



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

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

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

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.09 НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Доцент кафедры Информационно-измерительных систем, к.э.н.
Трофимов С. В.

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

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

Согласование и утверждение

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

Содержание

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

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - приобретение обучающимися знаний в области правового обеспечения информационной безопасности, охватывающих структуру и взаимосвязи национального законодательства, а также методологию оценки соответствия объектов информатизации требованиям международных и национальных стандартов в системе технического регулирования.

Задачи изучения дисциплины:

- сформировать целостное представление о системе российского и международного законодательства, а также методологии стандартизации в области защиты информации и обеспечения информационной безопасности;
- обучить ориентироваться в иерархии нормативных правовых актов, правильно интерпретировать требования регуляторов и применять положения ГОСТов для решения практических задач по созданию комплексных систем защиты информации;
- выработать способность проводить правовую экспертизу проектных решений в области информационной безопасности и разрабатывать организационно-распорядительную документацию, необходимую для приведения деятельности организации в соответствие с требованиями законодательства.

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

Компетенции, индикаторы и результаты обучения

ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности

ОПК-2.3.1 Знает характеристики, достоинства и недостатки различных мер, применяемых для обеспечения безопасности объекта защиты

Знать:

ОПК-2.3.1/Зн2 Иерархическую структуру законодательства РФ в области информации, информационных технологий и защиты информации

Уметь:

ОПК-2.3.1/Ум2 Осуществлять поиск актуальных редакций нормативных документов, приказов регулирующих органов и разъяснений судебной практики по вопросам информационной безопасности

Владеть:

ОПК-2.3.1/Нв3 Терминологическим аппаратом в области технического регулирования и стандартизации информационной безопасности

ОПК-2.3.2 Разрабатывает, внедряет и поддерживает работу по обеспечению безопасности объекта защиты автоматизированных систем

Знать:

ОПК-2.3.2/Зн2 Содержание ключевых федеральных законов в области информационной безопасности

Уметь:

ОПК-2.3.2/Ум3 Анализировать требования различных регуляторов применительно к конкретному объекту защиты и определять применимые меры защиты

Владеть:

ОПК-2.3.2/Нв2 Методиками оценки соответствия состояния информационной безопасности организации требованиям законодательства и стандартов

ОПК-2.3.3 Применяет нормативные правовые акты и стандарты, регламентирующие требования и порядок применения мер по обеспечению безопасности объекта защиты

Знать:

ОПК-2.3.3/Зн2 Классификацию и назначение национальных и международных стандартов, регламентирующих управление информационной безопасностью и менеджмент рисков

Уметь:

ОПК-2.3.3/Ум2 Составлять проекты локальных нормативных актов по обеспечению режима конфиденциальности и безопасности информации в организации

Владеть:

ОПК-2.3.3/Нв2 Навыками правовой экспертизы договоров, технических заданий и проектной документации на предмет их соответствия обязательным требованиям по защите информации

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.09 «Нормативные акты и стандарты по информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 5.

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

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
5 семестр	144	4	17	17	74	Экзамен (36)
Всего	144	4	17	17	74	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Лекционные занятия	Практические занятия	Самостоятельная работа	Промежуточная аттестация

	Всё	Лек	Пр	Сам	Плн обу рез: прс
Раздел 1. Федеральное законодательство и иные подзаконные акты	1	1			ОПК-2.3. 1
Тема 1.1. Федеральное законодательство и иные подзаконные акты	1	1			ОПК-2.3. 2 ОПК-2.3. 3
Раздел 2. Источники права	2	2			ОПК-2.3. 1
Тема 2.1. Источники права	2	2			ОПК-2.3. 2 ОПК-2.3. 3
Раздел 3. Федеральный уровень законодательства	13	2	1	10	ОПК-2.3. 1
Тема 3.1. Федеральный уровень законодательства	13	2	1	10	ОПК-2.3. 2 ОПК-2.3. 3
Раздел 4. Региональный уровень законодательства	6			6	ОПК-2.3. 1
Тема 4.1. Региональный уровень законодательства	6			6	ОПК-2.3. 2 ОПК-2.3. 3
Раздел 5. Отрасли права	2	2			ОПК-2.3. 1
Тема 5.1. Отрасли права	2	2			ОПК-2.3. 2 ОПК-2.3. 3
Раздел 6. Федеральные законы	22	2		20	ОПК-2.3. 1
Тема 6.1. Федеральные законы	22	2		20	ОПК-2.3. 2 ОПК-2.3. 3
Раздел 7. Международные организации по стандартизации	8	2		6	ОПК-2.3. 1
Тема 7.1. Международные организации по стандартизации	8	2		6	ОПК-2.3. 2 ОПК-2.3. 3
Раздел 8. ГОСТы и технические регламенты	8		2	6	ОПК-2.3. 1

Тема 8.1. ГОСТы и технические регламенты	8		2	6	ОПК-2.3. 2 ОПК-2.3. 3
Раздел 9. Организация информационной безопасности на основе применения международных и национальных стандартов	6	2	4		ОПК-2.3. 1 ОПК-2.3. 2 ОПК-2.3. 3
Тема 9.1. Организация информационной безопасности на основе применения международных и национальных стандартов	6	2	4		
Раздел 10. Обзор международных ИБ-стандартов	16	2	4	10	ОПК-2.3. 1 ОПК-2.3. 2 ОПК-2.3. 3
Тема 10.1. Обзор международных ИБ-стандартов	16	2	4	10	
Раздел 11. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ	24	2	6	16	ОПК-2.3. 1 ОПК-2.3. 2 ОПК-2.3. 3
Тема 11.1. Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ	24	2	6	16	
Итого	108	17	17	74	

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

Введение в правовое регулирование ИБ. Конституционные основы. Кодексы Российской Федерации. Указы Президента Российской Федерации. Постановления Правительства Российской Федерации.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Источники права

Тема 2.1. Источники права

Понятие источника права в информационной сфере. Конституция Российской Федерации.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 3. Федеральный уровень законодательства

Тема 3.1. Федеральный уровень законодательства

Федеральный уровень:

1. Конституция
2. Федеральные конституционные законы
3. Международные договоры и соглашения РФ
4. Федеральные законы
5. Акты президента РФ
6. Акты Правительства РФ
7. Ведомственные нормативные акты

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 4. Региональный уровень законодательства

Тема 4.1. Региональный уровень законодательства

Региональный уровень законодательства:

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

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 5. Отрасли права

Тема 5.1. Отрасли права

Отрасли права и субъекты законодательной инициативы.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 6. Федеральные законы

Тема 6.1. Федеральные законы

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

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.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 8. ГОСТы и технические регламенты

Тема 8.1. ГОСТы и технические регламенты

ГОСТы и технические регламенты:

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

Текущий контроль

Вид (форма) контроля
Тестирование

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

Организация информационной безопасности на основе применения международных и национальных стандартов:

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

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 10. Обзор международных ИБ-стандартов

Тема 10.1. Обзор международных ИБ-стандартов

Краткий обзор международных ИБ-стандартов:

1. COBIT
2. ITIL и ITSM
3. ISO
4. NIST
5. SANS. CIS 20
6. O-ISM3

Текущий контроль

Вид (форма) контроля
Тестирование

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.

1. Обзор особенностей стандарта ГОСТ Р ИСО/МЭК 15408 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» в трех частях.
2. Обзор особенностей стандарта ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология (ИТ)». Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.
3. Обзор особенностей стандарта ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
4. Обзор особенностей стандарта ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».
5. Обзор особенностей стандарта ГОСТ Р 58142-2018 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045» в двух частях
6. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС)
7. Перечень стандартов по ИБ в соответствии с их назначением:
 - Общие
 - Информационная технология
 - Менеджмент риска
 - Защита информации
8. ГОСТ 34 серия
9. ГОСТ Серия 27000
10. Перечень национальных стандартов, разработанных ТК 362 и принятых Ростехрегулированием (Росстандартом)

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, 5 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;

- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 1. Федеральное законодательство и иные подзаконные акты

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 1.1. Федеральное законодательство и иные подзаконные акты

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что из перечисленного относится к федеральному законодательству в сфере информационной безопасности?

- 1) Устав предприятия по защите коммерческой тайны
- 2) Федеральный закон «Об информации, информационных технологиях и о защите информации»
- 3) Инструкция по делопроизводству конкретного министерства
- 4) Правила внутреннего трудового распорядка организации

2. Какой документ имеет высшую юридическую силу после Конституции РФ в системе федерального законодательства?

- 1) Указ Президента РФ
- 2) Постановление Правительства РФ
- 3) Приказ Минцифры России
- 4) Федеральный конституционный закон

3. К подзаконным актам в сфере информационной безопасности относятся:

- 1) Конституция РФ
- 2) Приказы ФСТЭК России
- 3) Гражданский кодекс РФ
- 4) Ратифицированные международные договоры

Раздел 2. Источники права

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 2.1. Источники права

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой из перечисленных источников права является основным в российской правовой системе?

- 1) Правовой обычай
- 2) Судебный прецедент
- 3) Нормативный правовой акт
- 4) Религиозный текст

2. Международный договор Российской Федерации в области информационной безопасности:

- 1) Не является источником права

- 2) Применяется только после опубликования в ведомственной газете
- 3) Имеет приоритет перед внутренним законодательством, если предусмотрено правило о приоритете
- 4) Действует только на территории подписавших его регионов

3. Что из перечисленного является источником права в сфере технического регулирования информационной безопасности?

- 1) Лучшие практики, описанные в блогах экспертов
- 2) Технический регламент
- 3) Корпоративный стандарт разработки ПО
- 4) Устные распоряжения руководителя

Раздел 3. Федеральный уровень законодательства

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 3.1. Федеральный уровень законодательства

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. На федеральном уровне правовое регулирование в сфере ИБ осуществляет:

- 1) Только Президент РФ
- 2) Федеральное Собрание РФ
- 3) Органы местного самоуправления
- 4) Региональные законодательные собрания

2. Какой орган исполнительной власти на федеральном уровне уполномочен в области обеспечения безопасности критической информационной инфраструктуры?

- 1) Министерство просвещения
- 2) ФСТЭК России
- 3) Федеральное агентство по туризму
- 4) Пенсионный фонд РФ

3. Федеральный закон «О персональных данных» (152-ФЗ) распространяется на:

- 1) Только государственные органы
- 2) Все операторы, осуществляющие обработку персональных данных граждан РФ
- 3) Только коммерческие банки
- 4) Исключительно иностранные компании

Раздел 4. Региональный уровень законодательства

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 4.1. Региональный уровень законодательства

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Может ли субъект РФ принимать законы в области информационной безопасности, противоречащие федеральным?

- 1) Да, в приоритете региональное законодательство
- 2) Нет, региональные законы не могут противоречить федеральным
- 3) Да, если это одобрено местным референдумом
- 4) Нет, субъекты РФ вообще не имеют права законодательствовать в этой сфере

2. Пример регионального нормативного акта в сфере ИБ:

- 1) Постановление правительства Москвы о порядке обеспечения безопасности городских информационных систем
- 2) Федеральный закон «О связи»
- 3) Уголовный кодекс РФ
- 4) ГОСТ Р 57580.1-2017

3. Региональное законодательство в сфере ИБ обычно касается:

- 1) Вопросов обороны и безопасности государства
- 2) Вопросов использования региональных информационных систем и защиты данных граждан в рамках полномочий субъекта
- 3) Установления уголовной ответственности за киберпреступления
- 4) Лицензирования деятельности в области шифрования

Раздел 5. Отрасли права

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 5.1. Отрасли права

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Нормы какой отрасли права устанавливают ответственность за неправомерный доступ к компьютерной информации?

- 1) Гражданское право
- 2) Уголовное право
- 3) Административное право
- 4) Конституционное право

2. Какая отрасль права регулирует отношения, связанные с возмещением убытков от утечки персональных данных?

- 1) Гражданское право
- 2) Трудовое право
- 3) Налоговое право
- 4) Финансовое право

3. Кодекс об административных правонарушениях содержит составы правонарушений в сфере ИБ, например:

- 1) Шпионаж в пользу IT-компаний
- 2) Государственная измена
- 3) Нарушение требований о защите информации
- 4) Убийство, совершенное по принуждению со стороны нейросетей

Раздел 6. Федеральные законы

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 6.1. Федеральные законы

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой федеральный закон регулирует отношения, связанные с использованием электронной подписи?

- A) ФЗ-149
- b) ФЗ-63
- c) ФЗ-53
- d) ФЗ-67

2. Основной целью Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» является:

- 1) Защита персональных данных граждан
- 2) Регулирование работы поисковых систем
- 3) Обеспечение устойчивого функционирования значимых объектов КИИ при проведении компьютерных атак
- 4) Контроль за оборотом средств криптографии

3. Федеральный закон «О персональных данных» (152-ФЗ) требует от оператора:

- 1) Публиковать все базы данных в открытом доступе
- 2) Хранить данные граждан РФ только на серверах, расположенных за рубежом
- 3) Обеспечивать конфиденциальность персональных данных и принимать меры по их защите
- 4) Уведомлять каждого гражданина лично при каждой передаче данных третьим лицам

Раздел 7. Международные организации по стандартизации

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 7.1. Международные организации по стандартизации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какая международная организация разрабатывает стандарты в области информационных технологий, включая знаменитое семейство стандартов ISO/IEC 27000?

- 1) UN
- 2) WTO
- 3) ISO
- 4) Интерпол

2. Какой орган в рамках Международного союза электросвязи занимается вопросами стандартизации в телекоммуникациях и кибербезопасности?

- 1) МВФ
- 2) ITU-T
- 3) Всемирный банк
- 4) Европейский суд по правам человека

3. Какую роль играют международные стандарты в национальной системе стандартизации РФ?

- 1) Они не имеют никакой силы и не учитываются
- 2) Они могут быть приняты как национальные стандарты
- 3) Они обязательны к применению без всякой адаптации
- 4) Они действуют только на территории стран Евросоюза

Раздел 8. ГОСТы и технические регламенты

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 8.1. ГОСТы и технические регламенты

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Чем технический регламент отличается от ГОСТа в сфере информационной безопасности?

- 1) Технический регламент носит добровольный характер, а ГОСТ — обязательный
- 2) Технический регламент имеет обязательную силу, а ГОСТ применяется добровольно, если иное не оговорено
- 3) Технический регламент разрабатывает предприятие, а ГОСТ — государство
- 4) Это одно и то же

2. Какой ГОСТ устанавливает требования к защите информации при использовании технологии облачных вычислений?

- 1) ГОСТ Р 57580.1-2017
- 2) ГОСТ Р 51141-98
- 3) ГОСТ 28147-89
- 4) ГОСТ Р 6.30-2003

3. Какой статус имеет ГОСТ Р в России?

- 1) Это стандарт иностранного государства
- 2) Это национальный стандарт Российской Федерации

- 3) Это стандарт отрасли связи
- 4) Это внутренний стандарт конкретной компании

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

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

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

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой подход лежит в основе организации ИБ согласно стандартам семейства ISO/IEC 27000?

- 1) Реактивный подход
- 2) Процессный подход
- 3) Запретительный подход
- 4) Интуитивный подход

2. Для чего при организации ИБ применяют стандарт ГОСТ Р ИСО/МЭК 27001?

- 1) Для проектирования зданий и сооружений ОДК
- 2) Для создания, внедрения и улучшения СМИБ
- 3) Для расчета заработной платы сотрудников
- 4) Для написания технической документации на продукцию

3. Что означает термин «риск-ориентированный подход», заложенный в современных стандартах ИБ?

- 1) Защищать нужно всё и любой ценой
- 2) Меры защиты выбираются исходя из финансовых возможностей компании, без учета угроз
- 3) Меры защиты выбираются и расставляются по приоритету в зависимости от величины рисков
- 4) Защита не нужна, если ничего не случилось раньше

Раздел 10. Обзор международных ИБ-стандартов

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Тема 10.1. Обзор международных ИБ-стандартов

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой международный стандарт содержит требования к системе менеджмента информационной безопасности (СМИБ) и используется для сертификации?

- 1) ISO 9001
- 2) ISO/IEC 27001
- 3) ISO 14001
- 4) OHSAS 18001

2. Какой стандарт является международным руководством по управлению рисками информационной безопасности?

- 1) ISO/IEC 27005
- 2) ISO 31000
- 3) ISO 22301
- 4) PCI DSS

3. Стандарт ISO/IEC 27002 (ГОСТ Р ИСО/МЭК 27002) в первую очередь описывает:

- 1) Методы криптографической защиты
- 2) Практические правила и меры по обеспечению информационной безопасности
- 3) Требования к аппаратному обеспечению

4) Порядок расследования киберпреступлений

8. Оценочные материалы промежуточной аттестации

5 семестр, Экзамен

Контролируемые ИДК: ОПК-2.3.1 ОПК-2.3.2 ОПК-2.3.3

Вопросы/Задания:

1. Что входит в понятие «федеральное законодательство и иные подзаконные акты»?
2. Что является источниками права в Российской Федерации?
3. Что представляет собой федеральный уровень законодательства?
4. Какова роль Конституции в иерархии нормативных правовых актов?
5. Что такое федеральные конституционные законы и в чём их особенность?
6. Какое место занимают международные договоры и соглашения РФ в правовой системе?
7. Что регулируют федеральные законы?
8. Какова юридическая сила актов Президента РФ?
9. Какова юридическая сила актов Правительства РФ?
10. Что такое ведомственные нормативные акты и кем они принимаются?
11. Что представляет собой региональный уровень законодательства?
12. Что такое конституции и уставы субъектов РФ?
13. Что регулируют законы субъектов РФ?
14. Какова роль постановлений Правительства Российской Федерации?
15. Какова роль указов Президента Российской Федерации?
16. Что такое отрасли права?
17. Кто является субъектами законодательной инициативы?
18. Каково основное содержание Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
19. Каково основное содержание Федерального закона от 21.07.1993 г. № 5485-1 «О государственной тайне»?

20. Каково основное содержание Федерального закона 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»?

21. Каково основное содержание Федерального закона № 390-ФЗ от 28.12.2010 г. «О безопасности»?

22. Каково основное содержание Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»?

23. Каково основное содержание Федерального закона № 184-ФЗ от 27.12.2002 г. «О техническом регулировании»?

24. Каково основное содержание Федерального закона от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»?

25. Каково основное содержание Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»?

26. Какова роль Международной организации по стандартизации (ИСО/ИСО) в разработке стандартов?

27. Чем занимается Международная электротехническая комиссия (МЭК/IEC)?

28. Какую роль играет Европейская экономическая комиссия ООН (ЕЭК ООН) в стандартизации?

29. Какова роль Продовольственной и сельскохозяйственной организации ООН (ФАО)?

30. Какое отношение Всемирная организация здравоохранения (ВОЗ) имеет к стандартизации?

31. Что такое Комиссия «Кодекс Алиментариус» и чем она занимается?

32. Что такое ГОСТ?

33. Что такое технический регламент?

34. В чём заключается сравнение основных концепций подтверждения соответствия?

35. Зачем нужны стандарты в области информационной безопасности (ИБ)?

36. Какие бывают виды (классификация) стандартов информационной безопасности?

37. Что представляет собой стандарт/методология COBIT?

38. Что представляют собой библиотеки ITIL и концепция ITSM?

39. Что представляет собой стандарт ISO 17799 (история и значение)?

40. Каковы основные принципы обеспечения информационной безопасности и меры обеспечения ИБ процедурного уровня?

41. Каковы основные факторы, влияющие на информационную безопасность предприятия, и как проводится аудит состояния ИБ согласно ISO 17799?

42. Какова сфера применения и средства контроля в стандарте ISO 17799?

43. Каковы преимущества и недостатки проведения аудита по требованиям стандарта ISO 17799?

44. Что представляет собой серия стандартов ISO/IEC 27000 (27XXX)?

45. Что представляют собой стандарты ISO/IEC 15408 («Общие критерии»)?

46. Что такое Канадские критерии оценки безопасности надежных компьютерных систем (СТСРЕС)?

47. Что такое Федеральные критерии оценки безопасности надежных компьютерных систем (FC) США?

48. Что представляют собой Единые критерии оценки безопасности информационных технологий (ISO/IEC 15408)?

49. Что представляет собой Общая методология оценки безопасности информационных технологий (СЕМ)?

50. Каковы перспективы практической реализации положений ISO/IEC 15408 и СЕМ-97/017?

51. Чем занимается Национальный институт стандартов и технологий США (NIST)?

52. Что представляют собой проекты SANS и CIS Top 20 (CIS Controls)?

53. Что представляет собой стандарт O-ISM3 (Open Information Security Management Maturity Model)?

54. Краткий обзор национальных стандартов в сфере ИБ, применяемых для задач проведения аудита

55. Обзор особенностей стандарта ГОСТ Р ИСО/МЭК 15408 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» в трех частях

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

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

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

59. Обзор особенностей стандарта ГОСТ Р 58142-2018 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045» в двух частях

60. Что представляет собой стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС)?

61. Как классифицируются стандарты по информационной безопасности в соответствии с их назначением?

62. Каков перечень и содержание национальных стандартов, разработанных ТК 362 и принятых Ростехрегулированием (Росстандартом)?

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://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
2. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"
3. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
4. <https://www.elibrary.ru/> - НЭБ eLIBRARY
5. <https://www.iprbookshop.ru/> - IPR BOOKS
6. <https://intuit.ru/> - Электронная образовательная среда "ИНТУИТ"

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

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 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.

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.