



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.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.06 ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

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

Фонд оценочных средств по дисциплине (модулю) составлен 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

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

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики

Знать:

ОПК-10.1/Зн1 основные цели и задачи политики информационной безопасности как документа, регламентирующего стратегию и меры по защите информации в организации

Уметь:

ОПК-10.1/Ум1 анализировать требования организации и нормативных документов для формулировки целей и задач политики информационной безопасности

Владеть:

ОПК-10.1/Нв1 навыками разработки и документирования комплексной политики информационной безопасности с учетом современных стандартов и законодательства

ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности

Знать:

ОПК-10.2/Зн1 процессы и методы организации выполнения мер информационной безопасности на объекте защиты

Уметь:

ОПК-10.2/Ум1 организовывать работу по внедрению и сопровождению мер информационной безопасности в соответствии с утвержденной политикой и нормативными требованиями

Владеть:

ОПК-10.2/Нв1 методиками проведения контроля, аудита и мониторинга информационной безопасности в операционных системах

ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности

Знать:

ОПК-10.3/Зн1 основные компоненты и этапы процесса управления информационной безопасностью на объекте защиты

Уметь:

ОПК-10.3/Ум1 планировать и координировать выполнение комплекса мер по обеспечению информационной безопасности на объекте

Владеть:

ОПК-10.3/Нв1 навыками системного подхода к управлению процессами обеспечения информационной безопасности

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	Повышенный	ИДК ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики Знать: ОПК-10.1/Зн1 основные цели и задачи политики информационной безопасности как документа, регламентирующего стратегию и меры по защите информации в организации Уметь: ОПК-10.1/Ум1 анализировать требования организации и нормативных документов для формулировки целей и задач политики информационной безопасности Владеть: ОПК-10.1/Нв1 навыками разработки и документирования комплексной политики информационной безопасности с учетом современных стандартов и законодательства ИДК ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности Знать: ОПК-10.2/Зн1 процессы и методы организации выполнения мер информационной безопасности на объекте защиты Уметь: ОПК-10.2/Ум1 организовывать работу по внедрению и сопровождению мер информационной безопасности в соответствии с утвержденной политикой и нормативными требованиями Владеть: ОПК-10.2/Нв1 методиками проведения контроля, аудита и мониторинга информационной безопасности в операционных системах ИДК ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности Знать: ОПК-10.3/Зн1 основные компоненты и этапы процесса управления информационной безопасностью на объекте защиты Уметь: ОПК-10.3/Ум1 планировать и координировать выполнение комплекса мер по обеспечению информационной безопасности на объекте

	Владеть: ОПК-10.3/Нв1 навыками системного подхода к управлению процессами обеспечения информационной безопасности
Базовый	ИДК ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики Знать: ОПК-10.1/Зн1 основные цели и задачи политики информационной безопасности как документа, регламентирующего стратегию и меры по защите информации в организации Уметь: ОПК-10.1/Ум1 анализировать требования организации и нормативных документов для формулировки целей и задач политики информационной безопасности ИДК ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности Знать: ОПК-10.2/Зн1 процессы и методы организации выполнения мер информационной безопасности на объекте защиты Уметь: ОПК-10.2/Ум1 организовывать работу по внедрению и сопровождению мер информационной безопасности в соответствии с утвержденной политикой и нормативными требованиями ИДК ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности Знать: ОПК-10.3/Зн1 основные компоненты и этапы процесса управления информационной безопасностью на объекте защиты Уметь: ОПК-10.3/Ум1 планировать и координировать выполнение комплекса мер по обеспечению информационной безопасности на объекте

	Пороговый ИДК ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики Знать: ОПК-10.1/Зн1 основные цели и задачи политики информационной безопасности как документа, регламентирующего стратегию и меры по защите информации в организации ИДК ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности Знать: ОПК-10.2/Зн1 процессы и методы организации выполнения мер информационной безопасности на объекте защиты ИДК ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности Знать: ОПК-10.3/Зн1 основные компоненты и этапы процесса управления информационной безопасностью на объекте защиты
--	---

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Зачтено	ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики ОПК-10.1/Зн1 основные цели и задачи политики информационной безопасности как документа, регламентирующего стратегию и меры по защите информации в организации ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности ОПК-10.2/Зн1 процессы и методы организации выполнения мер информационной безопасности на объекте защиты ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности ОПК-10.3/Зн1 основные компоненты и этапы процесса управления информационной безопасностью на объекте защиты
Не зачтено	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
--------------	-----------------------------------

Текущий контроль	Тестирование
Промежуточная аттестация	Зачет

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Понятие «Организационной защиты информации»	ОПК-10.2 ОПК-10.3	Тестирование	Зачет
2	Организационные источники и каналы утечки. Силы, средства и условия организационной защиты информации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Тестирование	Зачет
3	Порядок подбора и текущая работа с персоналом. Организация допуска к различного рода информации и контроль ее сохранности	ОПК-10.1 ОПК-10.2 ОПК-10.3	Тестирование	Зачет
4	Аналитическая работа и контроль функционирования системы организационной защиты информации, как основа управления системой организационной защиты информации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Тестирование	Зачет

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, 7 семестр.

Зачет оценивается по следующей шкале:

- оценка «зачтено» 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; а также автоматически, когда обучающийся за промежуточную аттестацию имеет оценки «отлично»;
- оценка «не зачтено» выставляется обучающемуся в случае наличия грубых ошибок при изложении ответа на основные вопросы программы, свидетельствующих о неправильном понимании предмета; при решении практических задач показано незнание способов их

решения, материал изложен беспорядочно и неуверенно.

6. Оценочные материалы текущего контроля

Раздел 1. Понятие «Организационной защиты информации»

Контролируемые ИДК: ОПК-10.2 ОПК-10.3

Тема 1.13. Отчетно-учетные методы ограничения доступа к информации (каскадное моделирование отчетно-учетной системы организации)

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие три принципа составляют CIA-триаду?

1. Аутентичность, Достоверность, Надежность
2. Конфиденциальность, Целостность, Доступность
3. Шифрование, Аутентификация, Авторизация
4. Угрозы, Уязвимости, Риски
5. Защита, Контроль, Мониторинг

2. Какой стандарт является международным для систем управления информационной безопасностью?

1. ISO/IEC 27001
2. ГОСТ Р 57580
3. NIST SP 800-53
4. PCI DSS
5. GDPR

3. Какой закон РФ регулирует защиту персональных данных?

1. ФЗ-152
2. ФЗ-149
3. ФЗ-161
4. ФЗ-187
5. ФЗ-63

4. Что такое уязвимость в контексте информационной безопасности?

1. Действие злоумышленника
2. Слабое место в системе
3. Вид вредоносного ПО
4. Метод шифрования
5. Политика безопасности

5. Какой принцип предполагает минимально необходимые права доступа?

1. Разделение обязанностей
2. Минимальные привилегии
3. Экономическая целесообразность
4. Полная прозрачность
5. Коллективная ответственность

6. Какой этап управления рисками включает идентификацию активов?

1. Оценка угроз
2. Расчет рисков
3. Принятие риска
4. Мониторинг
5. Аудит

7. Какие методы используются для снижения рисков? (Выберите два)

1. Внедрение межсетевых экранов
2. Страхование киберрисков
3. Игнорирование угроз

4. Удаление резервных копий

5. Отключение антивирусов

8. Какой инструмент анализа рисков разработан NIST?

1. OCTAVE

2. NIST SP 800-30

3. FAIR

4. ISO 27005

5. COBIT

9. Какой метод оценки рисков основан на экспертных оценках?

1. Качественный

2. Количественный

3. Статистический

4. Вероятностный

5. Аналитический

10. Какой метод снижения рисков предполагает передачу ответственности страховой компании?

1. Избежание риска

2. Страхование

3. Принятие риска

4. Минимизация

5. Игнорирование

Раздел 2. Организационные источники и каналы утечки. Силы, средства и условия организационной защиты информации

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Тема 2.6. Особенность построения корпоративной безопасности в условиях экономического кризиса

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой этап построения СУИБ включает разработку политик?

1. Планирование

2. Внедрение

3. Эксплуатация

4. Аудит

5. Улучшение

2. Какие меры относятся к техническим контрмерам? (Выберите два)

1. Шифрование данных

2. Межсетевые экраны

3. Обучение сотрудников

4. Разработка регламентов

5. Страхование

3. Какой документ регламентирует правила использования паролей?

1. Политика информационной безопасности

2. План реагирования

3. Регламент резервного копирования

4. Договор с поставщиком

5. Инструкция пользователя

4. Какой этап жизненного цикла СУИБ включает мониторинг?

1. Планирование

2. Эксплуатация

3. Внедрение

4. Аудит

5. Улучшение

5. Что такое SOC?

1. Центр мониторинга безопасности
2. Система обнаружения вторжений
3. Программа шифрования
4. Стандарт безопасности
5. Метод оценки рисков

6. Какой метод шифрования использует один ключ?

1. Симметричное
2. Асимметричное
3. Хеширование
4. Электронная подпись
5. Квантовое

7. Какие функции обеспечивает электронная подпись? (Выберите два)

1. Аутентификацию
2. Целостность
3. Шифрование
4. Защиту от DDoS
5. Блокировку вирусов

8. Какой инструмент защищает сеть от несанкционированного доступа?

1. Межсетевой экран
2. Антивирус
3. VPN
4. SIEM
5. IDS

9. Что такое VPN?

1. Защищенное сетевое соединение
2. Система обнаружения атак
3. Метод шифрования
4. Средство резервного копирования
5. Инструмент аутентификации

10. Какой тип вредоносного ПО требует выкуп?

1. Ransomware
2. Троян
3. Червь
4. Spyware
5. Adware

Раздел 3. Порядок подбора и текущая работа с персоналом. Организация допуска к различного рода информации и контроль ее сохранности

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Тема 3.11. Утечка информации при использовании средств связи и различных проводных коммуникаций

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой этап инцидента включает сбор доказательств?

1. Подготовка
2. Расследование
3. Сдерживание
4. Ликвидация
5. Восстановление

2. Какие системы используются для мониторинга безопасности? (Выберите два)

1. SIEM
2. Антивирус
3. IDS/IPS
4. Фаервол
5. VPN

3. Какой документ определяет порядок действий при инциденте?

1. Политика паролей
2. План реагирования
3. Регламент копирования
4. Договор с поставщиком
5. Инструкция пользователя

4. Какой этап инцидента включает восстановление системы?

1. Обнаружение
2. Анализ
3. Восстановление
4. Документирование
5. Улучшение

5. Какие преимущества дает SOC?

1. Круглосуточный мониторинг
2. Автошифрование
3. Быстрое реагирование
4. Упрощение паролей
5. Отказ от антивирусов

6. Какой стандарт используется для сертификации СУИБ?

1. ISO/IEC 27001
2. PCI DSS
3. GDPR
4. NIST CSF
5. COBIT

7. Какие виды аудита существуют? (Выберите два)

1. Внутренний
2. Внешний
3. Автоматический
4. Случайный
5. Поверхностный

8. Какой стандарт регулирует безопасность платежных данных?

1. ISO 27001
2. PCI DSS
3. HIPAA
4. FSTEC
5. SOX

9. Какой этап аудита включает рекомендации?

1. Планирование
2. Сбор данных
3. Отчетность
4. Проверка
5. Сертификация

10. Что такое корректирующие действия?

1. Устранение несоответствий
2. Планирование аудита
3. Назначение ответственных
4. Разработка политик

5. Проведение тренингов

Раздел 4. Аналитическая работа и контроль функционирования системы организационной защиты информации, как основа управления системой организационной защиты информации

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Тема 4.5. "Дилерские" подходы

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие риски связаны с IoT?
 1. Недостаточная защита данных
 2. Увеличение скорости интернета
 3. Создание ботнетов
 4. Улучшение связи
 5. Снижение стоимости оборудования
2. Как ИИ применяется в информационной безопасности?
 1. Анализ аномалий трафика
 2. Уменьшение паролей
 3. Отказ от антивирусов
 4. Упрощение аудита
 5. Снижение стоимости оборудования
3. Какое влияние оказывает GDPR?
 1. Защита персональных данных ЕС
 2. Свободный обмен данными
 3. Отмена паролей
 4. Упрощение аудита
 5. Снижение требований к шифрованию
4. Что такое "угрозы нулевого дня"?
 1. Уязвимости без патчей
 2. Атаки в полночь
 3. Угрозы квантовых компьютеров
 4. Риски устаревшего оборудования
 5. Проблемы обновлений
5. Какие технологии относятся к перспективным?
 1. Квантовое шифрование
 2. Отказ от паролей
 3. Биометрическая аутентификация
 4. Упрощенное логирование
 5. Открытый доступ
6. Что такое "красная команда"?
 1. Разработчики антивирусов
 2. Специалисты по тестированию защиты
 3. Техподдержка
 4. Отдел продаж
 5. Аналитики логов
7. Какой метод эффективен против социальной инженерии?
 1. Увеличение длины паролей
 2. Обучение сотрудников
 3. Дополнительные серверы
 4. Отключение интернета
 5. Шифрование всех данных

8. Что проверяет тест на проникновение?

1. Уязвимости защиты
2. Скорость интернета
3. Качество бэкапов
4. Удобство интерфейса
5. Стоимость оборудования

9. Какой показатель измеряет эффективность защиты?

1. Количество сотрудников
2. Время реагирования
3. Стоимость оборудования
4. Количество паролей
5. Частота обновлений

10. Какой принцип реализует многофакторная аутентификация?

1. Открытый доступ
2. Усиленная проверка
3. Анонимность
4. Минимальные требования
5. Автоход

7. Оценочные материалы промежуточной аттестации

7 семестр, Зачет

Контролируемые ИДК: ОПК-10.1 ОПК-10.2 ОПК-10.3

Вопросы/Задания:

1. Принципы формирования (типы) организационных структур и регламентации их деятельности.

2. Линейно-функциональная организационная структура, принципы построения и функционирования. Место службы безопасности в ЛФОС.

3. Дивизиональная организационная структура, принципы построения и функционирования. Место службы безопасности в дивизиональной оргструктуре.

4. Особенности подчинения региональных структур службы безопасности в дивизиональных организациях. Модель матричного взаимодействия структурных подразделений.

5. Матричная организационная структура, принципы построения и функционирования. Понятия «слабой» и «сильной» матрицы. Подчинение по отдельным вопросам работы. Проектная матрица.

6. Процессная организационная структура, принципы построения и функционирования. Модель работы СБ в процессных структурах.

7. Функции, задачи и структура службы безопасности предприятия

8. Создание концепции безопасности на примере финансовой организации (банка)

9. Проектирование структуры службы безопасности

10. Функции, задачи и особенности деятельности подразделений службы безопасности
11. Создание службы информационной безопасности, организационная структура и основные функции
12. Служба безопасности объекта. Типовая структура службы безопасности.
13. Организация пропускного и внутри объектового режимов.
14. Общие принципы внутренней регламентации
15. Объекты и субъекты обеспечения безопасности
16. Внешняя регламентация деятельности по ЗИ (федеральное законодательство)
17. Стандартизация процессного описания
18. Стандарт описания IDEF, его значение в области международной и российской практики управленческой стандартизации
19. Отчетно-учетные методы ограничения доступа к информации (каскадное моделирование отчетно-учетной системы организации)
20. Каналы утечки информации
21. Причины утечки информации
22. Контроль исполнения документов
23. Технологические процедуры контроля исполнения документов
24. Технологические системы защиты и обработки конфиденциальных документов
25. Общая логика процесса защищенного документооборота
26. Задачи построения системы корпоративной безопасности
27. Основные виды угроз интересам компании
28. Организация и функционирование системы безопасности компании
29. Средства обеспечения безопасности
30. Подсистемы системы безопасности компании
31. Способы и особенности функционирования Служб безопасности организаций
32. Проверка работы Службы безопасности

33. Подготовка к созданию системы безопасности компании
34. Особенности построения корпоративной безопасности в условиях экономического кризиса
35. Информация, представляющая интерес при сборе и анализе сведений
36. Классификация угроз безопасности информации
37. Угрозы, не связанные с деятельностью человека
38. Угрозы, связанные с деятельностью человека
39. Порядок подбора и увольнения персонала, роль Службы безопасности в этом процессе
40. Управление в чрезвычайных ситуациях
41. Утечка акустической информации из-за применения подслушивающих устройств
42. Пути утечки информации в вычислительных системах
43. Утечка информации за счет побочных электромагнитные излучения и наводки (ПЭМИН)
44. Утечка информации при использовании средств связи и различных проводных коммуникаций
45. Корпоративная (конкурентная) разведка и промышленный шпионаж, сущность и отличия
46. Закрытые и открытые источники в конкурентной разведке
47. Рекрутинг, как средство конкурентной разведки
48. Тайное физическое проникновение
49. "Дилерские" подходы