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: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
24 марта 2025 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) «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): 2025

Срок получения образования: 2 года

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

Москва, 2025

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

Фонд оценочных средств по дисциплине (модулю) составлен 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	14.10.2024, № 10-24

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

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

ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных

Уметь:

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

ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы

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/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

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/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.2/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/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации

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

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
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)	Повышенный	ИДК ПК-1.1 Разрабатывает профили защиты компьютерных систем Знать: ПК-1.1/Зн1 Теоретические основы угроз безопасности информации ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных Уметь: ПК-1.1/Ум1 Разрабатывать политики безопасности, основываясь на анализе потребностей организации и действующих угроз ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы Владеть: ПК-1.1/Нв1 Разрабатывать комплексные профили защиты для различных типов компьютерных систем, учитывая их специфику и назначение ИДК ПК-1.2 Формирует политики безопасности компьютерных систем и сетей Знать: ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) 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/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/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/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации 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
	Базовый	ИДК ПК-1.1 Разрабатывает профили защиты компьютерных систем Знать: ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных 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 ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы
	Базовый	ИДК 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 ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) Уметь: ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

		ПК-1.2/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
	Пороговый	ИДК ПК-1.1 Разрабатывает профили защиты компьютерных систем Знать: ПК-1.1/Зн1 Теоретические основы угроз безопасности информации ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных
	Пороговый	ИДК ПК-1.2 Формирует политики безопасности компьютерных систем и сетей Знать: ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) 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

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ПК-1.1 Разрабатывает профили защиты компьютерных систем ПК-1.1/Зн1 Теоретические основы угроз безопасности информации ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных ПК-1.1/Ум1 Разрабатывать политики безопасности, основываясь на анализе потребностей организации и действующих угроз ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы 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 ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) 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 ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/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 ПК-1.2/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации 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
Хорошо	ПК-1.1 Разрабатывает профили защиты компьютерных систем ПК-1.1/Зн1 Теоретические основы угроз безопасности информации ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных ПК-1.1/Ум1 Разрабатывать политики безопасности, основываясь на анализе потребностей организации и действующих угроз ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы ПК-1.2 Формирует политики безопасности компьютерных систем и сетей ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) 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 ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/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

Удовлетворительно	ПК-1.1 Разрабатывает профили защиты компьютерных систем ПК-1.1/Зн1 Теоретические основы угроз безопасности информации ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных ПК-1.2 Формирует политики безопасности компьютерных систем и сетей ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) 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
Неудовле-творительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Практическая работа Тестирование
Промежуточная аттестация	Зачет с оценкой

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Федеральное законодательство и иные подзаконные акты	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
2	Источники права	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
3	Федеральный уровень законодательства	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
4	Региональный уровень законодательства	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
5	Отрасли права	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
6	Федеральные законы	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
7	Международные организации по стандартизации	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
8	ГОСТы и технические регламенты	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
9	Организация информационной безопасности на основе применения международных и национальных стандартов	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
10	Обзор международных ИБ-стандартов	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой

11	Обзор национальных стандартов в сфере ИБ с целью их применения для задач проведения аудита ИБ	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой

5. 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.

Промежуточная аттестация по дисциплине проводится в форме «дифференцированный зачет». Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, в случае, если основное содержание освоено, но допущены отдельные неточности, не влияющие на общее понимание материала;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и дал полные, правильные и логически последовательные ответы; терминология применяется корректно, приведены необходимые обоснования и примеры, дополнительные вопросы раскрыты;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если

вопросы раскрыты правильно и достаточно полно, а отдельные неточности исправлены после уточняющих вопросов;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если основные положения раскрыты фрагментарно, имеются существенные неточности, однако базовое понимание продемонстрировано;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, вопросы не раскрыты либо допущены принципиальные ошибки, отсутствует владение базовой терминологией.

6. Оценочные материалы текущего контроля

Раздел 1. Федеральное законодательство и иные подзаконные акты
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 1.1. Федеральное законодательство и иные подзаконные акты

Форма контроля/оценочное средство: Практическая работа

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется установленная статьей 15 Конституции необходимость официального доведения закона до всеобщего сведения?

2. Какой вид закона принимается по вопросам, прямо предусмотренным Конституцией, большинством не менее трех четвертей от общего числа сенаторов РФ и двух третей от общего числа депутатов Государственной Думы?

Раздел 2. Источники права
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 2.1. Источники права

Форма контроля/оценочное средство: Практическая работа

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется сложившееся широко применяемое в предпринимательской или иной деятельности правило поведения, не предусмотренное законодательством?

2. Как в учебной классификации называют источник права, если речь идет о правосознании и правовых идеях?

Раздел 3. Федеральный уровень законодательства
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 3.1. Федеральный уровень законодательства

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Нормативные основания требования защиты

Для одного правила доступа к учебной системе найти закон и связанный с ним подзаконный акт. Указать точные положения, полномочия органов и пределы применения, затем исправить неточную нормативную ссылку в проекте политики.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Куда вносятся законопроекты в соответствии со статьей 104 Конституции РФ?

2. На какой территории обязательны указы и распоряжения Президента РФ по статье 90 Конституции?

Раздел 4. Региональный уровень законодательства
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 4.1. Региональный уровень законодательства

Форма контроля/оценочное средство: Практическая работа

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Вне пределов ведения РФ и совместного ведения кто обладает всей полнотой государственной власти по статье 73 Конституции?

2. В случае противоречия федерального закона и акта субъекта, изданного по вопросу собственного регулирования вне ведения РФ и совместного ведения, какой акт действует по части 6 статьи 76?

Раздел 5. Отрасли права
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 5.1. Отрасли права

Форма контроля/оценочное средство: Практическая работа

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется право внесения законопроектов в Государственную Думу, которым обладают перечисленные в статье 104 субъекты?

2. Чье заключение требуется для законопроекта об изменении финансовых обязательств государства по части 3 статьи 104 Конституции?

Раздел 6. Федеральные законы
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 6.1. Федеральные законы

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Политика обработки учебных персональных данных

Для сервиса записи на консультацию определить цель, необходимый состав данных, круг доступа и срок хранения. На основе заданных законных условий обработки подготовить краткий раздел политики и убрать избыточные поля формы

2. Установление режима коммерческой тайны

На учебном перечне документов отделить потенциально защищаемые сведения от сведений, которые нельзя относить к коммерческой тайне. Подготовить проект перечня, правила допуска и учета лиц, объяснить роль маркировки

3. Разграничение режимов информации

Для трех учебных наборов сведений определить применимый режим, правовое основание и возможные ограничения передачи. Указать, каких исходных данных не хватает для окончательного вывода, не присваивая грифы государственной тайны самостоятельно

4. Регламент обращения с электронной подписью

Разработать короткий порядок использования усиленной электронной подписи: защита ключа, проверка полученного документа, реакция на подозрение компрометации. Проверить порядок на выданных примерах действительного и измененного документа.

5. Правила защиты информационной системы

По описанию учебной базы заявок выделить неправомерное чтение, изменение и уничтожение данных. Для каждого воздействия подготовить простое правило защиты и

наблюдаемый результат проверки, включить их в проект политики

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется лицо, которое самостоятельно создало информацию либо получило на основании закона или договора право разрешать или ограничивать доступ к ней?

2. Как называется режим конфиденциальности информации, позволяющий ее обладателю при предусмотренных законом условиях сохранять положение на рынке и получать коммерческую выгоду?

3. Как называется временное прекращение обработки персональных данных, кроме случаев уточнения данных?

4. Каким мерам обеспечения безопасности отдан приоритет в статье 2 закона № 390-ФЗ?

Раздел 7. Международные организации по стандартизации

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 7.1. Международные организации по стандартизации

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Стандарт и технический регламент

Для выданных карточек продукции и документов определить область применения, обязательные требования и добровольно применяемые положения. Объяснить, какой документ дает основание требованию в каждом случае

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Является комиссия Codex Alimentarius межправительственным органом или частной компанией?

2. Как называется способ выработки стандартов ISO с учетом позиций заинтересованных сторон, противоположный одностороннему решению одного поставщика?

Раздел 8. ГОСТы и технические регламенты

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 8.1. ГОСТы и технические регламенты

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Стандарт и технический регламент

Для выданных карточек продукции и документов определить область применения, обязательные требования и добровольно применяемые положения. Объяснить, какой документ дает основание требованию в каждом случае

2. Проверка комплекта подтверждения соответствия

На учебном комплекте из декларации, обязательного и добровольного сертификатов проверить объект, срок, область и предусмотренную форму подтверждения. Отметить документы, не подтверждающие нужное требование, и сформулировать недостающие сведения

3. Реестр применяемых стандартов

Для трех документов, включая ГОСТ Р ИСО/МЭК 27001-2021, проверить официальные обозначения, статус, дату введения и изменения. Подготовить небольшой реестр с источниками проверки и назначить порядок его актуализации.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется прямое или косвенное определение соблюдения требований, предъявляемых к объекту?

2. Как называется лицо, которое принимает декларацию о соответствии либо обращается за сертификатом и получает его?

3. Как называется государственный информационный ресурс, содержащий документы и сведения о документах национальной системы стандартизации по статье 29 закона № 162-ФЗ?

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

Контролируемые ИДК: ПК-1.1 ПК-1.2

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

Форма контроля/оценочное средство: Практическая работа

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется слабость актива или меры защиты, которая может быть использована угрозой?

2. Кто должен установить политику информационной безопасности по пункту 5.2 ГОСТ Р ИСО/МЭК 27001-2021?

3. Как пункт 9.3 ГОСТ Р ИСО/МЭК 27001-2021 называет запланированное рассмотрение СМИБ высшим руководством для оценки ее приемлемости, адекватности и результативности?

Раздел 10. Обзор международных ИБ-стандартов

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 10.1. Обзор международных ИБ-стандартов

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Область и проблема безопасности профиля

Для учебного типа средств управления доступом определить границы объекта, защищаемые данные, две угрозы, одну политику организации и предположение о среде. Оформить начало профиля защиты без привязки к производителю

2. Цели и требования профиля защиты

Продолжить учебный профиль: связать каждую угрозу с целью безопасности, а цель — с функциональным требованием. Отдельно указать цель для среды и простое свидетельство, необходимое для доверия к реализации

3. Политика и область СМИБ

Для небольшой организации определить границы СМИБ, потребности заинтересованных сторон и ответственных. Подготовить политику с обязательствами выполнять применимые требования и улучшать СМИБ, показать связь с выявленными рисками

4. Обоснование набора мер защиты

Для учебной системы выбрать меры обработки двух заданных рисков и сопоставить их с приложением А ГОСТ Р ИСО/МЭК 27001-2021. Подготовить фрагмент ведомости применимости с обоснованием включения, состояния внедрения и исключения неприменимой меры

5. Применимость результатов оценки средства

По выданному учебному заданию по безопасности и описанию развертывания сравнить версию, конфигурацию, функции и предположения о среде. Указать, какие выводы оценки можно использовать и что требуется проверить дополнительно

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется операция Общих критериев, при которой из приведенного в компоненте перечня выделяют один или несколько пунктов?

2. Как называется операция Общих критериев, при которой один компонент используют для выражения нескольких отдельных требований?

3. Как называется риск, который сохраняется после выполнения предусмотренной обработки риска?

4. Как называется операция задания определенного параметра в компоненте или требовании Общих критериев?

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

Контролируемые ИДК: ПК-1.1 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: Практическая работа

Вопросы/Задания:

1. План внутреннего аудита ИБ

Составить краткий план аудита управления доступом: цель, область, критерии, участники, период и необходимые свидетельства. Учесть независимость аудитора и ограничения доступа к данным проверки

2. Получение проверяемых свидетельств

На учебном наборе настроек и журналов выбрать свидетельства выполнения одного правила доступа. Зафиксировать источник, время, относящуюся версию и способ проверки, отделить подтвержденные данные от предположений

3. Оформление несоответствия

Сопоставить заданное требование о пересмотре прав с учебными записями. Если требование не выполнено, оформить несоответствие с точной ссылкой и фактом; если данных недостаточно, указать дополнительный запрос

4. Корректирующее действие и проверка результата

Для выявленного несоответствия предложить устранение причины, ответственного и срок. Подготовить способ повторной проверки и описать, как ее результат влияет на изменение политики или процедуры

5. Отчет и ограничения аудита

Подготовить короткий отчет по выданным результатам проверки, указав область, использованные критерии, наблюдения и ограничения выборки. Определить состав получателей и исключить ненужные персональные данные из общей версии

6. Аудит согласованности профиля защиты

Проверить небольшой учебный профиль и относящиеся к нему настройки средства: наличие целей для заданных угроз, требований для целей и свидетельств их реализации. Исправить один разрыв связи и подготовить заключение с ограничениями

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется понятие, описывающее объем и границы аудита, включая охваченные процессы и период?

2. Как называется невыполнение требования, установленное при сопоставлении свидетельства с критерием?

3. Как называется аудит, который организация проводит у себя или от своего имени для внутренних целей?

4. Как называется совокупность мероприятий для проведения одного или нескольких аудитов за определенный период и для определенной цели?

7. Оценочные материалы промежуточной аттестации

3 семестр, Зачет с оценкой
Контролируемые ИДК: ПК-1.1 ПК-1.2
Вопросы/Задания:

1. Почему правовое основание политики ИБ следует связывать с конкретным положением, а не только с названием закона?

2. Как связаны прямое действие Конституции и локальные правила организации?

3. В чем состоит значение официального опубликования нормы для адресата?

4. Почему термин «источник права» может иметь несколько значений?

5. Как общественная потребность в защите данных связана с формальным источником права?

6. Почему ссылка на «так принято» недостаточна для подтверждения правового обычая?

7. Зачем при анализе ведомственного акта проверять компетенцию органа?

8. Как различаются принятие закона Государственной Думой и подписание Президентом?

9. Может ли название «регламент» само по себе показать юридическую силу документа?

10. Для чего разграничиваются ведение РФ и совместное ведение?

11. Что нужно выяснить прежде, чем сравнивать федеральную и региональную норму?

12. Какой основной акт действует в республике и какой в области?

13. Почему отрасль права нельзя определять только по слову «информация» в споре?

14. Чем обращение граждан с предложением отличается от законодательной инициативы?

15. Как ограничено право законодательной инициативы Конституционного Суда?

16. Чем обладатель информации отличается от любого лица, которому показали файл?

17. Почему один и тот же набор сведений требует проверки нескольких правовых оснований?

18. Как цель обработки ограничивает состав собираемых персональных данных?

19. Как предмет деятельности международной организации помогает выбрать стандарт?

20. Как национальные участники связаны с подготовкой международного стандарта?

21. Чем различается общее назначение ISO и IEC?

22. Почему обязательность конкретного положения нельзя установить только по обозначению «ГОСТ»?

23. Какие сведения об объекте важны для выбора процедуры подтверждения соответствия?

24. Что нужно фиксировать в реестре стандартов помимо названия?

25. Почему уязвимость и угроза — разные элементы анализа?

26. Как область СМИБ связана с внешними исполнителями?

27. Как совместно используют требования СМИБ, рекомендации по мерам и руководство по рискам?

28. Зачем в профиле защиты явно задавать границы объекта?

29. Зачем до сбора свидетельств определять критерии и область аудита?

30. Как отделить рекомендацию по улучшению от установленного несоответствия?