



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.03 СТАНДАРТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ»**

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность(профиль) подготовки: Защита информации в геоинформационных системах
и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 2 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 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 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

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 - приобретение обучающимися знаний в области нормативных и технических требований, стандартов и методик, регулирующих процессы обеспечения защиты информации, а также систем менеджмента информационной безопасности.

Задачи изучения дисциплины:

- Изучение принципов оценки степени соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности.;
- Освоение навыков применения программно-аппаратных и технических средств защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности.;
- Исследование, совершенствование существующих и создание новых методов защиты информации..

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

Компетенции, индикаторы и результаты обучения

ПК-1 Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.1 Разрабатывает профили защиты компьютерных систем

Знать:

ПК-1.1/Зн1 Теоретические основы угроз безопасности информации

Уметь:

ПК-1.1/Ум1 Разрабатывать политики безопасности, основываясь на анализе потребностей организации и действующих угроз

Владеть:

ПК-1.1/Нв1 Разрабатывать комплексные профили защиты для различных типов компьютерных систем, учитывая их специфику и назначение

ПК-1.2 Формирует политики безопасности компьютерных систем и сетей

Знать:

ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

Уметь:

ПК-1.2/Ум2 Уметь применять стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

Владеть:

ПК-1.2/Нв2 Владеть навыками применения стандартов в области информационной безопасности при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.03 «Стандарты в области защиты информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 3.

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)
3 семестр	144	4	34	34	76	Зачет с оценкой
Всего	144	4	34	34	76	

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. Федеральное законодательство и иные подзаконные акты	10	2		8	ПК-1.1
Тема 1.1. Федеральное законодательство и иные подзаконные акты	10	2		8	
Раздел 2. Источники права	6	2		4	ПК-1.2
Тема 2.1. Источники права	6	2		4	

Раздел 3. Федеральный уровень законодательства	8	2	2	4	ПК-1.1 ПК-1.2
Тема 3.1. Федеральный уровень законодательства	8	2	2	4	
Раздел 4. Региональный уровень законодательства	6	2		4	ПК-1.1 ПК-1.2
Тема 4.1. Региональный уровень законодательства	6	2		4	
Раздел 5. Отрасли права	6	2		4	ПК-1.2
Тема 5.1. Отрасли права	6	2		4	
Раздел 6. Федеральные законы	24	8	8	8	ПК-1.1
Тема 6.1. Федеральные законы	24	8	8	8	
Раздел 7. Международные организации по стандартизации	12	4		8	ПК-1.2
Тема 7.1. Международные организации по стандартизации	12	4		8	
Раздел 8. ГОСТы и технические регламенты	10	2	4	4	ПК-1.2
Тема 8.1. ГОСТы и технические регламенты	10	2	4	4	
Раздел 9. Организация информационной безопасности на основе применения международных и национальных стандартов	12	2		10	ПК-1.1
Тема 9.1. Организация информационной безопасности на основе применения международных и национальных стандартов	12	2		10	
Раздел 10. Обзор международных ИБ-стандартов	20	4	8	8	ПК-1.1 ПК-1.2
Тема 10.1. Обзор международных ИБ-стандартов	20	4	8	8	
Раздел 11. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ	30	4	12	14	ПК-1.2
Тема 11.1. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ	30	4	12	14	
Итого	144	34	34	76	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Федеральное законодательство и иные подзаконные акты

Тема 1.1. Федеральное законодательство и иные подзаконные акты

1. Конституция РФ
2. Федеральные конституционные законы
3. Международные договоры и соглашения РФ

Раздел 2. Источники права

Тема 2.1. Источники права

Источник права в материальном, идеологическом и формальном (юридическом) смысле. Правовой обычай, общественные отношения, правосознание и правовая культура, способы закрепления и существования норм права.

Раздел 3. Федеральный уровень законодательства

Тема 3.1. Федеральный уровень законодательства

1. Федеральные законы
2. Акты президента РФ
3. Акты Правительства РФ
4. Ведомственные нормативные акты

Раздел 4. Региональный уровень законодательства

Тема 4.1. Региональный уровень законодательства

1. Конституции и уставы субъектов РФ
2. Законы субъектов РФ

Раздел 5. Отрасли права

Тема 5.1. Отрасли права

Отрасли права и субъекты законодательной инициативы

Раздел 6. Федеральные законы

Тема 6.1. Федеральные законы

1. Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
2. ФЗ от 21.07.1993г. №5485-1 «О государственной тайне»
3. Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»
4. Федеральный закон 390-ФЗ от 28.12.2010г. «О безопасности»
5. 63-ФЗ «Об электронной подписи»
6. Федеральный закон 184-ФЗ от 27.12.2002 «О техническом регулировании»
7. 98-ФЗ «О коммерческой тайне»
8. 152-ФЗ «О персональных данных»

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 7. Международные организации по стандартизации

Тема 7.1. Международные организации по стандартизации

1. Международная организация по стандартизации (ИСО)
2. Международная электротехническая комиссия (МЭК).
3. Европейская экономическая комиссия ООН (ЕЭК ООН).
4. Продовольственная и сельскохозяйственная организации ООН (ФАО).
5. Всемирная организация здравоохранения (ВОЗ).
6. Комиссия "Кодекс Алиментариус" по разработке стандартов на продовольственные товары

Раздел 8. ГОСТы и технические регламенты

Тема 8.1. ГОСТы и технические регламенты

1. Что такое ГОСТ?
2. Что такое технический регламент?
3. Сравнение основных концепций подтверждения соответствия

Раздел 9. Организация информационной безопасности на основе применения международных и национальных стандартов

Тема 9.1. Организация информационной безопасности на основе применения международных и национальных стандартов

1. Зачем нужны ИБ-стандарты
2. Какие бывают ИБ-стандарты

Раздел 10. Обзор международных ИБ-стандартов

Тема 10.1. Обзор международных ИБ-стандартов

Краткий обзор международных ИБ-стандартов с целью ознакомления с ними

Раздел 11. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ

Тема 11.1. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ

Краткий обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ

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: Зачет с оценкой, 3 семестр.

Зачет с оценкой 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 – 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 6. Федеральные законы

Контролируемые ИДК: ПК-1.1

Тема 6.1. Федеральные законы

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие бывают ИБ-стандарты:

1. Технические и ориентированные
2. Контрольные и процессные
3. Технические (контрольные) и процессно-ориентированные
4. Технические и контрольные

2. Что помогают сделать технические стандарты:

1. Вычислять уязвимости информационной системы
2. Выстраивать техническую защиту информации — выбрать необходимый комплекс защитных мер и провести их грамотную настройку
3. Выбрать необходимый комплекс защитных мер
4. Блокировать угрозы информационной системы

3. Электронная подпись это:

1. Электронный документ, выданный удостоверяющим центром и подтверждающий принадлежность подписи владельцу
2. Уникальная последовательность символов, предназначенная для подтверждения принадлежности подписи владельца
3. Уникальная последовательность символов, предназначенная для проверки подлинности подписи владельца
4. Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

4. Видами электронных подписей являются:

1. Простая электронная подпись и усиленная электронная подпись
2. Простая электронная подпись и сложная электронная подпись
3. Подтвержденная электронная подпись и усиленная электронная подпись
4. Утвержденная электронная подпись и усиленная электронная подпись

5. Усиленная электронная подпись различается на:

1. Усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись
2. Усиленная простая электронная подпись и усиленная сложная электронная подпись
3. Усиленная подтвержденная электронная подпись и усиленная квалифицированная электронная подпись
4. Усиленная утвержденная электронная подпись и усиленная квалифицированная электронная подпись

6. Согласно закону "О техническом регулировании", стандарт - это:

1. Документ, в котором в целях добровольного многократного использования сформулированы характеристики продукции
2. Требование соблюдения единообразия технических и иных характеристик
3. Изделие, характеристики которого считаются эталонными
4. Документ, содержащий требования к общей терминологии

7. Согласно закону "О техническом регулировании", стандартизация - это

1. Деятельность по выработке единых требований к техническим и иным характеристикам продукции
2. Деятельность по установлению правил и характеристик в целях их добровольного многократного использования
3. Деятельность по установлению единообразия в сфере производства и иных сферах
4. Деятельность по приведению к единым стандартам продукции

8. Согласно закону "О техническом регулировании", принципом стандартизации является

1. Приоритет национальных законодательных и технических актов
2. Обеспечение конкурентоспособности российских товаров и услуг на мировом рынке
3. Применение международного стандарта, как основы разработки национального стандарта
4. Лоббирование интересов РФ в межгосударственных отношениях

9. В "Оранжевой книге" (TCSEC) фигурируют понятия:

1. Ядро безопасности
2. Периметр безопасности
3. Центр безопасности
4. Круг безопасности

10. В "Гармонизированных критериях Европейских стран" фигурируют понятия:

1. Цель оценки
2. Система оценки
3. Объект оценки
4. Виды оценки

11. В рекомендациях X.800 (TCSEC) фигурируют понятия:

1. Регулятор безопасности
2. Сервис безопасности
3. Механизм безопасности
4. Стандарты безопасности

12. "Общие критерии" содержат следующие основные виды требований безопасности:

1. Архитектурные требования
2. Функциональные требования
3. Требования доверия
4. Виды требований

13. Сколько форм подтверждения соответствия выделено в ФЗ № 184 "О техническом регулировании":

1. 1
2. 2
3. 3
4. 4

14. В стандарте BS 7799 разъясняются следующие понятия и процедуры:

1. Безопасность интерфейсов
2. Безопасность персонала
3. Физическая безопасность
4. Общая безопасность

15. Изучение стандартов и спецификаций необходимо, поскольку:

1. Создаются условия для разработки безопасных систем
2. Они являются формой накопления знаний с целью многократного использования
3. Невыполнение их требований преследуется по закону
4. Является дополнительной профессиональной подготовкой специалиста

16. Стандарт это - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения

17. Стандартизация - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг

18. Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию

19. Главная задача стандартов информационной безопасности — согласовать позиции и цели производителей, потребителей и аналитиков-классификаторов в процессе создания и эксплуатации продуктов информационных технологий

20. Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

21. Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи

22. Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи

23. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом

24. ФСТЭК является федеральным органом осуществляющим деятельность по аккредитации объектов информатизации

25. ГОСТ — это нормативно-правовой документ, в соответствии требованиями которого производится стандартизация производственных процессов и оказания услуг

26. Автоматизированная система, в которой обрабатывается конфиденциальная информация, относится к основным техническим средствам и системам

27. Автоматизированная система это — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

28. ФСТЭК является лицензирующим органом в области технической защиты конфиденциальной информации

29. Аттестация объекта информатизации проводится до начала обработки информации, подлежащей защите

30. Стандарт ISO/IEC 15408 устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки, которой посвящены различные части стандарта, предназначенного в целом для использования в качестве основы при оценке характеристик безопасности продуктов ИТ

Раздел 11. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ

Контролируемые ИДК: ПК-1.2

Тема 11.1. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Согласно закону "О техническом регулировании", стандарты могут содержать требования к:

1. Структуре документации
2. Терминологии
3. Символике
4. Правилам исполнения документа

2. Какой ГОСТ определяет порядок создания системы защиты информации автоматизированной системы в защищенном исполнении:

1. ГОСТ Р 50922-2006
2. ГОСТ Р 51583-2014

3. ГОСТ Р ИСО/МЭК ТО 13335-5-2006

4. ГОСТ Р 56115-2014

3. Рекомендации X.509 регламентируют формат:

1. Сертификата безопасности
2. Сертификата открытого ключа
3. Сертификата директории
4. Сертификата качества

4. В стандарте BS 7799 выделены следующие ключевые регуляторы безопасности:

1. Документ о политике информационной безопасности
2. Программа безопасности
3. Регулярное выявление уязвимых мест
4. Стратегия безопасности

5. Версия 2.1 "Общих критериев" содержит:

1. 9 классов функциональных требований безопасности
2. 10 классов функциональных требований безопасности
3. 11 классов функциональных требований безопасности
4. 12 классов функциональных требований безопасности

6. Согласно "Общим критериям", предположения безопасности:

1. Являются частью описания среды, в которой функционирует объект оценки
2. Являются частью описания объекта оценки
3. Являются частью политики безопасности организации, эксплуатирующей объект оценки
4. Являются частью объекта оценки

7. Согласно стандарту BS 7799, меры по безопасному администрированию систем и сетей разбиты на следующие подгруппы:

1. Профилактическое обслуживание
2. Повседневное обслуживание
3. Сервисное обслуживание
4. Базовое обслуживание

8. В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

1. Удостоверение
2. Билет
3. Мандат
4. Пропуск

9. В профиле защиты, регламентирующем выпуск и управление сертификатами, предусмотрены следующие роли:

1. Офицера безопасности
2. Офицера по связям с удостоверяющими центрами
3. Аудитора
4. Контролера

10. Требования "Общих критериев" группируются в:

1. Классы
2. Подклассы
3. Группы
4. Подгруппы

11. Какой из федеральных законов регламентирует информационную безопасность в Российской Федерации:

1. "О безопасности"
2. "Об информации, информационных технологиях и о защите информации"
3. "О государственной тайне"
4. "О персональных данных"

12. Ведущим государственным учреждением в РФ, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне является

1. ФСБ
2. ФСТЭК
3. Роспотребнадзор
4. Минкомсвязь

13. Из скольких частей состоит стандарт ГОСТ Р ИСО/МЭК 15408:

1. Одной
2. Двух
3. Трех
4. Четырех

14. Сколько устанавливается классов защищенности автоматических систем от не санкционированного доступа к информации?

1. Семь
2. Восемь
3. Девять
4. Десять

15. В соответствии с ФЗ №149 "Об информации, информационных технологиях и о защите информации" информация разделяется на следующие категории:

1. Общедоступная и конфиденциальная
2. Общедоступная и ограниченного доступа
3. Ограниченного доступа и государственная тайна
4. Конфиденциальная информация и государственная тайна

16. Какой документ является основным нормативным документом в области регулирования в Российской Федерации?

1. Федеральный закон N 184 "О техническом регулировании"
2. Федеральный закон N 149 "Об информации, информационных технологиях и о защите информации"
3. Федеральный закон N 162 "О стандартизации в Российской Федерации"
4. Федеральный закон N 101 "О международных договорах Российской Федерации"

17. Под аудитом информационной безопасности следует понимать форму независимой оценки состояния информационной безопасности объекта аудита (информационная система, автоматизированная система, организация как объект защиты в целом и т.п.) на соответствие заданным критериям (например, требованиям действующего законодательства или принятых корпоративных стандартов, отсутствия уязвимостей, содержащиеся в банке данных угроз безопасности информации и т.п.)

18. Угроза безопасности информации это - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

19. Контроль эффективности защиты информации - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации

20. Защита информации это направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

21. Система защиты информации это совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации

22. Объект защиты информации это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации

23. Носитель защищаемой информации это физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин

24. Уязвимость информационной системы это свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации

25. Вредоносная программа это программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы

26. Модель угроз безопасности информации это физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации

27. Средство защиты информации это техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации

28. Лицензирование в области защиты информации это деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ

29. Сертификация на соответствие требованиям по безопасности информации это форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров

30. Специальное исследование объекта защиты информации это исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации

31. Специальная проверка это проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств

8. Оценочные материалы промежуточной аттестации

3 семестр, Зачет с оценкой

Контролируемые ИДК: ПК-1.1 ПК-1.2

Вопросы/Задания:

1. Что входит в понятие информационных систем согласно ФЗ от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

2. Средства защиты информации согласно ФЗ от 21.07.1993г. № 5485-1 «О государственной тайне»

3. Кто относится к понятию инсайдер согласно ФЗ от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»

4. Основные принципы обеспечения безопасности согласно ФЗ 390-ФЗ от 28.12.2010г. «О безопасности»

5. Виды электронных подписей согласно 63-ФЗ «Об электронной подписи»

6. Правила формирования перечня документов по стандартизации согласно ФЗ 184-ФЗ от 27.12.2002 «О техническом регулировании»

7. Охрана конфиденциальности информации согласно 98-ФЗ «О коммерческой тайне»

8. Что относится к понятию персональные данные согласно 152-ФЗ «О персональных данных»

9. Что разрабатывает и публикует Международная организация по стандартизации (ИСО)

10. Что готовит и публикует Международная электротехническая комиссия (МЭК)

11. Для чего служит и что обеспечивает Европейская экономическая комиссия ООН (ЕЭК ООН)

12. Приоритетные направления деятельности и стандарты Продовольственной и сельскохозяйственной организации ООН (ФАО)

13. Задачи решаемые Всемирной организацией здравоохранения (ВОЗ)

14. Основные направления деятельности Комиссии "Кодекс Алиментариус" по разработке стандартов на продовольственные товары

15. Что такое ГОСТ?

16. Что такое технический регламент?

17. Сравнение основных концепций подтверждения соответствия

18. Зачем нужны ИБ-стандарты

19. Какие бывают ИБ-стандарты

20. Что означает COBIT?

21. Что такое ITIL?

22. Основные факторы, влияющие на информационную безопасность предприятия согласно ISO 17799

23. Основные принципы обеспечения информационной безопасности и меры обеспечения информационной безопасности процедурного уровня

24. Аудит состояния информационной безопасности на предприятии согласно ISO 17799

25. Сфера применения и средства контроля в ISO 17799

26. Преимущества, получаемые после аудита по требованиям стандарта ISO 17799 и недостатки

27. Стандарты Серии ISO/IEC 27XXX

28. Область применения ISO/IEC 15408

29. Канадские критерии оценки безопасности надежных компьютерных систем

30. Федеральные критерии безопасности информационных технологий

31. Единые критерии оценки безопасности информационных технологий, ISO/IEC 15408

32. Общая методология оценки безопасности информационных технологий

33. Перспективы практической реализации положений ISO/IEC 15408 и СЕМ - 97/017

34. Что обозначает NIST и его функции?

35. Как действует SANS. CIS 20?

36. Что оценивает модель O-ISM3?

37. Краткий обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ

38. Краткий обзор особенностей стандарта ГОСТ Р ИСО/МЭК 15408 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

39. Краткий обзор особенностей стандарта ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология (ИТ)». Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем

40. Краткий обзор особенностей стандарта ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»

41. Краткий обзор особенностей стандарта ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

42. Краткий обзор особенностей стандарта ГОСТ Р 58142-2018 Информационная технология (ИТ). Методы и средства обеспечения безопасности

43. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС)

44. Стандарты по ИБ в соответствии с их назначением: общие, информационная технология, менеджмент риска, защита информации

45. Национальные стандарты, разработанные ТК 362 и принятые Ростехрегулированием (Росстандартом)

46. Что такое ITSM?

47. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045»

48. Требования ГОСТ 34 серия

49. Правовое обеспечение РФ в области информационной безопасности и защиты информации

50. Международные договоры и соглашения РФ в области информационной безопасности и защиты информации

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Сычев Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие: учебное пособие / Ю. Н. Сычев. - Стандарты информационной безопасности. Защита и обработка конфиденциальных документов - Саратов: Вузовское образование, 2018. - 195 с. - 978-5-4487-0128-3. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/72345.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Белоус А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. - Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения - Москва: Техносфера, 2021. - 482 с. - 978-5-94836-612-8. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/108023.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Бекетнова Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем: учебное пособие: учебное пособие / Ю. М. Бекетнова, Г. О. Крылов, С. Л. Ларионова. - Международные основы и стандарты информационной безопасности финансово-экономических систем - Москва: Прометей, 2018. - 174 с. - 978-5-907003-27-9. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/94454.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. 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

Не используются.

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://www.elibrary.ru/> - НЭБ eLIBRARY

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

Учебная аудитория

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.