



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.02 ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 7 з.е.
в академических часах: 252 ак.ч.

Москва, 2024

Разработчики:

Старший преподаватель кафедры
Информационно-измерительных систем Болгов А. О.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся способности решать задачи, связанные с применением знаний об основных аспектах организационного и правового обеспечения информационной безопасности: проблемами информационного взаимодействия и обмена информацией ограниченного доступа, допуска к защищаемой информации, правовых гарантий на получение информации, аналитической работы с правовой информацией, в информационных системах и в сети интернет.

Задачи изучения дисциплины:

- Рассмотрение правовых аспектов организации деятельности субъектов при работе с информацией ограниченного доступа.;
- Изучение практических основ организации учетной, допускной, контрольной, аналитической работы с документированной информацией..

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

Компетенции, индикаторы и результаты обучения

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-2.1 Формулирует проблему, решение которой напрямую связано с достижением цели проекта

Знать:

УК-2.1/Зн1 Основные подходы к постановке проблемы в области информационной безопасности, принципы формулирования целей и задач проектов в сфере информационной безопасности, основы проектного управления

Уметь:

УК-2.1/Ум1 Выделять ключевые проблемы в организационно-правовой сфере информационной безопасности, формулировать проблемы, решение которых необходимо для достижения целей проекта, уточнять проектные цели с учётом нормативных и правовых требований

Владеть:

УК-2.1/Нв1 Методы постановки задач в проектной деятельности в информационной безопасности, навыки критического анализа проблемных ситуаций в правовом обеспечении информационной безопасности, инструменты описания проблемной области проекта

УК-2.2 Определяет связи между поставленными задачами и ожидаемые результаты их решения

Знать:

УК-2.2/Зн1 Методики декомпозиции задач и планирования проектов, основы логической структуры проектной деятельности, показатели эффективности решений в сфере информационной безопасности

Уметь:

УК-2.2/Ум1 Устанавливать взаимосвязи между задачами в рамках правового и организационного обеспечения информационной безопасности, соотносить задачи с ожидаемыми правовыми и организационными результатами, оценивать вклад отдельных задач в достижение цели проекта

Владеть:

УК-2.2/Нв1 Приёмы логической структуризации проектной деятельности, навыки построения связей «задача–результат», методы оценки достижимости результатов в правовом контексте

УК-2.3 Анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач

Знать:

УК-2.3/Зн1 Принципы календарного и сетевого планирования проектов, методы оптимизации проектных решений, ограничения и риски в реализации проектов по информационной безопасности

Уметь:

УК-2.3/Ум1 Читать и анализировать план-графики реализации проектов, сравнивать альтернативные способы достижения задач

Владеть:

УК-2.3/Нв1 Инструменты анализа проектных планов, методы выбора оптимального сценария проектной реализации, навыки применения инструментов управления проектами (например, Gantt, PERT, диаграммы)

УК-2.4 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы

Знать:

УК-2.4/Зн1 Основы ресурсного обеспечения проектов, действующее законодательство в области информационной безопасности и смежных областях, ограничения, накладываемые нормативными актами и регуляторами

Уметь:

УК-2.4/Ум1 Идентифицировать правовые, ресурсные и организационные ограничения, оценивать доступные ресурсы (трудовые, временные, информационные), применять правовые нормы в контексте проектной деятельности

Владеть:

УК-2.4/Нв1 Методы правового анализа и правоприменения, навыки учета ресурсных и нормативных ограничений при планировании проекта, приемы оценки соответствия проекта действующему законодательству

УК-2.5 Оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач и выбирает оптимальный способ решения поставленных задач

Знать:

УК-2.5/Зн1 Подходы к контролю и оценке проектных результатов, методы оценки эффективности реализованных мероприятий, критерии качества выполнения задач в области информационной безопасности

Уметь:

УК-2.5/Ум1 Проводить оценку выполнения задач на всех этапах проекта, корректировать проектные решения в зависимости от отклонений, обосновывать необходимость изменений и выбирать альтернативные пути решения

Владеть:

УК-2.5/Нв1 Навыки мониторинга и контроля проектной деятельности, инструментами оценки соответствия результатов поставленным задачам, методами адаптивного управления в условиях правовых и организационных ограничений

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ОПК-5.1 Разрабатывает текстовую документацию в соответствии с нормативными требованиями

Знать:

ОПК-5.1/Зн1 Основные нормативные правовые акты в области обеспечения информационной безопасности

Уметь:

ОПК-5.1/Ум1 Применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности

Владеть:

ОПК-5.1/Нв1 Навыки работы с нормативными правовыми актами

ОПК-5.2 Разрабатывает методическую и организационно-распорядительную документацию в соответствии с нормативными требованиями

Знать:

ОПК-5.2/Зн1 Нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации

Уметь:

ОПК-5.2/Ум1 Составлять и оформлять положения, регламенты, инструкции и иные документы, обеспечивающие реализацию организационно-правовых мер по защите информации, применять требования нормативных правовых актов и стандартов при разработке внутренней документации по информационной безопасности

Владеть:

ОПК-5.2/Нв1 Навык организации и обеспечения режима секретности

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

ОПК-6.1 Применяет технологии, методы и средства защиты информации ограниченного доступа

Знать:

ОПК-6.1/Зн1 Классификацию информации с ограниченным доступом, основные методы и технологии защиты информации, требования законодательства РФ и регуляторов (ФСТЭК, ФСБ, Роскомнадзор) к защите информации

Уметь:

ОПК-6.1/Ум1 Выбирать и обосновывать применение конкретных методов и средств защиты информации в зависимости от категории защищаемых данных, применять организационно-технические меры защиты информации в соответствии с установленными требованиями, оценивать эффективность применяемых мер защиты и соответствие установленным нормативам.

Владеть:

ОПК-6.1/Нв1 Навыки практического применения методов защиты информации ограниченного доступа, средства документирования применённых мер защиты и обоснования их выбора, приёмы анализа защищённости информационных систем на предмет соответствия требованиям по защите информации

ОПК-6.2 Знает и применяет положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа

Знать:

ОПК-6.2/Зн1 Основные нормативные правовые акты, регулирующие защиту информации ограниченного доступа в РФ, структуру и содержание типовой нормативной документации в области защиты информации

Уметь:

ОПК-6.2/Ум1 Ориентироваться в действующем законодательстве РФ и нормативных документах по защите информации, оформлять документы в соответствии с правовыми и методическими нормами

Владеть:

ОПК-6.2/Нв1 Навыки правового анализа в области защиты информации ограниченного доступа, методы интеграции нормативных требований в организационно-распорядительные документы

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.02 «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 5, 6.

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

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
5 семестр	108	3	34	34	40	Зачет
6 семестр	144	4	36	36	36	Экзамен (36)
Всего	252	7	70	70	76	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

				а	ы	е	с
--	--	--	--	---	---	---	---

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Предыстория возникновения органов защиты информации	14	6	6	2	УК-2.1
Тема 1.1. История возникновения органов защиты информации	6	2	2	2	
Тема 1.2. Информационная безопасность в информационном обществе	4	2	2		
Тема 1.3. Современное информационное противоборство и обеспечение информационной безопасности	4	2	2		
Раздел 2. Концептуальные основы информационной безопасности	6	2	2	2	УК-2.1
Тема 2.1. Концептуальные основы информационной безопасности	6	2	2	2	
Раздел 3. Организационные основы защиты информации	14	4	4	6	УК-2.1
Тема 3.1. Основные принципы и условия организационной защиты информации	4	2	2		
Тема 3.2. Основные подходы и требования к организации системы защиты информации	4	2	2		
Тема 3.3. Основные силы и средства, используемые для организации защиты информации	6			6	
Раздел 4. Отнесение сведений к конфиденциальной информации, засекречивание, рассекречивание сведений	14	4	4	6	УК-2.1 УК-2.2 УК-2.3 ОПК-5.1 ОПК-5.2
Тема 4.1. Отнесение сведений к различным видам конфиденциальной информации	4	2	2		
Тема 4.2. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну	4	2	2		

Тема 4.3. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну	6			6	
Раздел 5. Организация допуска и доступа персонала к конфиденциальной информации	24	6	6	12	УК-2.4 УК-2.5
Тема 5.1. Основные положения допуска персонала предприятия к конфиденциальной информации	4	2	2		
Тема 5.2. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска	4	2	2		
Тема 5.3. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска	4	2	2		
Тема 5.4. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну	6			6	
Тема 5.5. Порядок доступа к конфиденциальной информации командированных лиц	6			6	
Раздел 6. Правовые гарантии поиска и получения информации, право на поиск и получение документированной информации. Особенности реализации информационных правоотношений в интернет	10	4	4	2	ОПК-5.1
Тема 6.1. Принципы правового и организационного обеспечения отношений в сфере обеспечения информационной безопасности (информации, информационных технологий и защиты информации)	6	2	2	2	
Тема 6.2. Правовое регулирование информационной безопасности в системе российского информационного права	4	2	2		
Раздел 7. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	4	2	2		УК-2.1 УК-2.2 УК-2.3

Тема 7.1. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	4	2	2		
Раздел 8. Организация внутриобъектового и пропускного режимов на предприятии	14	4	4	6	ОПК-6.2
Тема 8.1. Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии	4	2	2		
Тема 8.2. Основные цели, подходы и принципы организации внутриобъектового режима	4	2	2		
Тема 8.3. Силы и средства, используемые при организации внутриобъектового режима	6			6	
Раздел 9. Организация охраны предприятий	8	2	2	4	УК-2.1 ОПК-6.2
Тема 9.1. Организация охраны предприятий	8	2	2	4	
Раздел 10. Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности	22	8	8	6	УК-2.1 УК-2.2 УК-2.3 ОПК-6.1
Тема 10.1. Планирование мероприятий по защите информации при подготовке к проведению совещания	4	2	2		
Тема 10.2. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания	4	2	2		
Тема 10.3. Порядок проведения совещания и использования его материалов	4	2	2		
Тема 10.4. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия	4	2	2		
Тема 10.5. Организация подготовки материалов к открытому опубликованию	6			6	

Раздел 11. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу	18	6	6	6	ОПК-6.1 ОПК-6.2
Тема 11.1. Порядок передачи различных видов конфиденциальной информации иностранным государствам	4	2	2		
Тема 11.2. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам	4	2	2		
Тема 11.3. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу	4	2	2		
Тема 11.4. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам	6			6	
Раздел 12. Допуск предприятий к проведению работ с конфиденциальной информацией	12	2	2	8	УК-2.1 УК-2.2 УК-2.3 ОПК-6.1
Тема 12.1. Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну	4	2	2		
Тема 12.2. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий	4			4	
Тема 12.3. Организация проведения государственной аттестации руководителей предприятий	4			4	
Раздел 13. Организация аналитической работы и контроля состояния защиты конфиденциальной информации	4	2	2		УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5
Тема 13.1. Организация аналитической работы и контроля состояния защиты конфиденциальной информации	4	2	2		ОПК-5.1 ОПК-5.2 ОПК-6.1 ОПК-6.2

Раздел 14. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений	4	2	2		УК-2.5 ОПК-5.1 ОПК-5.2 ОПК-6.1
Тема 14.1. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений	4	2	2		
Раздел 15. Правовая защита конфиденциальной информации	18	6	6	6	УК-2.1 УК-2.2 УК-2.4 ОПК-6.1
Тема 15.1. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну	4	2	2		
Тема 15.2. Уголовно-правовая защита в сфере компьютерной информации	4	2	2		
Тема 15.3. Уголовно-правовая защита сведений, составляющих государственную тайну	4	2	2		
Тема 15.4. Административно-правовая защита информации с ограниченным доступом	4			4	
Тема 15.5. Гражданско-правовая защита служебной и коммерческой тайны	2			2	
Раздел 16. Актуальные проблемы правового и организационного обеспечения информационной безопасности	8	2	2	4	УК-2.1 УК-2.2 УК-2.4 ОПК-6.2
Тема 16.1. Противодействие экстремистской деятельности в информационной сфере	4	2	2		
Тема 16.2. Защита детей от информации, причиняющей вред их здоровью и развитию	4			4	
Раздел 17. Особенности организационноправового обеспечения защиты информационных систем	10	4	4	2	УК-2.1 УК-2.2 УК-2.3

Тема 17.1. Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении	4	2	2		
Тема 17.2. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства	4	2	2		
Тема 17.3. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем	2			2	
Раздел 18. Правовые проблемы обеспечения информационной безопасности в сети интернет	12	4	4	4	УК-2.1 УК-2.2 УК-2.3
Тема 18.1. Создание российского государственного сегмента информационно-телекоммуникационной сети Интернет	4	2	2		
Тема 18.2. Система адресации в сети Интернет	4	2	2		
Тема 18.3. Мониторинг и блокирование доступа к информации в сети Интернет	2			2	
Тема 18.4. Проблема идентификации пользователей сети Интернет	2			2	
Итого	216	70	70	76	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Предыстория возникновения органов защиты информации

Тема 1.1. История возникновения органов защиты информации

История возникновения органов защиты информации. Информационная безопасность в информационном обществе. Обеспечение информационной безопасности. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности. Методика выявления функциональной направленности режима информационной безопасности. Информационное общество и развитие института правового и организационного обеспечения информационной безопасности. Современное информационное противоборство и обеспечение информационной безопасности. Общие положения. Информационно-техническое противоборство. Идеологическое противоборство.

Тема 1.2. Информационная безопасность в информационном обществе

История возникновения органов защиты информации. Информационная безопасность в информационном обществе. Обеспечение информационной безопасности. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности. Методика выявления функциональной направленности режима информационной безопасности Информационное общество и развитие института правового и организационного обеспечения информационной безопасности. Современное информационное противоборство и обеспечение информационной безопасности. Общие положения. Информационно-техническое противоборство. Идеологическое противоборство.

Тема 1.3. Современное информационное противоборство и обеспечение информационной безопасности

История возникновения органов защиты информации. Информационная безопасность в информационном обществе. Обеспечение информационной безопасности. Правовое обеспечение информационной безопасности. Организационное обеспечение информационной безопасности. Методика выявления функциональной направленности режима информационной безопасности Информационное общество и развитие института правового и организационного обеспечения информационной безопасности. Современное информационное противоборство и обеспечение информационной безопасности. Общие положения. Информационно-техническое противоборство. Идеологическое противоборство.

Раздел 2. Концептуальные основы информационной безопасности

Тема 2.1. Концептуальные основы информационной безопасности

Концептуальные основы информационной безопасности

Раздел 3. Организационные основы защиты информации

Тема 3.1. Основные принципы и условия организационной защиты информации

Основные принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации.

Тема 3.2. Основные подходы и требования к организации системы защиты информации

Основные принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации.

Тема 3.3. Основные силы и средства, используемые для организации защиты информации

Основные принципы и условия организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Основные силы и средства, используемые для организации защиты информации.

Раздел 4. Отнесение сведений к конфиденциальной информации, засекречивание рассекречивание сведений

Тема 4.1. Отнесение сведений к различным видам конфиденциальной информации

Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне.

Тема 4.2. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну

Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне.

Тема 4.3. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну

Отнесение сведений к различным видам конфиденциальной информации. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей. Основания и порядок рассекречивания сведений и их носителей. Отнесение сведений к коммерческой тайне.

Раздел 5. Организация допуска и доступа персонала к конфиденциальной информации

Тема 5.1. Основные положения допуска персонала предприятия к конфиденциальной информации

Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну. Порядок доступа к конфиденциальной информации командированных лиц.

Тема 5.2. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска

Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну. Порядок доступа к конфиденциальной информации командированных лиц.

Тема 5.3. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска

Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну. Порядок доступа к конфиденциальной информации командированных лиц.

Тема 5.4. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну

Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну. Порядок доступа к конфиденциальной информации командированных лиц.

Тема 5.5. Порядок доступа к конфиденциальной информации командированных лиц

Основные положения допуска персонала предприятия к конфиденциальной информации. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну. Порядок доступа к конфиденциальной информации командированных лиц.

Раздел 6. Правовые гарантии поиска и получения информации, право на поиск и получение документированной информации. Особенности реализации информационных правоотношений в интернет

Тема 6.1. Принципы правового и организационного обеспечения отношений в сфере обеспечения информационной безопасности (информации, информационных технологий и защиты информации)

Принципы правового и организационного обеспечения отношений в сфере обеспечения информационной безопасности (информации, информационных технологий и защиты информации). Правовое регулирование информационной безопасности в системе российского информационного права.

Тема 6.2. Правовое регулирование информационной безопасности в системе российского информационного права

Принципы правового и организационного обеспечения отношений в сфере обеспечения информационной безопасности (информации, информационных технологий и защиты информации). Правовое регулирование информационной безопасности в системе российского информационного права.

Раздел 7. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации

Тема 7.1. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации

Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации

Раздел 8. Организация внутриобъектового и пропускного режимов на предприятии

Тема 8.1. Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии

Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима. Силы и средства, используемые при организации внутриобъектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

Тема 8.2. Основные цели, подходы и принципы организации внутриобъектового режима

Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима. Силы и средства, используемые при организации внутриобъектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

Тема 8.3. Силы и средства, используемые при организации внутриобъектового режима

Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима. Силы и средства, используемые при организации внутриобъектового режима. Цели и задачи пропускного режима. Основные элементы системы организации пропускного режима, используемые силы и средства.

Раздел 9. Организация охраны предприятий

Тема 9.1. Организация охраны предприятий

Организация охраны предприятий

Текущий контроль	
Вид (форма) контроля	
Тестирование	

Раздел 10. Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности

Тема 10.1. Планирование мероприятий по защите информации при подготовке к проведению совещания

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации. Основные правила общения со средствами массовой информации.

Тема 10.2. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации. Основные правила общения со средствами массовой информации.

Тема 10.3. Порядок проведения совещания и использования его материалов

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации. Основные правила общения со средствами массовой информации.

Тема 10.4. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации. Основные правила общения со средствами массовой информации.

Тема 10.5. Организация подготовки материалов к открытому опубликованию

Планирование мероприятий по защите информации при подготовке к проведению совещания. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания. Порядок проведения совещания и использования его материалов. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия. Организация подготовки материалов к открытому опубликованию. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации. Основные правила общения со средствами массовой информации.

Раздел 11. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу

Тема 11.1. Порядок передачи различных видов конфиденциальной информации иностранным государствам

Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

Тема 11.2. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам

Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

Тема 11.3. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу

Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

Тема 11.4. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам

Порядок передачи различных видов конфиденциальной информации иностранным государствам. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам.

Раздел 12. Допуск предприятий к проведению работ с конфиденциальной информацией

Тема 12.1. Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну

Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий. Организация проведения государственной аттестации руководителей предприятий.

Тема 12.2. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий

Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий. Организация проведения государственной аттестации руководителей предприятий.

Тема 12.3. Организация проведения государственной аттестации руководителей предприятий

Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий. Организация проведения государственной аттестации руководителей предприятий.

Раздел 13. Организация аналитической работы и контроля состояния защиты конфиденциальной информации

Тема 13.1. Организация аналитической работы и контроля состояния защиты конфиденциальной информации

Организация аналитической работы и контроля состояния защиты конфиденциальной информации

Раздел 14. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений

Тема 14.1. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений

Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.

Раздел 15. Правовая защита конфиденциальной информации

Раздел 16. Актуальные проблемы правового и организационного обеспечения информационной безопасности

Тема 16.1. Противодействие экстремистской деятельности в информационной сфере

Противодействие экстремистской деятельности в информационной сфере. Ответственность за распространение экстремистских материалов. Защита детей от информации, причиняющей вред их здоровью и развитию. Ответственность за нарушение законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

Тема 16.2. Защита детей от информации, причиняющей вред их здоровью и развитию

Противодействие экстремистской деятельности в информационной сфере. Ответственность за распространение экстремистских материалов. Защита детей от информации, причиняющей вред их здоровью и развитию. Ответственность за нарушение законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

Раздел 17. Особенности организационноправового обеспечения защиты информационных систем

Тема 17.1. Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении

Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении. Автоматизированные системы в защищенном исполнении с применением системы защиты информации в соответствии с законодательством РФ. Обеспечение информационной безопасности АС и задач пользовательских систем. Практика применения профилей стандартов информационных систем.

Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства. Особенности управления защитой информации в сфере судопроизводства. Особенности обеспечения защиты информации в сфере судопроизводства. Проблемы защиты информации в условиях интеграции ИС государственных структур, обеспечивающих судопроизводство. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем. Политика информационной безопасности государственных и коммерческих структур. Основные функции службы информационной безопасности АС. Организационно-методологические основы реализации политики информационной безопасности с применением стандартов систем менеджмента информационной безопасности.

Тема 17.2. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства

Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении. Автоматизированные системы в защищенном исполнении с применением системы защиты информации в соответствии с законодательством РФ. Обеспечение информационной безопасности АС и задач пользовательских систем. Практика применения профилей стандартов информационных систем.

Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства. Особенности управления защитой информации в сфере судопроизводства. Особенности обеспечения защиты информации в сфере судопроизводства. Проблемы защиты информации в условиях интеграции ИС государственных структур, обеспечивающих судопроизводство. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем. Политика информационной безопасности государственных и коммерческих структур. Основные функции службы информационной безопасности АС. Организационно-методологические основы реализации политики информационной безопасности с применением стандартов систем менеджмента информационной безопасности.

Тема 17.3. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем

Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении. Автоматизированные системы в защищенном исполнении с применением системы защиты информации в соответствии с законодательством РФ. Обеспечение информационной безопасности АС и задач пользовательских систем. Практика применения профилей стандартов информационных систем.

Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства. Особенности управления защитой информации в сфере судопроизводства. Особенности обеспечения защиты информации в сфере судопроизводства. Проблемы защиты информации в условиях интеграции ИС государственных структур, обеспечивающих судопроизводство. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем. Политика информационной безопасности государственных и коммерческих структур. Основные функции службы информационной безопасности АС. Организационно-методологические основы реализации политики информационной безопасности с применением стандартов систем менеджмента информационной безопасности.

Раздел 18. Правовые проблемы обеспечения информационной безопасности в сети интернет

Тема 18.1. Создание российского государственного сегмента информационно-телекоммуникационной сети Интернет

Создание российского государственного сегмента информационно-телекоммуникационной сети Интернет. Система адресации в сети Интернет. Мониторинг и блокирование доступа к информации в сети Интернет. Проблема идентификации пользователей сети Интернет. Охрана прав субъекта персональных данных. Право быть забытым. Проблема правового статуса субъектов информационных правоотношений в сети Интернет.

Тема 18.2. Система адресации в сети Интернет

Создание российского государственного сегмента информационно-телекоммуникационной сети Интернет. Система адресации в сети Интернет. Мониторинг и блокирование доступа к информации в сети Интернет. Проблема идентификации пользователей сети Интернет. Охрана прав субъекта персональных данных. Право быть забытым. Проблема правового статуса субъектов информационных правоотношений в сети Интернет.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 18.3. Мониторинг и блокирование доступа к информации в сети Интернет

Создание российского государственного сегмента информационно-телекоммуникационной сети Интернет. Система адресации в сети Интернет. Мониторинг и блокирование доступа к информации в сети Интернет. Проблема идентификации пользователей сети Интернет. Охрана прав субъекта персональных данных. Право быть забытым. Проблема правового статуса субъектов информационных правоотношений в сети Интернет.

Тема 18.4. Проблема идентификации пользователей сети Интернет

Создание российского государственного сегмента информационно-телекоммуникационной сети Интернет. Система адресации в сети Интернет. Мониторинг и блокирование доступа к информации в сети Интернет. Проблема идентификации пользователей сети Интернет. Охрана прав субъекта персональных данных. Право быть забытым. Проблема правового статуса субъектов информационных правоотношений в сети Интернет.

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет, 5 семестр.

Зачет оценивается по следующей шкале:

- оценка «зачтено» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний; а также автоматически, когда обучающийся за промежуточную аттестацию имеет оценки «отлично»;
- оценка «не зачтено» выставляется обучающемуся в случае наличия грубых ошибок при изложении ответа на основные вопросы программы, свидетельствующих о неправильном понимании предмета; при решении практических задач показано незнание способов их решения, материал изложен беспорядочно и неуверенно.

Промежуточная аттестация: Экзамен, 6 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 9. Организация охраны предприятий

Контролируемые ИДК: ОПК-6.2 УК-2.1

Тема 9.1. Организация охраны предприятий

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Определите виды информационной безопасности:
 1. Персональная, корпоративная, государственная
 2. Клиентская, серверная, сетевая
 3. Локальная, глобальная, смешанная
 4. Государственная, сетевая, глобальная
2. Как осуществляется допуск к работе с государственной тайной для организаций:
 1. Путем выдачи лицензии организации
 2. Только по желанию руководителя организации
 3. Организации не имеют права работать с государственной тайной
 4. На основании внутриведомственных приказов организации
3. Основными направлениями защиты информации являются:
 1. Правовая
 2. Организационная
 3. Инженерно-техническая
 4. Все перечисленные
4. Какое структурное подразделение осуществляет защиту информации на предприятии:
 1. Финансово-плановый отдел
 2. Отдел кадров
 3. Отдел режима и охраны
 4. Отдел международных связей
5. Степени секретности сведений, составляющих государственную тайну:
 1. Особой важности
 2. Совершенно секретно
 3. Секретно
 4. Все перечисленные

6. Отнесение сведений к государственной тайне осуществляется в соответствии с федеральным законом:

1. «О персональных данных»
2. «Об информации, информационных технологиях и защите информации»
3. «О государственной тайне»
4. Все перечисленные

7. Допуск сотрудников к государственной тайне осуществляется:

1. Отделом противодействия техническим разведкам
2. Отделом кадров организации
3. Отделом режима и охраны организации
4. Руководством организации

8. Первая форма допуска к сведениям, составляющим государственную тайну, является:

1. Допуском к сведениям особой важности
2. Допуском к секретным сведениям
3. Допуском к совершенно секретным сведениям
4. Допуском к сведениям для служебного пользования

9. Какой раздел содержит план мероприятий по защите информации при подготовке и проведении совещания:

1. Рассадка участников совещания
2. Регламент выступлений участников совещания
3. Подготовка служебного помещения к проведению совещания
4. Очередность выступлений участников совещания

10. Непосредственную ответственность за обеспечение защиты информации в ходе международного сотрудничества несут:

1. Сотрудники отдела режима и охраны
2. Сотрудники отдела международного сотрудничества
3. Руководители органов государственной власти и предприятий
4. Сотрудники отдела кадров

11. Государственная аттестация руководителей предприятий, ответственных за защиту сведений, составляющих государственную тайну, проводится в форме:

1. Тестирования
2. Экзамена
3. Опроса
4. Собеседования

12. Кто назначается в экспертную комиссию по оценке материалов, подготовленных к открытому опубликованию:

1. Сотрудники службы безопасности
2. Составители и редакторы публикуемых материалов
3. Специалисты в различных областях деятельности предприятия
4. Все перечисленные

13. Сколько, согласно Закону РФ "О государственной тайне", существует грифов секретности:

1. 4
2. 3
3. 5
4. 6

14. Кто несет основную ответственность в организации за то, что данные отнесены к соответствующей категории и защищены:

1. Сотрудники, работающие с данными
2. Руководство
3. Системные администраторы
4. Сотрудники отдела режима и охраны

15. Какая категория является наиболее рискованной для организации с точки зрения информационной безопасности:

1. Хакеры
2. Контрагенты
3. Сотрудники
4. Спецслужбы

Раздел 18. Правовые проблемы обеспечения информационной безопасности в сети интернет

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3

Тема 18.2. Система адресации в сети Интернет

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Организационно-правовая защита информации – это регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

1. Да
2. Нет

2. Целью информационной безопасности считается формирование условий, в которых будет обеспечена качественная и высокоэффективная защита конфиденциальной информации от ненамеренного или специального вмешательства, потенциально способного привести к утрате, удалению, изменению, подлогу и иным видам воздействия на информацию.

1. Да
2. Нет

3. Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая в соответствии с требованиями о защите информации.

1. Да
2. Нет

4. Технические средства защиты информации — устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

1. Да
2. Нет

5. Методы защиты информации - выборочно применяемые универсальные и специфические способы реализации элементов системы защиты информации и входящих в них содержательных частей для формирования комплексной и индивидуальной структуры данной системы.

1. Да
2. Нет

6. Общие методы защиты информации включают в себя правовые, организационно-технические и экономические.

1. Да
2. Нет

7. Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

1. Да
2. Нет

8. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

- 1. Да
- 2. Нет

9. Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

- 1. Да
- 2. Нет

10. Допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.

- 1. Да
- 2. Нет

11. Доступ к информации, составляющей коммерческую тайну - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

- 1. Да
- 2. Нет

12. Режим секретности – совокупность требований, правил, административно-правовых, организационных, инженерно-технических мер, направленных на сохранение сведений, составляющих государственную тайну.

- 1. Да
- 2. Нет

13. Анализ состояния защиты информации — это комплексное изучение фактов, событий, процессов, явлений, связанных с проблемами защиты информации, в том числе данных о состоянии работы по выявлению возможных каналов утечки информации, о причинах и обстоятельствах, способствующих утечке и нарушениям режима секретности (конфиденциальности) в ходе повседневной деятельности предприятия.

- 1. Да
- 2. Нет

14. Под разглашением сведений, составляющих государственную тайну, следует понимать противоправное предание огласке этих сведений (сообщение в доверительной беседе, демонстрирование схем и т.п., доклад, лекция, публикация в средствах массовой информации и т.д.), в результате чего они стали достоянием других лиц.

- 1. Да
- 2. Нет

15. Автоматизированная система в защищенном исполнении (АСЗИ) - автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации.

- 1. Да
- 2. Нет

8. Оценочные материалы промежуточной аттестации

5 семестр, Зачет

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-5.1 ОПК-6.1 ОПК-5.2 ОПК-6.2

Вопросы/Задания:

1. История возникновения органов защиты информации
2. Информационная безопасность в информационном обществе
3. Обеспечение информационной безопасности в информационном обществе
4. Правовое обеспечение информационной безопасности
5. Организационное обеспечение информационной безопасности
6. Методика выявления функциональной направленности режима информационной безопасности
7. Информационное общество и развитие института правового и организационного обеспечения информационной безопасности
8. Современное информационное противоборство и обеспечение информационной безопасности
9. Информационно-техническое противоборство
10. Идеологическое противоборство
11. Концептуальные основы информационной безопасности
12. Основные принципы и условия организационной защиты информации
13. Основные подходы и требования к организации системы защиты информации
14. Основные силы и средства, используемые для организации защиты информации
15. Отнесение сведений к различным видам конфиденциальной информации
16. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну
17. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну
18. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей
19. Основания и порядок рассекречивания сведений и их носителей
20. Отнесение сведений к коммерческой тайне
21. Основные положения допуска персонала предприятия к конфиденциальной информации

22. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска

23. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска

24. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну

25. Порядок доступа к конфиденциальной информации командированных лиц

26. Принципы правового и организационного обеспечения отношений в сфере обеспечения информационной безопасности (информации, информационных технологий и защиты информации)

27. Правовое регулирование информационной безопасности в системе российского информационного права

28. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации

29. Роль и место внутриобъектового и пропускного режимов в общей системе защиты информации на предприятии

30. Основные цели, подходы и принципы организации внутриобъектового режима

31. Силы и средства, используемые при организации внутриобъектового режима

32. Цели и задачи пропускного режима

33. Основные элементы системы организации пропускного режима, используемые силы и средства

34. Организация охраны предприятий

35. Планирование мероприятий по защите информации при подготовке к проведению совещания

36. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка места проведения совещания

37. Порядок проведения совещания и использования его материалов

38. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия

39. Организация подготовки материалов к открытому опубликованию

40. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации

41. Основные правила общения со средствами массовой информации
42. Порядок передачи различных видов конфиденциальной информации иностранным государствам
43. Организация подготовки к передаче сведений, составляющих государственную тайну, другим государствам
44. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу
45. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам
46. Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну

6 семестр, Экзамен

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-5.1 ОПК-6.1 ОПК-5.2 ОПК-6.2

Вопросы/Задания:

1. Правовое обеспечение информационной безопасности
2. Организация охраны предприятия
3. Организационное обеспечение информационной безопасности
4. Цели и задачи организации пропускного режима на предприятии
5. Информационно-техническое противоборство
6. Планирование мероприятий по защите информации при проведении совещаний
7. Основные принципы и условия организационной защиты информации
8. Организация допуска участников совещания к обсуждаемым вопросам. Подготовка помещений
9. Основные подходы и требования к организации системы защиты информации
10. Порядок проведения совещаний и использование его материалов
11. Основные силы и средства, используемые для организации защиты информации
12. Основы организации защиты информации в ходе издательской и рекламной деятельности предприятия
13. Отнесение сведений к различным видам конфиденциальной информации

14. Организация подготовки материалов к открытому опубликованию
15. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну
16. Основы организации защиты информации в ходе взаимодействия со СМИ
17. Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей
18. Порядок передачи различных видов конфиденциальной информации представителям иностранных государств
19. Отнесение сведений к коммерческой тайне
20. Организация передачи сведений, составляющих гостайну, представителям иностранных государств
21. Основание и порядок рассекречивания сведений и их носителей
22. Ограничение прав гражданина, осведомленного в сведениях, относящихся к гостайне
23. Основные положения допуска персонала предприятия к конфиденциальной информации
24. Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих гостайну
25. Порядок оформления и переоформления допуска к гостайне. Формы допуска
26. Алгоритм работы лицензирующего органа по лицензированию предприятий
27. Основания для отказа должностному лицу или гражданину в допуске к гостайне и условия прекращения допуска
28. Организация проведения государственной аттестации руководителей предприятия
29. Организация доступа сотрудников к сведениям, составляющим гостайну
30. Организация аналитической работы и контроля состояния защиты конфиденциальной информации
31. Порядок доступа к конфиденциальной информации командированных лиц
32. Уголовно-правовая защита сведений, составляющих конфиденциальную информацию
33. Правовое регулирование информационной безопасности в системе российского законодательства

34. Организация и проведение служебного расследования в случае разглашения конфиденциальной информации или утраты ее носителя
35. Основные направления работы с персоналом, допущенным к конфиденциальной информации
36. Уголовно-правовая защита сведений, составляющих государственную тайну
37. Роль и место внутриобъектового режима в системе защиты информации на предприятии
38. Дисциплинарная ответственность за разглашение или утрату конфиденциальных сведений
39. Основные цели и принципы организации внутриобъектового режима
40. Ответственность за распространение материалов экстремистского характера
41. Силы и средства, используемые для организации внутриобъектового режима
42. Обеспечение защиты информации в автоматизированных системах

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Газизов А. Р. Организационное и правовое обеспечение информационной безопасности: учебное пособие: учебное пособие / А. Р. Газизов; под редакцией А. Р. Айдиняна. - Организационное и правовое обеспечение информационной безопасности - Ростов-на-Дону: Донской государственный технический университет, 2017. - 156 с. - 978-5-7890-1384-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/117813.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Дронов В. Ю. Международные и отечественные стандарты по информационной безопасности: учебно-методическое пособие: учебно-методическое пособие / В. Ю. Дронов. - Международные и отечественные стандарты по информационной безопасности - Новосибирск: Новосибирский государственный технический университет, 2016. - 34 с. - 978-5-7782-3112-2. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/91395.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Арзуманян А. Б. Международные стандарты правовой защиты информации и информационных технологий: учебное пособие: учебное пособие / А. Б. Арзуманян. - Международные стандарты правовой защиты информации и информационных технологий - Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2020. - 140 с. - 978-5-9275-3546-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/107955.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

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

Профессиональные базы данных

1. <https://student2.consultant.ru/cgi/online.cgi> - Правовой Сервер КонсультантПлюс

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://www.elibrary.ru/> - НЭБ eLIBRARY
3. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)

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

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

- Маркерная доска - 0 шт.
- Моноблок - 64 шт.
- Проектор - 4 шт.

Лекционная аудитория

- Лекционный мультимедийный комплекс - 4 шт.
- Проектор - 4 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется:

- Методическими рекомендациями по дисциплине;
- Методическими рекомендациями по организации самостоятельной работы студентов МИИГАиК;

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.