена на предотвращение неправомерного доступа, уничтожения, модифицирования или блокирования данных, а также на обеспечение соблюдения конфиденциальности и возможности восстановления информации. Обладатели информации и операторы информационных систем обязаны локализовать базы данных с персональными данными граждан РФ на территории России и принимать меры по недопущению воздействия на технические средства обработки данных. Ограничение доступа к информации допускается только федеральными законами в целях защиты конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, а также обеспечения обороны страны и безопасности государства.
7	Система документов в области обеспечения информационной безопасности и защиты информации	Система документов в области обеспечения информационной безопасности и защиты информации в Российской Федерации представляет собой многоуровневую иерархическую структуру, включающую нормативно-правовые и нормативно-методические акты. Эта система охватывает все уровни регулирования — от международного и конституционного до ведомственного и корпоративного.

Занятия семинарского типа
(Практические занятия)

Общие рекомендации по подготовке к практическим занятиям. При подготовке к работе во время проведения занятий практического типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний. Предварительная подготовка к учебному занятию практического типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия.

Работа во время проведения занятия практического типа включает несколько моментов: а) консультирование обучающихся преподавателями с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач; б) самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Тема 1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации

Вопросы и/или задания

1. Каким образом Доктрина информационной безопасности РФ, не являясь нормативным правовым актом прямого действия, влияет на содержание федеральных законов и ведомственных приказов?
2. В чем заключается принципиальное различие правовых режимов защиты государственной тайны и коммерческой тайны с точки зрения субъекта, устанавливающего режим, и оснований для ограничения доступа?
3. Каким образом изменения 2025 года в ФЗ "О безопасности КИИ" трансформируют обязанности частных компаний, владеющих объектами в сфере энергетики или транспорта, в части обеспечения технологической независимости?
4. Как соотносятся административная ответственность за разглашение тайны в СМИ (ст. 13.15 КоАП РФ) и уголовная ответственность за государственную измену в условиях современной правовой системы?
5. Какова роль методических документов ФСТЭК России в процессе легитимизации используемых средств защиты информации в государственных органах?

Тема 2. Информационная безопасность как объект правового регулирования

Вопросы и/или задания

1. Каким образом включение требований по импортозамещению в законодательство о критической информационной инфраструктуре изменило правовой статус субъектов и их обязанности по обеспечению технологической устойчивости?
2. В чем заключается комплексный характер правового регулирования информационной безопасности и как соотносятся нормы административного и уголовного права при квалификации киберинцидентов?
3. Какова роль правовых режимов в дифференциации ответственности и мер защиты для различных категорий информации, таких как государственная тайна, персональные данные и служебная информация?
4. Каким образом расширение полномочий государственной системы обнаружения компьютерных атак и введение обязанности информировать о самих атаках влияет на объем юридических рисков для государственных корпораций?
5. Какую роль играют разъяснения высших судебных инстанций в формировании единообразной практики применения норм об информационной безопасности при наличии пробелов в текущем законодательстве?

Тема 3. Система законодательного регулирования общественных отношений в области обеспечения информационной безопасности

Вопросы и/или задания

1. Каким образом иерархия нормативных актов (от Конституции и Доктрины до приказов ФСТЭК) обеспечивает баланс между защитой конституционных прав граждан на информацию и необходимостью обеспечения национальной безопасности?
2. Как изменения 2025 года в ФЗ "О безопасности критической информационной инфраструктуры" (в части импортозамещения и контроля структуры собственности) трансформируют правовой статус частных компаний, владеющих значимыми объектами инфраструктуры?
3. В чем заключается комплексный характер правового института информационной безопасности и как нормы гражданского, трудового и уголовного права взаимодействуют при расследовании утечки данных в коммерческой организации?
4. Какова роль созданной в 2025 году государственной антифрод-системы в перераспределении юридической ответственности между финансовыми организациями, операторами связи и цифровыми платформами за предотвращение кибермошенничества?
5. Каким образом новые требования Приказа ФСТЭК № 117 к защите государственных информационных систем влияют на обязанности муниципалитетов и бюджетных учреждений, ранее имевших упрощенные режимы безопасности?

Тема 4. Защита государственной тайны

Вопросы и/или задания

1. Каким образом изменения в Законе "О государственной тайне" (в частности, новая редакция определения гостайны от 2023 года) уточняют критерии ущерба безопасности РФ для отнесения сведений к той или иной степени секретности?
2. Каковы правовые последствия для гражданина, имеющего допуск к государственной тайне, в случае установления его постоянного проживания за границей или наличия у него близких родственников с иностранным гражданином согласно Постановлению Правительства № 132?
3. В чем заключается разграничение полномочий между Межведомственной комиссией по защите государственной тайны и руководителями федеральных органов исполнительной власти при формировании развернутых перечней засекречиваемых сведений?
4. Каков правовой статус "носителей сведений, составляющих государственную тайну", и как закон регулирует ограничение права собственности организаций и граждан на информацию в связи с ее засекречиванием (ст. 10 Закона)?
5. Каким образом система защиты государственной тайны интегрируется с мерами по защите критической информационной инфраструктуры (КИИ) в случаях, когда объекты КИИ одновременно обрабатывают сведения, составляющие государственную тайну?

Тема 5. Информационные ресурсы

Вопросы и/или задания

1. Как соотносятся понятия "информация", "документированная информация" и "информационный ресурс" в контексте возникновения права собственности на них?
2. Каким образом правовой режим информационных ресурсов ограничивает принцип свободы информации, закрепленный в Конституции РФ, и какие основания для введения таких ограничений являются законными?
3. В чем заключается специфика правового режима государственных информационных ресурсов по сравнению с ресурсами, находящимися в частной собственности?
4. Как изменения в ФЗ № 149-ФЗ, касающиеся регистрации доменных имен и идентификации пользователей (вступающие в силу в 2026 году), трансформируют правовой статус владельцев сайтов и провайдеров хостинга?
5. Какова роль категории "документирование" в определении информационного ресурса и какие юридические последствия наступают при отсутствии надлежащего документирования информации?

Тема 6. Регламентация вопросов защиты информации в Федеральных законах общего характер

Вопросы и/или задания

1. Каким образом статья 9 закона № 149-ФЗ определяет баланс между конституционным правом граждан на поиск и получение информации и законными основаниями для ограничения доступа к ней?
2. В чем заключается различие в правовом статусе информации, защищаемой в рамках законов общего характера (например, коммерческой тайны), и информации, защищаемой специальными законами (государственная тайна)?
3. Каким образом требования статьи 16 закона № 149-ФЗ о локализации баз данных на территории РФ соотносятся с принципами трансграничной передачи данных в условиях глобализации информационных потоков?
4. Как изменения 2025 года в регулировании критической информационной инфраструктуры (КИИ) расширили понятие безопасности, включив в него технологическую независимость и контроль цепочек поставок?
5. Какова роль государства в установлении требований к защите общедоступной информации и в каких случаях такие требования могут быть признаны законными?

Тема 7. Система документов в области обеспечения информационной безопасности и защиты информации

Вопросы и/или задания

1. Каким образом иерархия документов (от ФЗ до локального регламента) обеспечивает принцип "законности" при внедрении средств защиты информации в коммерческой организации?
2. Какова юридическая сила методических документов ФСТЭК России (например, Методики анализа защищенности 2025 года) для частных компаний, не являющихся субъектами КИИ?
3. Как соотносятся требования международных стандартов (серия ISO/IEC 27000) и национальных ГОСТов в рамках системы управления информационной безопасностью российского предприятия?
4. Каким образом Указы Президента РФ и Доктрина информационной безопасности влияют на содержание технических заданий на создание государственных информационных систем?
5. Какова роль стандартов (ГОСТ) в процессе сертификации средств защиты информации и почему их применение часто является добровольным, но де-факто обязательным для прохождения аттестации систем?

Раздел 5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Наряду с чтением лекций и проведением практических занятий неотъемлемым элементом учебного процесса является *самостоятельная работа.* При самостоятельной работе достигается конкретное усвоение учебного материала, развиваются теоретические способности, столь важные для успешной подготовки и защиты выпускной работы обучающегося. Формы самостоятельной работы, обучаемых могут быть разнообразными. Самостоятельная работа включает: изучение литературы, веб-ресурсов, оценку, обсуждение и рецензирование публикуемых статей; ответы на контрольные вопросы; решение задач; самотестирование. Выполнение всех видов самостоятельной работы увязывается с изучением конкретных тем.

Типовые задания для самостоятельной работы и примерная тематика курсовых работ (проектов), предусмотренных учебным планом, представлены в фонде оценочных средств по дисциплине.

Раздел 6. Оценочные и методические материалы по образовательной программе (фонд оценочных средств) для проведения текущего контроля успеваемости и промежуточной аттестации

В процессе освоения учебной дисциплины для оценивания сформированности требуемых компетенций используются оценочные материалы (фонды оценочных средств).

Типовые тестовые задания, типовые практические задания, типовые задания для контрольных работ, материалы для оценки результатов промежуточной аттестации и материалы для диагностической работы представлены в фонде оценочных средств по дисциплине.

Методические материалы, определяющие процедуру оценивания сформированных компетенций в соответствии с ООП

Качество знаний характеризуется способностью обучающегося точно, структурированно и уместно воспроизводить информацию, полученную в процессе освоения дисциплины, в том виде, в котором она была изложена в учебном издании или преподавателем.

Умения, как правило, формируются на занятиях семинарского типа. Задания, направленные на оценку умений, в значительной степени требуют от обучающегося проявления стереотипности мышления, т.е. способности выполнить работу по образцам, с

которыми он работал в процессе обучения. Преподаватель же оценивает своевременность и правильность выполнения задания.

Навыки можно трактовать как автоматизированные умения, развитые и закрепленные осознанным самостоятельным трудом. Навыки формируются при самостоятельном выполнении обучающимися практико-ориентированных заданий, моделирующих решение им производственных и социокультурных задач в соответствующей области профессиональной деятельности, как правило, при выполнении домашних заданий, курсовых проектов (работ), научно-исследовательских работ, прохождении практик, при работе индивидуально или в составе группы и т.д.

Устный опрос – это процедура, организованная как специальная беседа преподавателя с группой обучающихся (фронтальный опрос) или с отдельными обучающимися (индивидуальный опрос) с целью оценки сформированности у них основных понятий и усвоения учебного материала. Устный опрос может использоваться как вид контроля и метод оценивания формируемых компетенций (как и качества их формирования) в рамках самых разных форм контроля, таких как: собеседование, коллоквиум, зачет, экзамен по дисциплине. Устный опрос (УО) позволяет оценить знания и кругозор обучающегося, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. УО обладает большими возможностями воспитательного воздействия преподавателя. Воспитательная функция УО имеет ряд важных аспектов: профессионально-этический и нравственный аспекты, дидактический (систематизация материала при ответе, лучшее запоминание материала при интеллектуальной концентрации), эмоциональный (радость от успешного прохождения собеседования) и др. Обучающая функция УО состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту или экзамену. УО обладает также мотивирующей функцией: правильно организованные собеседование, коллоквиум, зачёт и экзамен могут стимулировать учебную деятельность студента, его участие в научной работе.

Тесты являются простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест может предоставлять возможность выбора из перечня ответов (один или несколько правильных ответов).

Семинарские занятия. Основное назначение семинарских занятий по дисциплине – обеспечить глубокое усвоение обучающимися материалов лекций, прививать навыки самостоятельной работы с литературой, воспитывать умение находить оптимальные решения в условиях изменяющихся отношений, формировать современное профессиональное мышление обучающихся. На семинарских занятиях преподаватель проверяет выполнение самостоятельных заданий и качество усвоения знаний, умений, определяет уровень сформированности компетенций.

Раздел 7. Методические указания для обучающихся по основанию дисциплины

Освоение обучающимся учебной дисциплины предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы учебной дисциплины. Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе Университета. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку: знакомит с новым учебным материалом;

разъясняет учебные элементы, трудные для понимания; систематизирует учебный материал; ориентирует в учебном процессе.

С этой целью: внимательно прочитайте материал предыдущей лекции; ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции; внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради; запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции; постарайтесь уяснить место изучаемой темы в своей подготовке; узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия.

Самостоятельная работа. Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала.

Подготовка к зачету, экзамену. К зачету, экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты. При подготовке к зачету обратите внимание на защиту практических заданий на основе теоретического материала. При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения

Раздел 8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 5-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2026. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/162521/details

2. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 с. — ISBN 978-5-4487-1026-1. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/142805/details

Дополнительная литература

3. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : Российский государственный университет правосудия имени В.М. Лебедева, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/152309/details

4. Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2023. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Образовательная платформа IPR CMAPT : [сайт]. — URL: https://www.iprbookshop.ru/books/141624/details

8.1. Требования к материально-техническому и учебно-методическому обеспечению программы специалитета

8.1.1. Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех

видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).

В Университете имеются специализированные аудитории для проведения занятий по информационным технологиям.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.

Электронная информационно-образовательная среда Университета включает:

1. Официальный сайт Университета (https://www.iile.ru/)
2. Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)
3. Программы для ЭВМ. Система дистанционного обучения «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 01.07.2026 по 30.06.2027 г.) https://impe.lms.mirapolis.ru/mira/
4. Программа для ЭВМ. Виртуальная комната «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 01.07.2026 по 30.06.2027 г.) https://impe.lms.mirapolis.ru/mira/
5. Система тестирования INDIGO лицензионное соглашение (Договор от 07.11.2018 г. №Д-54792, бессрочно) http://212.48.35.211:85/

8.1.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

1. Операционная система «Атлант» - Atlant Academ от 24.01.2024 г. (бессрочно)
2. Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition договор-оферта № Tr000941765 от 16.10.2025 г.

8.1.3. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и обновляется при необходимости, но не реже одного раз в год.

Перечень современных профессиональных баз данных и информационных справочных систем:

1. Информационно-поисковая система «Консультант Плюс» - Договор №МИ-ВИП-79717-56/2022 (бессрочно)
2. Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2024 г. №11652/24С (срок действия до 31.08.2027 г.) https://www.iprbookshop.ru/
3. Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2026 от 30.01.2026 г. (срок действия до 29.01.2027г.) https://elibrary.r

8.1.4. Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Раздел 9. Материально-техническое обеспечение образовательного процесса

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Оборудование: специализированная мебель (мебель аудиторная (столы, стулья, доска аудиторная навесная), стол преподавателя, стул преподавателя. Технические средства обучения: персональный компьютер; мультимедийное оборудование (проектор, экран).
Помещение для самостоятельной работы	Специализированная мебель (столы, стулья), персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета