



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)
«Б1.В.02 СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ ЗАРУБЕЖНЫХ
СТРАНАХ»**

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: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Доцент кафедры Информационно-измерительных систем, к.н.,
доцент Еремеева В. И.

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 - получение обучающимися теоретических и практических знаний о закономерностях становления, тенденциях развития и совершенствования систем защиты информации в ведущих зарубежных странах, особенностях их современной организации и функционирования, перспективах развития с целью формирования способности критически переосмысливать накопленный зарубежный опыт для его дальнейшего применения при построении систем защиты информации в России.

Задачи изучения дисциплины:

- формирование понятий о составе и классификации защищаемой информации, структуре угроз защищаемой информации, каналах несанкционированного доступа к защищаемой информации и методах ее добывания, направлениях и методах защиты информации в зарубежных странах, особенностях государственной политики в области защиты информации; процессах развития и совершенствования организационно-правовых основ защиты информации; составе органов защиты информации в ведущих зарубежных странах; особенностях и направлениях международного сотрудничества в области защиты информации;;
- формирование навыков анализа зарубежного законодательства в области защиты информации;;
- формирование умений применять полученные знания в научно-исследовательской и практической деятельности, решения проблем, связанных с организацией систем защиты информации, с учетом зарубежного опыта; построения систем защиты информации в России с учетом опыта зарубежных стран..

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

Компетенции, индикаторы и результаты обучения

ПК-2 Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах

ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах

Знать:

ПК-2.1/Зн2 Основные особенности организации и функционирования процессов защиты информации в ведущих зарубежных странах

Уметь:

ПК-2.1/Ум2 Применять современные информационные технологии в целях совершенствования системы защиты информации с учетом зарубежного опыта

Владеть:

ПК-2.1/Нв2 Навыками сбора и обработки информации, имеющей значения для реализации правовых норм в соответствующих сферах профессиональной деятельности с учетом зарубежного опыта

ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности

Знать:

ПК-2.2/Зн2 Основы государственной политики в области защиты информации в ведущих зарубежных странах

Уметь:

ПК-2.2/Ум2 применять полученные знания в научно-исследовательской и практической работе

ПК-2.2/Ум3 совершенствовать процессы защиты информации с учетом зарубежного опыта

Владеть:

ПК-2.2/Нв2 практического осуществления основных работ, связанных с организацией и технологией защиты информации с учетом зарубежного опыта

ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации

Знать:

ПК-2.3/Зн2 состав, особенности классификации, структуру угроз защищаемой информации в ведущих зарубежных странах

ПК-2.3/Зн3 состав, структуру и основные направления деятельности органов защиты информации в ведущих зарубежных странах

Уметь:

ПК-2.3/Ум2 анализировать зарубежное законодательство в области защиты информации

ПК-2.3/Ум3 обобщать международный опыт организации и совершенствования систем защиты информации

Владеть:

ПК-2.3/Нв2 обосновывать возможности использования зарубежного опыта при разработке комплексной системы защиты информации

ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах

Знать:

ПК-2.4/Зн2 особенности нормативной базы защиты информации в ведущих зарубежных странах

Уметь:

ПК-2.4/Ум2 формулировать научные проблемы, возникающие при построении систем защиты информации и предлагать методы их решения с использованием зарубежного опыта защиты информации

ПК-2.4/Ум3 анализировать основные тенденции и перспективы применения зарубежного опыта защиты информации в российских условиях

Владеть:

ПК-2.4/Нв1 навыками планирования и проведения аудита и мониторинга информационной безопасности в автоматизированных системах

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.02 «Системы защиты информации в ведущих зарубежных странах» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 2.

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)
2 семестр	108	3	34	34	13	Экзамен (27)
Всего	108	3	34	34	13	27

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий (часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты с обучения, соответствующие результатам освоения программы
Раздел 1. Введение	5	2	2	1	ПК-2.1
Тема 1.1. Входной контроль. Введение.	5	2	2	1	
Раздел 2. Становление и развитие систем защиты информации в ведущих зарубежных странах	10	4	4	2	ПК-2.2
Тема 2.1. Становление и развитие систем защиты информации в ведущих зарубежных странах	10	4	4	2	
Раздел 3. Организация защиты информации в США	14	6	6	2	ПК-2.3
Тема 3.1. Организация защиты информации в США	14	6	6	2	
Раздел 4. Организация защиты информации в Германии	14	6	6	2	ПК-2.3
Тема 4.1. Организация защиты информации в Германии	14	6	6	2	
Раздел 5. Организация защиты информации в Великобритании	10	4	4	2	ПК-2.3
Тема 5.1. Организация защиты информации в Великобритании	10	4	4	2	

Раздел 6. Организация защиты информации во Франции	10	4	4	2	ПК-2.3
Тема 6.1. Организация защиты информации во Франции	10	4	4	2	
Раздел 7. Организация защиты информации в Японии	10	4	4	2	ПК-2.3
Тема 7.1. Организация защиты информации в Японии	10	4	4	2	
Раздел 8. Международное сотрудничество в области защиты информации	8	4	4		ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4
Тема 8.1. Международное сотрудничество в области защиты информации	8	4	4		
Итого	81	34	34	13	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Введение

Тема 1.1. Входной контроль. Введение.

Предмет, содержание и задачи курса, методы его изучения.

Терминология. Особенности формирования терминологии защиты информации в зарубежных странах.

Методы исследования зарубежного опыта защиты информации.

Назначение курса и его место в подготовке специалистов по защите информации.

Связь курса с другими дисциплинами учебного плана.

Общий анализ источников и литературы по курсу.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Становление и развитие систем защиты информации в ведущих зарубежных странах

Тема 2.1. Становление и развитие систем защиты информации в ведущих зарубежных странах

Становление систем, формирование основных понятий, выработка принципов, методов, основных подходов и направлений защиты информации.

Особенности опыта организации защиты информации на Древнем Востоке. Истоки разделения и классификации видов тайн. Основные методы защиты государственной тайны. Опыт создания служб безопасности. Организация проверок, методика работы с персоналом, классификация личностных характеристик, необходимых для сотрудника, владеющего сведениями, составляющими тайну.

Становление основных направлений, принципов и методов защиты информации в средневековой Европе.

Основные направления совершенствования защиты информации в Новое время. Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии). Опыт криптографической защиты информации в странах Западной Европы. Методы защиты коммерческих сведений. Банковская тайна и особенности ее защиты.

Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы, США и Японии в XVIII- начале XX вв.

Формирование правовых и организационных основ защиты информации.

Разведка и контрразведка как необходимые элементы политики обеспечения безопасности государств и как факторы взаимного развития и совершенствования.

Промышленный шпионаж: его значение для формирования систем защиты информации. Особенности государственной политики по отношению к промышленному шпионажу в национальных и межгосударственных рамках.

Формирование авторского и патентного права.

Защита информации, содержащейся в торговых книгах, в XIX- начале XX вв. (на примере Германии, Франции, Италии, Голландии, Австрии, Венгрии).

Особенности формирования современных систем защиты информации в ведущих зарубежных странах в XX- начале XXI вв.

Влияние исторического опыта защиты информации на последующее формирование и развитие современных основ защиты информации в зарубежных странах.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 3. Организация защиты информации в США

Тема 3.1. Организация защиты информации в США

Особенности государственного устройства США.

Государственная политика в области защиты информации. Организация и ограничение доступа к документам государственных органов.

Организация защиты информации по национальной безопасности.

Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности. Структура разведывательного сообщества США и его роль в осуществлении политики защиты информации по национальной безопасности. Защита секретной информации, используемой в международных программах. Защита информации в ходе деловых визитов и встреч.

Классификация защищаемой информации. Состав грифов ограничения доступа к документам. Право первоначальной классификации информации. Состав информации, не подлежащей классификации по степени секретности. Порядок изменения степени секретности.

Допуск и доступ к защищаемой информации по вопросам национальной безопасности. Организация доступа к информации ограниченного доступа. Доступ к правительственной информации. Обязанности руководителей ведомств, разрешающих доступ лиц к секретным документам. Обязанности лиц, имеющих право на доступ к защищаемой информации. Особенности организации доступа к научно-технической информации.

Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации.

Правовые основы защиты информации. Законодательные основы обеспечения информационной безопасности. Ответственность за разглашение секретных сведений.

Организация защиты коммерческой тайны. Функции по защите коммерческой тайны частных охранных агентств и служб промышленной и коммерческой безопасности. Осуществление контроля за их деятельностью. Ассоциации частных охранных агентств и служб промышленной и коммерческой безопасности, основные функции в области защиты информации.

Классификация информации, составляющей коммерческую тайну.

Доступ к информации, принадлежащей частным лицам.

Разработка программы защиты информации. Обязательный минимум защитных мер обеспечения деятельности фирмы.

Защита коммерческой тайны в процессе организации работы с клиентами (продавцы, покупатели, торговые агенты и другие).

Организация контроля надежности функционирования системы защиты коммерческой тайны фирмы.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 4. Организация защиты информации в Германии

Тема 4.1. Организация защиты информации в Германии

Особенности государственного устройства Германии. Государственная политика в области защиты информации. Организация и ограничение доступа к документам государственных органов.

Основные этапы становления и особенности современной системы органов защиты информации. Организация системы органов защиты информации. Основные принципы организации их деятельности. Функции разведывательных, контр-разведывательных и полицейских органов в области защиты информации. Парламентско-правительственный контроль за деятельностью органов защиты информации.

Состав, структура и основные направления деятельности служб безопасности Германии. Основные категории служб безопасности. Агентства, предоставляющие частным фирмам, банкам и государственным учреждениям услуги по обеспечению безопасности зданий, объектов и лиц, подлежащих охране. Частные промышленные и коммерческие службы безопасности. Подразделения внутренней охраны, создаваемые частными предприятиями, фирмами, финансово-кредитными организациями. Общественные организации по борьбе с экономическим шпионажем и преступностью. Особенности решения вопросов обеспечения безопасности и защиты информации в совместных фирмах. Роль специальных служб в подборе, проверке персонала и контроле коммерческой деятельности совместных фирм. Добывание информации, контроль иностранных граждан на территории Германии. Взаимодействие системы специальных служб и правоохранительных органов с частными промышленными и коммерческими службами безопасности. Основные функции служб безопасности. Основные направления совершенствования работы служб безопасности.

Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Функциональные обязанности работников подразделений защиты информации. Требования к персоналу в совместных фирмах.

Организация защиты информации.

Особенности защиты информации в банковской сфере.

Правовые основы защиты информации. Государственная тайна и доступ к правительственной, парламентской и судебной информации. Порядок проведения проверки лиц, которым предоставляется допуск к государственной тайне. Классификация защищаемой информации. Состав грифов ограничения доступа к документам.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 5. Организация защиты информации в Великобритании

Тема 5.1. Организация защиты информации в Великобритании

Особенности государственного устройства Великобритании. Государственная политика в области защиты информации. Организация и ограничение доступа к документам государственных органов.

Организация системы органов защиты информации Великобритании. Организация и координация их деятельности. Основные функции специальных служб Великобритании в области защиты информации.

Состав, структура и основные направления деятельности служб безопасности Великобритании. Основные категории служб безопасности. Службы по борьбе с коммерческими преступлениями, создаваемые на государственном уровне. Функции специальных подразделений министерства торговли и промышленности по предупреждению коммерческих преступлений. Службы безопасности предприятий и фирм. Частные фирмы и консультанты, занимающиеся вопросами безопасности и защиты коммерческой тайны. Основные функции служб безопасности. Основные направления совершенствования работы служб безопасности.

Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Функциональные обязанности работников подразделений защиты информации.

Организация защиты информации. Содержание программы обеспечения безопасности предприятия. Особенности защиты информации и предупреждение компьютерных преступлений в банковской сфере.

Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации. Классификация защищаемой информации. Состав грифов ограничения доступа к документам.

Правовая защита тайны корреспонденции. Коммерческая тайна и доступ к информации, принадлежащей частным лицам. Ответственность за компьютерные преступления.

Особенности защиты служебной тайны. Особенности защиты персональных данных.

Профессиональная тайна. Вопросы конфиденциальности в деятельности СМИ.

Профессиональная тайна журналистов.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 6. Организация защиты информации во Франции

Тема 6.1. Организация защиты информации во Франции

Особенности государственного устройства Франции. Государственная политика в области защиты информации. Организация и ограничение доступа к документам государственных органов.

Органы защиты информации и основные направления их деятельности. Организация и координация их деятельности. Основные функции специальных служб Франции в области защиты информации.

Состав, структура и основные направления деятельности служб безопасности Франции. Основные категории служб безопасности. Службы безопасности в промышленно-торговых фирмах и финансовых учреждениях. Службы безопасности в фирмах, выполняющих государственные заказы в сфере оборонной промышленности, космических и ядерных исследований, новых видов вооружений, средств связи и транспорта. Частные службы безопасности и частные охран-но-сыскные бюро, основная сфера их деятельности. Профессиональные объединения частных служб промышленной и коммерческой безопасности и частных охранных бюро, цели их создания. Основные функции служб безопасности. Методы и основные направления совершенствования работы служб безопасности.

Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Функциональные обязанности работников подразделений защиты информации.

Организация защиты информации. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов. Правовая защита служебной, профессиональной тайны, тайны корреспонденции. Особенности защиты информации в банковской сфере. Коммерческая тайна и организация доступа к информации, принадлежащей частным предприятиям. Ответственность за компьютерные преступления. Ответственность за нарушение требований к организации деятельности частных служб безопасности.

Особенности защиты персональных данных. Вопросы конфиденциальности в деятельности СМИ. Профессиональная тайна журналистов.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 7. Организация защиты информации в Японии

Тема 7.1. Организация защиты информации в Японии

Особенности государственного устройства Японии. Государственная политика в области защиты информации. Особенности формирования системы защиты информации в Японии. Организация и ограничение доступа к документам государственных органов. Органы защиты информации и основные направления их деятельности. Организация и координация их деятельности. Функции в области защиты информации управления обороны, управления национальной безопасности, главного полицейского управления, министерств юстиции, иностранных дел, внешней торговли и промышленности. Состав, структура и основные направления деятельности служб безопасности Японии. Основные категории служб безопасности. Частные сыскные бюро и их функции в сфере защиты информации. Частные фирмы охраны и безопасности и их функции в сфере защиты информации. Ассоциации служб охраны и безопасности. Общественные организации, оказывающие помощь органам полиции в сфере защиты экономической информации (территориальные советы по предупреждению преступности, общества содействия полиции, пункты связи по предупреждению преступности). Службы безопасности отдельных организаций. Подразделения внутреннего самоконтроля отдельных организаций и их функции в сфере защиты информации. Основные функции служб безопасности. Методы и основные направления совершенствования работы служб безопасности. Требования к персоналу. Особенности подбора, проверки, профессиональной подготовки, текущей работы с персоналом, допущенным к защищаемой информации. Функциональные обязанности работников подразделений защиты информации. Организация защиты информации. Принцип корпоративной защиты и обеспечения безопасности объекта. Защита информации в процессе взаимодействия фирм с иностранными партнерами. Классификация защищаемой информации. Правовые основы защиты информации. Особенности защиты государственной тайны. Классификация защищаемой информации. Ответственность за компьютерные преступления. Особенности защиты служебной тайны. Особенности защиты коммерческой тайны. Особенности защиты персональных данных. Профессиональная тайна. Вопросы конфиденциальности в деятельности СМИ. Профессиональная тайна журналистов.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 8. Международное сотрудничество в области защиты информации

Тема 8.1. Международное сотрудничество в области защиты информации

Международная защита интеллектуальной собственности. Международный опыт стандартизации в области защиты информации. Особенности организации защиты информации в Европейском Союзе. Безопасность информационного пространства в ЕС и особенности защиты информации. Особенности защиты коммерческой тайны. Особенности защиты банковской тайны. Особенности защиты служебной и профессиональной тайны. Особенности защиты персональных данных.

Текущий контроль

Вид (форма) контроля
Тестирование

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: Экзамен, 2 семестр.

При проведении оценивания по вопросам и заданиям, указанным в билете, в ходе промежуточной аттестации, преподаватель может учитывать результаты текущего контроля.

Устанавливаются следующие шкалы оценивания уровней освоения компетенций, предусмотренных рабочей программой при проведении экзамена:

«ПОВЫШЕННЫЙ» - выставляется оценка - 5 «ОТЛИЧНО», если среднее арифметическое значение оценок по элементам контроля находится в интервале от 4.5-5.0;

«БАЗОВЫЙ» - выставляется оценка - 4 «ХОРОШО», если среднее арифметическое значение оценок по элементам контроля находится в интервале от 3.5 - 4.4;

«Пороговый» - выставляется оценка - 3 «УДОВЛЕТВОРИТЕЛЬНО», если среднее арифметическое значение оценок по элементам контроля находится в интервале от 2.5 - 3.4.

«НЕДОСТАТОЧНЫЙ» - выставляется оценка - 2 «НЕУДОВЛЕТВОРИТЕЛЬНО», если среднее арифметическое значение оценок по элементам контроля менее 2.5.

7. Оценочные материалы текущего контроля

Раздел 1. Введение

Контролируемые ИДК: ПК-2.1

Тема 1.1. Входной контроль. Введение.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В Великобритании применяются следующие грифы секретности:

1. Ограниченный доступ
2. Совершенно секретно
3. Особой важности

2. В Уголовном кодексе Японии определяются меры ответственности за разглашение:

1. Государственной тайны
2. Профессиональной тайны
3. Коммерческой тайны

3. В Германии приняты следующие законы:

1. О государственной тайне
2. О коммерческой тайне
3. О предупреждении недобросовестной конкуренции

4. Главным разведывательным органом Франции является:

1. Главное управление внешней безопасности
2. Служба внешней документации и контрразведки
3. Служба общей разведки

5. Дополнения, касающиеся компьютерных преступлений и защиты информации в процессе автоматизированной обработки данных, внесены в Уголовный кодекс Японии в:

1. 1986 г.
2. 1991 г.
3. 1965 г.

6. В Великобритании закон «Об измене» был принят в:

1. 1351 г.
2. 1967 г.
3. 1909 г.

7. Является ли верным следующее утверждение:

Промышленный образец охраняется средствами авторского права в ФРГ.

8. В Германии осуществляется ведомственный контроль за деятельностью основных спецслужб, исключение составляет:

9. «Сертификаты персональной информации» («сертификаты приватности») для коммерческих организаций выдаются:

10. В ФРГ впервые была предпринята попытка установить парламентский контроль за деятельностью органов защиты информации:

11. Следующее определение понятия «ноу-хау»:

«Это техническая информация (реже коммерческая или финансовая) секретного или несекретного характера, предназначенная исключительно для промышленных и коммерческих целей и имеющая в отношении правовой охраны меньшее значение, чем изобретение или секретный процесс» применяется:

Раздел 2. Становление и развитие систем защиты информации в ведущих зарубежных странах

Контролируемые ИДК: ПК-2.2

Тема 2.1. Становление и развитие систем защиты информации в ведущих зарубежных странах

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Ответственность юридических лиц за нарушение порядка обработки персональных данных в Японии устанавливается в соответствии с:

2. В какой стране в соответствии с законом «О государственной службе» требования по сохранению служебной тайны включены в раздел «Дисциплина»

3. Является ли верным утверждение о том, что основу правового регулирования отношений, связанных с использованием коммерческой тайны, в Великобритании составляют: прецедентное право и ряд специальных законов?

4. Правительственная криптографическая школа создана в Англии:

5. Авторское право на произведения юридического лица действует в Японии в течение:

6. Служащим государственных учреждений во Франции запрещается принимать участие в форме работы, консультаций и капиталов в частном предприятии, за которым осуществляет контроль данное государственное учреждение:

7. § 203 (нарушение тайны частной жизни) Уголовного кодекса Германии применяется:

1. В случаях разглашения коммерческой, служебной и профессиональной тайны
2. В случаях разглашения профессиональной тайны
3. В случаях разглашения служебной тайны

8. Нарушение договорных обязательств о воздержании от конкуренции во Франции относится к актам:

1. Недобросовестной конкуренции
2. Запрещенной конкуренции
3. Паразитической конкуренции

9. К США относится следующее утверждение:

1. Должности, связанные с необходимостью сохранения служебной тайны, исключаются из конкурсной службы
2. В соответствии с законом «О государственной службе» требования по сохранению служебной тайны включены в раздел «Дисциплина»
3. Все перечисленное

10. Контроль за соблюдением положений закона о защите персональных данных во Франции осуществляет:

1. Комиссия по доступу к административным документам
2. Национальная комиссия по информатике и свободам
3. Центральная служба безопасности информационных систем

11. Закон о предупреждении недобросовестной конкуренции принят в:

1. Германии
2. Англии
3. Франции

12. Ответственность физических лиц за нарушение порядка обработки персональных данных в Японии устанавливается в соответствии с:

1. Уголовным кодексом
2. Гражданским кодексом
3. Законом «О персональной информации»

Раздел 3. Организация защиты информации в США

Контролируемые ИДК: ПК-2.3

Тема 3.1. Организация защиты информации в США

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Федеральный уполномоченный по защите данных осуществляет в ФРГ:

1. Межведомственный контроль
2. Правительственный контроль
3. Парламентско-правительственный контроль

2. В Великобритании:

1. Принято специальное законодательство о пресечении недобросовестной конкуренции (НДК)
2. В судебной практике нет общего понятия НДК. НДК рассматривается как часть понятия «нарушение интересов бизнеса»
3. Все перечисленное

3. В Германии юридические лица, представляющие негосударственные организации, которые заняты автоматизированной обработкой персональных данных, назначают уполномоченного по защите данных, если:

1. В организации не менее 5 постоянных сотрудников
2. В организации не менее 20 постоянных сотрудников
3. Вопрос решается администрацией предприятия

4. Первый в истории Японии закон об авторском праве 1722 г. регулировал вопросы охраны:

1. Прав автора
2. Прав издателя произведения
3. Все перечисленное

5. В Великобритании охрана ноу-хау и торговых секретов:

1. Регулируется в рамках уголовного права
2. Строится на базе прецедентного права
3. Все перечисленное

6. Нормы по защите персональных данных во Франции включены в закон:

- 1..Закон «Об информатике, картотеках и свободах»
- 2..Закон «О правах граждан в их отношениях с администрацией»
3. Закон «Об административной процедуре»

7. Следующее утверждение:

«Для предоставления доступа к защищаемой информации требуется выполнение следующих условий:

1. Проведение специальной проверки служащего.
2. Составление специального соглашения о неразглашении информации.
3. «Очевидная необходимость в знании».
4. Письменное разрешение служащего ведомству-нанимателю о проведении через специальное агентство проверки в период работы служащего, а также в течение 3-х лет после прекращения службы следующих материалов служащего:
 - 1) финансовые записи, которые ведутся финансовыми органами;
 - 2) отчеты потребителя, принадлежащие служащему;
 - 3) записи, которые ведутся любыми коммерческими структурами, относящиеся к поездкам служащего за пределы страны» относится к:

8. Следующее утверждение:

«Тайну национальной обороны» составляют:

Важные для национальной обороны сведения, технологии, методы, предметы, документы, информационные данные, содержащиеся в памяти ЭВМ, данные картотек, ставшие объектом специальных защитных мер, предусмотренных декретом Государственного Совета, направленных на исключение их распространения или предоставления недозволенным лицам» относится к:

9. Является ли верным утверждение о том, что § 202 а) Уголовного кодекса Германии (действия, направленные на получение данных) применяется: при рассмотрении всех случаев «компьютерных» преступлений, в т.ч. «компьютерного» шпионажа, неправомерного изъятия данных, если эта информация является конфиденциальной.

10. Управление стратегических служб – первый в истории США национальный орган разведки, объединивший военную и политическую разведки создан:

11. Центральное разведывательное управление, Совет национальной безопасности, Министерство обороны (объединены 2 министерства: Военное и Военно-морское) были созданы в США в соответствии с законом «О национальной безопасности», который принят 26 июля:

Раздел 4. Организация защиты информации в Германии

Контролируемые ИДК: ПК-2.3

Тема 4.1. Организация защиты информации в Германии

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Агентство национальной безопасности США, которое организует и осуществляет сбор информации с помощью радиоэлектронной разведки, а также разработку кодов и шифров и защиту правительственной информации было создано в:

2. В какой стране в конце 18 в. была создана Ассоциация борьбы с патентами и монополиями – организация, поощрявшая промышленный шпионаж?

3. В какой стране в 1810 г. был издан Уголовный кодекс, в котором фабричный секрет определялся как секрет, который может быть предметом патента и любая особенность производства.

4. Является ли верным утверждение о том, что законы США О свободном доступе к информации (1966 г., с поправками 1986 г.) и Об охране прав личности (1974 г.), ограничивая доступ к информации государственных органов, устанавливают: исключения; особые исключения и конкретные исключения

5. Первый в истории США закон об информационной безопасности принят в:
6. В какой стране Своды уголовных и гражданских законов (702-718 гг.) устанавливали следующую классификацию секретных сведений: государственная тайна; негосударственная тайна; сведения, косвенно касающиеся государственных дел, распространение которых может нанести вред государству
7. В Германии юридические лица, представляющие негосударственные организации, которые заняты обработкой персональных данных традиционным способом (ручная обработка), назначают уполномоченного по защите данных, если:
1. В организации не менее 5 постоянных сотрудников
 2. В организации не менее 20 постоянных сотрудников
 3. Вопрос решается администрацией предприятия
8. В Великобритании впервые термин «конфиденциальная информация» был применен в судебном прецеденте в:
1. 1948 г.
 2. 1916 г.
 3. 1861 г.
9. В Великобритании в соответствии с законом «О государственных документах» запрещается ознакомление общественности с протоколами Кабинета в течение:
1. 30 лет
 2. 50 лет
 3. 100 лет
10. Специальная проверка персонала, допускаемого к секретным сведениям, в США осуществляется:
1. Органами ФБР
 2. Агентством национальной безопасности
 3. Следственным управлением общественной безопасности
11. В рамках ЕС законодательное регулирование вопросов, связанных с защитой коммерческой тайны, осуществляется на основе:
1. Общих принципов законодательства ЕС в отношении установления благоприятных рыночных условий и справедливой конкурентной практики
 2. Национальных законов каждой страны
 3. Директивы Европейского Парламента и Европейского Союза «О защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения и раскрытия»

Раздел 5. Организация защиты информации в Великобритании

Контролируемые ИДК: ПК-2.3

Тема 5.1. Организация защиты информации в Великобритании

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Первый в истории законодательный акт «О свободе личности» (1679 г.), устанавливающий права и обязанности государства и других субъектов в области защиты прав человека, был принят в:
1. Японии
 2. Франции
 3. Англии
2. Во Франции осуществление профессиональной деятельности без соответствующих дипломов (врача, адвоката и др.) относится к актам:
1. Недобросовестной конкуренции
 2. Запрещенной конкуренции
 3. Паразитической конкуренции

3. Защита персональных данных в ЕС осуществляется в соответствии с:

1. Директивой Европейского парламента и Совета Европейского Союза 95/46/ ЕС
2. Регламентом Европейского парламента и Совета Европейского Союза №2016/679
3. Все перечисленное

4. В Великобритании суд не вправе требовать от журналистов раскрыть профессиональную тайну журналиста, источник опубликованной информации в соответствии с законом:

1. Об ответственности за неуважение к суду
2. О свободе информации
3. О защите данных

5. В ФРГ комитет доверенных лиц, созданный в 1956 г., являлся:

1. Парламентской комиссией по контролю за деятельностью спецслужб
2. Органом контроля за защитой персональных данных
3. Совещательным органом СМИ, созданным в целях недопущения появления в прессе защищаемой информации в области национальной обороны

6. § 201 УК ФРГ «Нарушение конфиденциальности слова» преследует цель уголовно-правовой защиты:

1. Устной конфиденциальной информации
2. Письменной и устной конфиденциальной информации
3. Профессиональной тайны

7. Федеральным координирующим центром в области обеспечения информационной безопасности в США является:

8. В какой стране на федеральном уровне доступ к документам государственных органов осуществляется в соответствии со ст. 5 Конституции, устанавливает информационную свободу, право на доступ к документам государственных органов?

9. В какой стране в 1754 г. группа промышленников и банкиров учредила Общество поощрения ремесел и торговли, предлагавшее премии изобретателям, которые отказывались брать патенты или хранить свои изобретения в тайне и предоставляли свои изобретения в распоряжение всех?

10. Является ли верным утверждение:

«В соответствии с Уголовным кодексом Китая (Танский уголовный кодекс, 618-907 гг.) секретные сведения разделялись по степени важности на 2 группы: большие секретные сведения (наиболее важные и секретные) и сведения, не являющиеся большими, но подлежащие сохранению в тайне».

11. Является ли верным утверждение:

«Национальный институт стандартов и технологий в США по запросам компаний частного сектора должен готовить стандарты, руководства, инструкции о средствах и методах построения информационных систем, что позволяет сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральной информационной инфраструктурой»

12. Первые профессиональные спецслужбы созданы в VII веке:

Раздел 6. Организация защиты информации во Франции

Контролируемые ИДК: ПК-2.3

Тема 6.1. Организация защиты информации во Франции

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Состав основных грифов ограничения доступа: совершенно секретно, секретно и конфиденциально, а также гриф «ограниченного пользования» – для информации по вопросам ядерной энергии, определялся в соответствии с исполнительным указом президента США от 1 февраля:

2. Главная контрразведывательная служба ФРГ – Федеральное ведомство по охране конституции (БФФ), а также земельные ведомства по охране конституции (ЛФФ) созданы в:

3. Следующее определение понятия государственной тайны: “государственной тайной являются факты, предметы или сведения, которые доступны только ограниченному кругу лиц и должны держаться в тайне от иностранного государства, с тем, чтобы предотвращать опасность причинения серьёзного вреда внешней безопасности государства» содержится в § 93 УК:

4. Является ли верным утверждение: «Европейской Комиссией в 2006 г. была разработана и опубликована Стратегия безопасности информационного общества «Диалог, партнерство и расширение возможностей», в которой анализировались основные угрозы безопасности информационного общества, предлагались меры по обеспечению IT-безопасности на общеевропейском и национальном уровнях»

5. Регламент №2016/679 Европейского парламента и Совета ЕС от 27 апреля 2016г. «О защите прав физических лиц в отношении обработки персональных данных и о свободе перемещения таких данных» отменяет Директиву 95/46/ЕС?

6. Федеральный закон «О проверке на благонадежность» от 20 апреля 1994 г. регулирует вопросы допуска к государственной тайне в:

7. Япония относится к группе стран, в которых:

1. Приняты специальные законы о предупреждении недобросовестной конкуренции
2. Отсутствуют специальные законы о предупреждении недобросовестной конкуренции, а нормы о пресечении данных правонарушений содержатся в гражданских кодексах
3. Отсутствуют специальные законы о предупреждении недобросовестной конкуренции

8. Во Франции нарушение государственной монополии в некоторых областях хозяйственной деятельности относится к актам:

1. Недобросовестной конкуренции
2. Запрещенной конкуренции
3. Паразитической конкуренции

9. Термин «ноу-хау» впервые был применен в:

1. 1916 г. в американской судебной практике
2. Великобритании в судебном прецеденте 1948 г.
3. 40-е гг. XIX века в международных правовых документах

10. В Великобритании законодательное регулирование вопросов защиты государственной тайны осуществляется в соответствии с:

1. Законом о государственной тайне
2. Уголовным кодексом
3. Законом об измене

11. Ответственность за нарушение авторского права в Японии устанавливается в соответствии с:

1. Уголовным кодексом
2. Законом «Об авторском праве»
3. Законом «Об авторском праве и смежных правах»

Раздел 7. Организация защиты информации в Японии

Контролируемые ИДК: ПК-2.3

Тема 7.1. Организация защиты информации в Японии

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Патент на промышленный образец выдается в:

1. США
2. Франции
3. ФРГ

2. К странам, в которых отсутствуют специальные законы о предупреждении недобросовестной конкуренции, а нормы о пресечении данных правонарушений содержатся в гражданских кодексах, относятся:

1. Франция
2. Япония
3. Все перечисленное

3. В Германии специальная проверка лиц на разрешения допуска к государственной тайне в системе разведывательной службы осуществляется:

1. БНД
2. БФФ
3. МАД

4. Во Франции применяются следующие грифы секретности:

1. Особой важности
2. Ограниченный доступ
3. Секретно-оборона

5. Патент на промышленный образец выдается в:

1. Японии
2. Франции
3. ФРГ

6. Бернская конвенция по охране литературных и художественных произведений от 9 сентября 1886 г. имеет всемирный или региональный характер?

7. Является ли верным утверждение:

«В соответствии с Директивой 2019/790/EU об авторском праве и смежных правах на Едином цифровом рынке (ст. 6) в отношении учреждений, занимающихся сохранением культурного наследия, предусматривается право на создание копий любых произведений или других объектов авторского права, которые находятся в их постоянной коллекции, в любом формате или на любом носителе для целей сохранения данных объектов в том объеме, который необходим для данных целей. При этом данное исключение не налагает обязательств по обеспечению вознаграждения авторам или иным правообладателям».

8. Конвенция по охране промышленной собственности была принята в Париже 20 марта:

9. Европейское Агентство сетевой и информационной безопасности было создано с целью изучения рисков и угроз в отношении информационных систем, консультирования предприятий и государственных органов, координирования действий заинтересованных организаций:

10. Утверждение:

«Законодательно вводится понятие, которое отсутствует в правовой системе РФ – «деятельность, чувствительная с точки зрения безопасности». Лицо, которое допускается к такой деятельности, проходит проверку на благонадежность (разрешение на допуск к секретным сведениям)»
относится к:

11. Директива 2019/790/EU об авторском праве и смежных правах на Едином цифровом рынке имеет всемирный или региональный характер?

12. Понятие «Публицистический шпионаж», включающее разглашение государственной тайны в печатных органах или журналистами», применяется в УК:

Раздел 8. Международное сотрудничество в области защиты информации

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4

Тема 8.1. Международное сотрудничество в области защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Основным источником уголовного права Японии является Уголовный кодекс, принятый в:

1. 1907 г.
2. 1946 г.
3. 1985 г.

2. Законодательное регулирование вопросов защиты персональных данных в ФРГ первоначально было осуществлено:

1. В земле Гессен
2. На федеральном уровне
3. Вопросы решались одновременно на федеральном уровне и в федеральных землях

3. Во Франции Генеральный секретариат национальной обороны:

1. Является структурным подразделением Министерства обороны
2. Является органом парламентского контроля за деятельностью спецслужб
3. Осуществляет обобщение и анализ разведывательной информации, поступившей из спецслужб, министерств обороны и иностранных дел

4. Промышленный образец охраняется средствами авторского права в:

1. США
2. Франции
3. Японии

5. В Японии приняты следующие законы:

1. О коммерческой тайне
2. О предупреждении недобросовестной конкуренции
3. Все перечисленное

6. Главным контрразведывательным органом Франции является:

1. Следственное управление общественной безопасности
2. Управление по обеспечению оборонной безопасности
3. Управление государственной безопасности

7. В Великобритании приняты следующие законы:

1. О государственной тайне
2. О служебной тайне
3. О коммерческой тайне

8. Закон США об авторском праве в цифровую эпоху принят в:

9. В какой стране в 2004 г. принят Закон о доверии в цифровой экономике, в котором закреплено, что информационный посредник не несет какой-либо ответственности за размещенный контент при условии, что он "не знал о противозаконном характере материала или о фактах и обстоятельствах, которые указывают на такой характер, и с момента, когда он был об этом осведомлен, изъясл указанный материал или сделал доступ к нему невозможным"?

10. Следующее определение «Незаконная тайна – сведения, сохраняющиеся в тайне по отношению к партнерам по договорам, согласованным на государственном уровне, связанным с ограничением вооружений; факты нарушения свободного демократического конституционного строя» содержится в § 93 УК:

8. Оценочные материалы промежуточной аттестации

2 семестр, Экзамен

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4

Вопросы/Задания:

1. «Артхашастра или наука политики» и «Трактат о военном искусстве» как источники, характеризующие особенности и закономерности становления систем защиты информации в Древнем мире.

2. Формирование и особенности системы защиты информации в Древней Индии.
3. Формирование и особенности системы защиты информации в Древнем Китае.
4. Особенности формирования системы защиты информации в Японии в I – VIII вв.
5. Особенности систем защиты коммерческой тайны в странах Западной Европы в XIX – начале XX вв.
6. Правовая защита информации во Франции в XIX в. и ее влияние на формирование систем защиты информации в странах Западной Европы и Японии.
7. Этапы становления системы защиты информации в Германии в XIX – XX вв.
8. Особенности современного законодательства зарубежных стран по вопросам предупреждения недобросовестной конкуренции.
9. Становление системы защиты информации в США (начало XX в. – 30-е гг. XX в.).
10. Становление системы защиты информации в США в 40-е гг. XX в.
11. Становление системы защиты информации в США в 50—80-е гг. XX в.
12. Организация доступа к документам государственных органов в Великобритании. Основные критерии ограничения доступа к документам государственных органов, связанные с защитой информации.
13. Состав и основные направления деятельности органов защиты информации в Великобритании.
14. Контроль и координация деятельности органов защиты информации в Великобритании.
15. Организация доступа к документам государственных органов в Германии. Основные критерии ограничения доступа к документам государственных органов, связанные с защитой информации.
16. Состав и основные направления деятельности органов защиты информации в Германии.
17. Контроль и координация деятельности органов защиты информации в Германии.
18. Организация доступа к документам государственных органов во Франции. Основные критерии ограничения доступа к документам государственных органов, связанные с защитой информации.
19. Состав и основные направления деятельности органов защиты информации во Франции.
20. Контроль и координация деятельности органов защиты информации во Франции.

21. Организация доступа к документам государственных органов в Японии. Основные критерии ограничения доступа к документам государственных органов, связанные с защитой информации.
22. Состав и основные направления деятельности органов защиты информации в Японии.
23. Контроль и координация деятельности органов защиты информации в Японии.
24. Состав и основные направления деятельности органов защиты информации в США.
25. Обеспечение допуска и доступа к государственной тайне в США.
26. Особенности защиты государственной тайны в Великобритании и США.
27. Особенности защиты государственной тайны в Германии и Франции.
28. Особенности защиты служебной тайны в Германии и Франции.
29. Особенности защиты государственной тайны в Японии и США.
30. Особенности защиты служебной тайны в Японии и США.
31. Особенности защиты профессиональной тайны в Германии и Франции.
32. Особенности защиты служебной тайны в Великобритании и США.
33. Предупреждение недобросовестной конкуренции в Германии и Франции.
34. Предупреждение недобросовестной конкуренции в Германии и Японии.
35. Особенности защиты коммерческой тайны в Великобритании и США.
36. Особенности защиты персональных данных в Великобритании и США.
37. Особенности защиты коммерческой тайны в Германии и Франции.
38. Особенности защиты персональных данных в Германии и Франции.
39. Особенности защиты коммерческой тайны в Японии и США.
40. Особенности защиты персональных данных в Японии и Германии.
41. Особенности защиты банковской тайны в Германии и Франции
42. Особенности защиты интеллектуальной собственности в Германии и Японии
43. Особенности защиты интеллектуальной собственности в США и Великобритании

44. Особенности защиты интеллектуальной собственности в Германии и Франции
45. Классификация защищаемой информации в США и Германии
46. Классификация защищаемой информации в Германии и Франции
47. Особенности становления и развития правовой защиты государственной тайны в США и Японии
48. Особенности становления и развития правовой защиты государственной тайны в США и Великобритании
49. Требования к сотрудникам, имеющим доступ к защищаемой информации в США и Германии
50. Законодательство о доступе и ограничении доступа к документам государственных органов во Франции и Японии.
51. Возможности использования опыта защиты государственной тайны в Великобритании и США в Российской Федерации.
52. Возможности использования опыта защиты государственной тайны в Германии и Франции в Российской Федерации.
53. Возможности использования опыта защиты служебной тайны в Германии и Франции в Российской Федерации.
54. Возможности использования опыта защиты государственной тайны в Японии и США в Российской Федерации.
55. Возможности использования опыта защиты служебной тайны в Японии и США в Российской Федерации.
56. Возможности использования опыта защиты профессиональной тайны в Германии и Франции в Российской Федерации.
57. Возможности использования опыта защиты служебной тайны в Великобритании и США в Российской Федерации.
58. Возможности использования опыта предупреждения недобросовестной конкуренции в Германии и Франции в Российской Федерации.
59. Возможности использования опыта предупреждения недобросовестной конкуренции в Германии и Японии в Российской Федерации.
60. Возможности использования опыта защиты коммерческой тайны в Великобритании и США в Российской Федерации.
61. Возможности использования опыта защиты персональных данных в Великобритании и США в Российской Федерации.

62. Возможности использования опыта защиты коммерческой тайны в Германии и Франции в Российской Федерации.

63. Возможности использования опыта защиты персональных данных в Германии и Франции в Российской Федерации.

64. Возможности использования опыта защиты коммерческой тайны в Японии и США в Российской Федерации.

65. Возможности использования опыта защиты персональных данных в Японии и Германии в Российской Федерации.

66. Возможности использования опыта защиты банковской тайны в Германии и Франции в Российской Федерации.

67. Возможности использования опыта защиты интеллектуальной собственности в Германии и Японии в Российской Федерации.

68. Возможности использования опыта защиты интеллектуальной собственности в США и Великобритании в Российской Федерации.

69. Возможности использования опыта защиты интеллектуальной собственности в Германии и Франции в Российской Федерации.

70. Возможности использования опыта классификации защищаемой информации в США и Германии в Российской Федерации.

71. Возможности использования опыта классификации защищаемой информации в Германии и Франции в Российской Федерации.

72. Возможности использования опыта правовой защиты государственной тайны в США и Японии в Российской Федерации.

73. Возможности использования опыта правовой защиты государственной тайны в США и Великобритании в Российской Федерации.

74. Возможности использования опыта работы с сотрудниками, имеющими доступ к защищаемой информации в США и Германии в Российской Федерации.

75. Возможности использования опыта правовой защиты вопросов о доступе и ограничениях к доступу к документам государственных органов во Франции и Японии в Российской Федерации.

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Шлюндт Н. Ю. Международное право: практикум: практикум / Н. Ю. Шлюндт. - Международное право - Ставрополь: Северо-Кавказский федеральный университет, 2016. - 166 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/69402.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Международное право: учебник для студентов вузов, обучающихся по направлению подготовки «юриспруденция»: учебник для студентов вузов, обучающихся по направлению подготовки «юриспруденция» / А. Х. Абашидзе, К. К. Гасанов, Н. Д. Эриашвили [и др.]; под редакцией А. Х. Абашидзе. - Международное право - Москва: ЮНИТИ-ДАНА, 2023. - 519 с. - 978-5-238-03025-8. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/141599.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Никифоров С. Н. Защита информации: учебное пособие / С. Н. Никифоров. - Защита информации - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015. - 384 с. - 978-5-9227-0585-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/74365.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Прохорова О. В. Информационная безопасность и защита информации: учебник для вузов: учебник для вузов / О. В. Прохорова. - 5-е изд., стер. - Санкт-Петербург: Лань, 2023. - 124 с. - 978-5-507-46010-6. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/293009.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Меньшенина Н. Н. Международное право: учебное пособие: учебное пособие / Н. Н. Меньшенина. - Международное право - Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2016. - 100 с. - 978-5-7996-1805-6. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/69628.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Международное право: учебное пособие для студентов вузов, обучающихся по специальности 030501 «юриспруденция»: учебное пособие для студентов вузов, обучающихся по специальности 030501 «юриспруденция» / Ю. В. Трунцевский, О. Ш. Петросян, Р. С. Маковик, А. В. Лобаков, А. Э. Сорокина. - Международное право - Москва: ЮНИТИ-ДАНА, 2017. - 455 с. - 978-5-238-01815-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/81658.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)

4. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"

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

Автоматизированное рабочее место (АРМ) - 15 шт.
Доска настенная одноэлементная - 2 шт.
Проектор - 1 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.
Доска настенная одноэлементная - 2 шт.
Интерактивная панель - 1 шт.
Проектор - 1 шт.

Учебная аудитория

Автоматизированное рабочее место (АРМ) - 6 шт.
Доска настенная одноэлементная - 1 шт.
Проектор - 1 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.