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.09 ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРАВОНАРУШЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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:
Преподаватель кафедры Информационно-измерительных систем
Деринг К. В.

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	Правовые основы защиты информации и виды правонарушений	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
2	Обнаружение признаков нарушения и первичная фиксация сведений	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
3	Сохранение цифровых следов и документирование действий	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
4	Организационные меры предупреждения нарушений и контроль доступа	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
5	Реагирование на инциденты и взаимодействие ответственных лиц	ПК-1.1 ПК-1.2	Практическая работа Тестирование	Зачет с оценкой
6	Разбор учебных ситуаций и подготовка предложений по профилактике	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, 1 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

6. Оценочные материалы текущего контроля

Раздел 1. Правовые основы защиты информации и виды правонарушений
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 1.1. Правовые основы защиты информации и виды правонарушений

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Границы правового и технического вывода

Для учебной геоинформационной системы сопоставьте три случая: отклоненный вход, подтвержденное изменение координат посторонней учетной записью и плановое изменение редактором. Отделите наблюдаемые факты от предположений, укажите охраняемые интересы и сведения, которых не хватает для правового вывода.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Укажите порядок первичного определения требований защиты: следующий шаг использует предыдущий.

А. Сформулировать требования защиты
Б. Выделить применимые ограничения и угрозы
В. Определить данные и назначение системы

2. Упорядочьте учебный правовой разбор; окончательная квалификация реального дела не выполняется.

А. Описать наблюдаемые действия и последствия
Б. Указать признаки, которые подтверждены, и сведения, которых не хватает
В. Найти относящиеся к ним положения закона

3. Упорядочьте формирование цели безопасности для угрозы изменения координат.

А. Описать возможное неразрешенное изменение
Б. Сформулировать цель предотвращения такого изменения
В. Определить защищаемый набор координат

4. Упорядочьте исправление предположения о контроле серверного помещения, если контроль не подтвержден.

А. Пересмотреть угрозы и требования по уточненным условиям
Б. Отметить неподтвержденное предположение
В. Уточнить фактические условия среды

Раздел 2. Обнаружение признаков нарушения и первичная фиксация сведений
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 2.1. Обнаружение признаков нарушения и первичная фиксация сведений

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Карточка первичного события

По учебной записи «29 сентября, 10:15, UTC+3; слой Здания; учетная запись reader; удаление объекта 17; отказ» заполните карточку события: источник, время, субъект, действие, объект, результат и недостающие сведения. Определите, кому передать карточку по предложенному внутреннему правилу.

2. Сопоставление времени событий

Сопоставьте записи одного учебного события: журнал приложения 12:00 UTC+3 и журнал шлюза 09:00 UTC. Сохраните исходные отметки, покажите общую шкалу времени и объясните, какие дополнительные сведения нужны для подтверждения связи записей.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Для учебной организации закон и локальное правило задают ограничения. Упорядочьте согласование политики.

А. Выявить применимое законодательное требование
Б. Устранить обнаруженное противоречие до утверждения правила
В. Сопоставить с ним локальное правило

2. Упорядочьте подготовку первичного внутреннего сообщения о замеченном событии; отправка использует собранные сведения.

А. Составить краткое сообщение с отделением фактов от предположений
Б. Передать сообщение по установленному внутреннему каналу
В. Зафиксировать наблюдение, время и источник

3. Два журнала используют разные часовые пояса. Укажите порядок их сопоставления.

А. Привести отображение времени к общей шкале
Б. Сохранить исходные отметки и сведения о часовых поясах
В. Построить хронологию с указанием неопределенности

4. Упорядочьте оценку уже полученного сообщения по учебному регламенту.

А. Зафиксировать решение о дальнейших действиях
Б. Зарегистрировать сообщение
В. Проверить относящиеся к нему сведения

5. Упорядочьте анализ записи об изменении слоя после получения копии журнала.

А. Сопоставить действие с действовавшим правилом доступа
Б. Определить субъект, объект, действие и результат
В. Описать подтвержденное несоответствие или отсутствие данных для вывода

Раздел 3. Сохранение цифровых следов и документирование действий

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 3.1. Сохранение цифровых следов и документирование действий

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Протокол получения учебной копии

На предоставленных преподавателем искусственных данных составьте протокол копирования журнала в выделенное защищенное хранилище. Укажите источник, полномочие, исполнителя, время, метод, имя копии, выполненную проверку читаемости и выявленные изменения или ошибки.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Полученная учебная копия журнала должна быть передана другому уполномоченному сотруднику. Укажите порядок.

А. Выполнить передачу по разрешенному каналу
Б. Зафиксировать прием, участников и время передачи
В. Идентифицировать передаваемый объект и проверить полномочия получателя

2. Упорядочьте разрешенную работу с заранее предоставленным учебным файлом.

А. Выполнить анализ копии и записать действия
Б. Сохранить исходный экземпляр от изменения
В. Подготовить отдельную рабочую копию

3. Составьте порядок документирования выполненной операции; запись результата появляется после операции.

А. Записать наблюдаемый результат и возникшие изменения
Б. Выполнить разрешенную операцию
В. Записать цель, основание и исходное состояние

Раздел 4. Организационные меры предупреждения нарушений и контроль доступа
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 4.1. Организационные меры предупреждения нарушений и контроль доступа

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Матрица доступа к геоданным

Для ролей наблюдатель, редактор и согласующий составьте матрицу чтения, изменения и разрешения публикации слоя. Наблюдатель только читает, редактор готовит изменения, согласующий разрешает публикацию; собственное изменение нельзя согласовать самому. Сформулируйте соответствующие требования профиля защиты.

2. Изменение прав при смене роли

Сотрудник перестал быть редактором и стал наблюдателем. Разработайте правило изменения доступа: событие запуска, согласование, отзыв старых прав, выдача необходимых прав, проверка и запись результата. Рассмотрите сохраненную активную сессию.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте выдачу доступа по учебной политике: изменение разрешено после согласования.

А. Проверить разрешенное и запрещенное действия
Б. Определить задачи и требуемые действия пользователя
В. Выдать права
Г. Получить согласование нужных прав

2. Упорядочьте подготовку политики безопасности после определения области ее применения.

А. Довести правила до исполнителей
Б. Сформулировать правила и обязанности
В. Согласовать и утвердить документ уполномоченным лицом

3. При переводе сотрудника новые права определяются новой ролью. Укажите порядок пересмотра.

А. Сопоставить действующие права с необходимыми
Б. Проверить результат
В. Получить подтвержденные сведения о новой роли
Г. Согласованно убрать лишние и добавить необходимые права

Раздел 5. Реагирование на инциденты и взаимодействие ответственных лиц
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 5.1. Реагирование на инциденты и взаимодействие ответственных лиц

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Порядок реагирования на изменение слоя

Для сообщения о неразрешенном изменении координат разработайте порядок оценки, ограничения воздействия, сохранения сведений, восстановления и проверки. Назначьте роли координатора, администратора и владельца данных; определите основания действий и фиксацию решений.

2. Уведомления при установленном инциденте

В условии установлено, что инцидент подпадает под часть 3.1 статьи 21 закона 152-ФЗ и выявлен 1 октября в 10:00. Определите предельные моменты двух уведомлений, состав первичных сведений и результатов расследования. Не заполняйте неизвестные причины вымышленными фактами.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В учебном регламенте техническое ограничение выполняется только после решения координатора. Укажите порядок.

А. Исполнитель выполняет меру и фиксирует результат
Б. Координатор согласует допустимую меру ограничения
В. Координатор оценивает подтвержденные сведения

2. Упорядочьте возврат учебной системы к обычной работе после локализации причины: запуск разрешен после проверки.

А. Проверить данные и требуемые функции защиты
Б. Получить разрешение на обычную эксплуатацию
В. Выполнить согласованное восстановление

3. Условия части 3.1 статьи 21 закона 152-ФЗ уже установлены. Упорядочьте два уведомления и проверку их оснований.

А. Зафиксировать момент выявления и исходные сведения инцидента
Б. Направить результаты внутреннего расследования в пределах 72 часов с того же момента
В. Направить первичное уведомление в пределах 24 часов с этого момента

Раздел 6. Разбор учебных ситуаций и подготовка предложений по профилактике

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 6.1. Разбор учебных ситуаций и подготовка предложений по профилактике

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Сборка учебного проекта профиля защиты

Для типовой геоинформационной системы объедините назначение, границы, проблему безопасности, цели, требования и их обоснование. Для угроз неразрешенного изменения и потери регистрационных записей покажите цепочки «угроза — цель — требование — проверка». Отметьте учебный статус и ограничения подтверждения.

2. Согласование политики и профиля защиты

Составьте политику для выбранного учебного объекта: доступ, регистрация, сохранение сведений и реагирование. Сопоставьте ее с профилем защиты. Если в одном документе наблюдателю запрещено изменение, а в другом оно разрешено всем сотрудникам, обоснуйте и внесите согласованную правку.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте обоснование одного требования учебного профиля защиты.

А. Сформулировать требование, реализующее цель
Б. Описать угрозу или обязательное правило
В. Указать соответствующую цель безопасности

2. После разбора учебного инцидента установлена причина, допускаемая старой политикой. Укажите порядок улучшения.

А. Подготовить изменение правила по выявленной причине
Б. Проверить выполнение обновленного правила
В. Согласовать и внедрить новую редакцию

3. Упорядочьте проверку связи требования с тестовым случаем.

А. Сопоставить факт с ожидаемым результатом
Б. Указать наблюдаемое условие выполнения требования
В. Выполнить проверку
Г. Подготовить входной случай и ожидаемый результат

7. Оценочные материалы промежуточной аттестации

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

1. Какие группы мер включает защита информации?

2. Для чего разрабатывают профиль защиты?

3. Почему технический инцидент нельзя автоматически назвать преступлением?

4. Чем угроза отличается от предположения о среде?

5. Когда в учебном случае нужно учитывать требования к персональным данным?

6. Что нужно записать о событии?

7. Зачем оценивать событие до выбора реакции?

8. Доказывает ли отказ входа успешное проникновение?

9. Как сопоставлять журналы с разными часовыми поясами?

10. Кому передавать сообщение о возможном нарушении?

11. Почему фиксируют метод и время получения копии?

12. Что содержит история хранения?

13. Почему изменчивые данные требуют отдельного решения?

14. Как оформлять неизвестное значение протокола?

15. Гарантирует ли технически корректная копия допустимость доказательства в суде?

16. Чем авторизация отличается от аутентификации?

17. Что означает минимальность привилегий?

18. Когда нужно пересматривать права сотрудника?

19. Почему журналы тоже нуждаются в защите?

20. Как проверить запрет изменения слоя?

21. Зачем заранее назначать роли реагирования?

22. От какого момента отсчитываются 24 и 72 часа в части 3.1 статьи 21 закона 152-ФЗ?

23. Что делать при неизвестном результате защитной команды?

24. Что проверяют после восстановления?

25. Почему при реагировании документируют решения?

26. Как связаны угроза, цель и требование?

27. Для чего нужен способ проверки требования?

28. Почему политика должна согласовываться с профилем защиты?

29. Что нужно зафиксировать при изменении политики?

30. Доказывает ли неделя без зарегистрированных инцидентов абсолютную защищенность?