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

Факультет оптического приборостроения
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
Протокол от 31 мая 2021 г. № 34

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) «Б1.О.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Уровень высшего образования: специалитет

Специальность: 12.05.01 Электронные и оптико-электронные приборы и системы специального назначения

Направленность (профиль) подготовки: Электронные и оптико-электронные приборы и системы дистанционного зондирования Земли

Квалификация (степень) выпускника: инженер

Форма обучения: очная

Год набора (приема на обучение): 2021

Срок получения образования: 5 лет 6 месяца(-ев)

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

Москва, 2021

Разработчики:
Старший преподаватель кафедры
Информационно-измерительных систем Бондарев И. Н.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по специальности 12.05.01 Электронные и оптико-электронные приборы и системы специального назначения, утвержденного приказом Минобрнауки от 09.08.2018 № 93

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Оптического приборостроения	Председатель ученого совета факультета	Торшина И. П.	Рассмотрено	09.04.2021, № 4

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

ОПК-2 Учет факторов внешней среды

ОПК-2.3 Осуществляет профессиональную деятельность с учетом интеллектуально правовых ограничений на всех этапах жизненного цикла технических систем и процессов.

Знать:

ОПК-2.3/Зн1 Основные правовые и государствоведческие понятия, необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей публичного права (конституционного, уголовного, административного), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей частного права (гражданского, семейного, трудового), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов

Уметь:

ОПК-2.3/Ум1 Использует правовые знания в ходе профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов

Владеть:

ОПК-2.3/Нв1 Осуществляет профессиональную деятельность с учетом предписаний законодательства и положений правоприменительной практики на всех этапах жизненного цикла технических систем и процессов

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)

ОПК-2 Учет факторов внешней среды	Повышенный	ИДК ОПК-2.3 Осуществляет профессиональную деятельность с учетом интеллектуально правовых ограничений на всех этапах жизненного цикла технических систем и процессов. Знать: ОПК-2.3/Зн1 Основные правовые и государствоведческие понятия, необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей публичного права (конституционного, уголовного, административного), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей частного права (гражданского, семейного, трудового), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов Уметь: ОПК-2.3/Ум1 Использует правовые знания в ходе профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов Владеть: ОПК-2.3/Нв1 Осуществляет профессиональную деятельность с учетом предписаний законодательства и положений правоприменительной практики на всех этапах жизненного цикла технических систем и процессов
	Базовый	ИДК ОПК-2.3 Осуществляет профессиональную деятельность с учетом интеллектуально правовых ограничений на всех этапах жизненного цикла технических систем и процессов. Знать: ОПК-2.3/Зн1 Основные правовые и государствоведческие понятия, необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей публичного права (конституционного, уголовного, административного), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей частного права (гражданского, семейного, трудового), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов Уметь: ОПК-2.3/Ум1 Использует правовые знания в ходе профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов

	Пороговый	ИДК ОПК-2.3 Осуществляет профессиональную деятельность с учетом интеллектуально правовых ограничений на всех этапах жизненного цикла технических систем и процессов. Знать: ОПК-2.3/Зн1 Основные правовые и государствоведческие понятия, необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей публичного права (конституционного, уголовного, административного), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей частного права (гражданского, семейного, трудового), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Зачтено	ОПК-2.3 Осуществляет профессиональную деятельность с учетом интеллектуально правовых ограничений на всех этапах жизненного цикла технических систем и процессов. ОПК-2.3/Зн1 Основные правовые и государствоведческие понятия, необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей публичного права (конституционного, уголовного, административного), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов - основные положения отраслей частного права (гражданского, семейного, трудового), необходимые в профессиональной деятельности на всех этапах жизненного цикла технических систем и процессов
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	Контрольная работа Зачет

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Информационная безопасность в системе национальной безопасности Российской Федерации	ОПК-2.3	Тестирование	Зачет

2	Информационная война, методы и средства ее ведения	ОПК-2.3	Тестирование	Зачет
3	Обеспечения информационной безопасности компьютерных систем	ОПК-2.3	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, 1 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. Информационная безопасность в системе национальной безопасности Российской Федерации

Контролируемые ИДК: ОПК-2.3

Тема 1.3. Основные понятия и общеметодологические принципы теории информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое аутентификация?

1) Проверка полномочий пользователя
2) Подтверждение личности
3) Выдача прав доступа
4) Шифрование данных

2. Какие механизмы могут использоваться при многофакторной аутентификации?

1) Пароль
2) Смарт карта

3) Биометрия
4) TTL

3. Что такое политика управления доступом?

1) Набор правил, определяющих, кто имеет право на доступ к определенным ресурсам (например, данным, приложениям, системам) и какие действия они могут выполнять с этими ресурсами
2) Временная блокировка аккаунта
3) Автоматизация обновлений
4) VPN требования

4. Какие модели контроля доступа существуют?

1) DAC
2) MAC
3) RBAC
4) TLS

5. Какие этапы управления рисками?

1) Идентификация
2) Анализ
3) Обработка
4) Сжатие

6. Что описывает модель нарушителя?

1) Протоколы
2) Кто может атаковать и какими способами
3) Сетевую топологию
4) Архитектуру ОС

7. Модель угроз включает элементы:

1) Уязвимости
2) Атакующие
3) Последствия
4) CPU

8. Что означает СКУД?

1) Система контроля управления данными
2) Система контроля и управления доступом
3) Система камерами USB
4) Система криптографической защиты

Тема 1.4. Понятие и виды защищаемой информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что делает маскирование данных?

1) Удаляет данные
2) Замещает реальные значения
3) Шифрует диски
4) Сравнивает базы

2. Где применяют маскирование?

1) Тестовые среды
2) Отчёты
3) Аналитика
4) OpenVPN

Раздел 2. Информационная война, методы и средства ее ведения

Контролируемые ИДК: ОПК-2.3

Тема 2.1. Понятие и виды угроз информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие признаки фишинга?

1) Поддельный URL
2) Ошибки в тексте
3) Срочность
4) TLS-сертификат

2. Для обучения персонала распространено использование _____ писем. (Ответ предоставить одним словом с заглавной буквы)

Тема 2.2. Информационная безопасность и информационное противоборство

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое антифрод система?

1) Антивирус
2) Система борьбы с мошенничеством
3) VPN шлюз
4) Учёт расходов

2. Какие показатели анализируются антифродом?

1) Геоданные
2) Частота транзакций
3) Устройства
4) Видео поток

Тема 2.3. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что делает WAF?

1) Шифрует HTTP
2) Фильтрует веб трафик
3) Управляет DNS
4) Контролирует файлы

2. Какие защитные функции есть у Anti DDoS?

1) Rate limiting
2) Geo блокировка
3) Маскировка IP
4) Backup

3. WAF защищает от _____ атак. (Ответ предоставить одним словом латинскими буквами начиная с заглавной буквы)

Раздел 3. Обеспечения информационной безопасности компьютерных систем

Контролируемые ИДК: ОПК-2.3

Тема 3.1. Методы и средства обеспечения информационной безопасности компьютерных систем

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое полное резервное копирование?

1) Копирование всех данных независимо от изменений
2) Копирование только изменённых файлов
3) Копирование только новых файлов
4) Копирование только метаданных

2. Какие бывают типы бэкапа?

1) Полный
2) Инкрементный
3) Дифференциальный
4) Вертикальный

3. Стратегия «3-2-1» означает три копии, на двух разных носителях и одну копию _____. (Ответ предоставить одним словом с заглавной буквы)

4. Что обнаруживает антивирус?

1) Незащищённые порты
2) Вредоносные файлы
3) Уязвимости ОС
4) Атаки по сети

5. Какие функции выполняет антивирус?

1) Сканирование файлов
2) Обнаружение сигнатур
3) Песочница
4) Присвоение прав

6. Антивирус защищает систему, прежде всего, от _____. (Ответ предоставить одним словом с заглавной буквы)

7. Что делает традиционный межсетевой экран?

1) Шифрует данные
2) Контролирует трафик по IP/портам
3) Обнаруживает уязвимости
4) Управляет паролями

8. Какие функции характерны для NGFW?

1) DPI
2) Интеграция с IDS
3) Контроль приложений
4) VPN сессии

9. Что такое контейнер?

1) Виртуальная машина
2) Изолированный процесс с зависимостями
3) Физический сервер
4) Сетевой шлюз

10. Какие из технологий относятся к виртуализации?

1) Hyper V
2) VMware
3) Docker
4) OpenSSL

11. Контейнер обеспечивает _____ на уровне процесса. (Ответ предоставить одним словом с заглавной буквы)

12. Что делает сканер уязвимостей?

1) Шифрует трафик
2) Ищет известные уязвимости
3) Управляет правами
4) Резервирует данные

13. Что делает DLP?

1) Шифрует диск

2) Предотвращает утечку данных
3) Сканирует на вирусы
4) Контролирует доступ

14. Какие способы внедрения DLP применяют?

1) На уровне сети
2) На конечных точках
3) В облаке
4) Только на серверах

15. Что делает VPN?

1) Увеличивает скорость
2) Шифрует соединение
3) Ускоряет Wi Fi
4) Сравнивает IP

16. Какие режимы корпоративного VPN?

1) Site to Site
2) Remote Access
3) SSL VPN
4) DNS VPN

17. VPN обеспечивает _____ соединение. (Ответ предоставить одним словом с заглавной буквы)

18. Что делает MDM?

1) Управляет антивирусом
2) Контролирует мобильные устройства
3) Администрирует DNS
4) Шифрует файлы

19. MDM обеспечивает _____ мобильных устройств. (Ответ предоставить одним словом с заглавной буквы)

20. Что делает IDS?

1) Блокирует трафик
2) Обнаруживает атаки
3) Шифрует каналы
4) Удаляет лог

Тема 3.2. Механизмы защиты информации в автоматизированных системах

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что делает PAM?

1) Хранит логи
2) Управляет правами суперпользователей
3) Отключает аккаунты
4) Выполняет шифрование

2. Какие функции PIM/PAM выполняют?

1) Ротация паролей
2) Управление сессиями
3) Удалённый доступ
4) Антивирус

3. Что делает SPF?

1) Шифрует письмо
2) Проверяет, разрешено ли отправителю направлять письма от имени домена
3) Сканирует вложения
4) Аннулирует письмо

4. SPF, DKIM, DMARC – это механизмы?

1) Аутентификации почтовых доменов
2) Защиты от спуфинга
3) Улучшения доставки
4) Мониторинга трафика

Тема 3.5. Методы и критерии оценки защищенности компьютерных систем

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое pen test?

1) Аудит соответствия
2) Тестирование на проникновение
3) Установка патчей
4) Мониторинг трафика

2. Какие этапы pen test?

1) Разведка
2) Эксплуатирование
3) Отчётность
4) Управление паролями

3. Кто выполняет атакующие действия в тестах безопасности?

1) Blue Team
2) Red Team
3) SOC
4) Yellow Team

4. Какие функции выполняет Blue Team?

1) Обнаружение
2) Реагирование
3) Мониторинг
4) Exploit

Тема 3.7. Защита информации, обрабатываемой в автоматизированных системах от технических разведок

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Первый этап в обработке инцидента – это:

1) Устранение ущерба
2) Обнаружение
3) Уничтожение угрозы
4) Отчёт

2. Какие инструменты используются для реагирования на события и инциденты ИБ?

1) SIEM
2) EDR
3) Forensic
4) DHCP

3. Что такое SIEM?

1) Антивирус
2) Система корреляции событий
3) Межсетевой экран
4) Мониторинг производительности

4. Какие модули есть в SIEM?

1) Сбор логов
2) Корреляция
3) Уведомления

4) DNS-рекрутинг

5. SIEM собирает и анализирует _____. (Ответ предоставить одним словом с заглавной буквы)

6. Что такое Security Awareness?

1) Антивирус
2) Обучение пользователей безопасности
3) Фаервол
4) Backup

7. Что такое OSINT?

1) Шифрование данных
2) Сбор информации из открытых источников
3) Анализ логов
4) Обеспечение защиты от вирусов

8. К инструментам OSINT относятся?

1) Shodan
2) Maltego
3) Google Dorks
4) Hyper-V

9. Чем занимается SOC?

1) Обновляет ОС
2) Отслеживает события, инциденты ИБ и реагирует на них
3) Резервирует данные
4) Ведёт бухгалтерию

10. Какие источники данных используют в SOC?

1) Логи
2) Сетевой трафик
3) События EDR
4) PowerShell

11. Что такое SAST?

1) Динамический тест
2) Статический анализ кода
3) Контейнеризация
4) Мониторинг

12. Какие инструменты относятся к DAST и IAST?

1) OWASP ZAP
2) Burp Suite
3) Veracode
4) Hypervisor

13. Отличие DevSecOps от DevOps — это:

1) Добавление тестов
2) Интеграция безопасности в CI/CD
3) Использование VPN
4) Изоляция контейнеров

14. Какие инструменты применяются в DevSecOps?

1) SAST
2) DAST
3) IaC анализаторы
4) SSH

15. Какие элементы включает СКУД + видеонаблюдение?

1) Считыватели
2) Камеры
3) Сервер записи

4) Документы

7. Оценочные материалы промежуточной аттестации

1 семестр, Зачет
Контролируемые ИДК: ОПК-2.3
Вопросы/Задания:

1. Дайте определения терминам «Информация», «Информационные технологии», «Информационная система», «Информационная безопасность».

2. Основные свойства информации, триада CIA.

3. Основные руководящие документы и регуляторы в сфере информационной безопасности.

4. Доктрина информационной безопасности: цели документа, национальные интересы рассматриваемые доктриной ИБ.

5. Доктрина информационной безопасности: основные угрозы ИБ, направления обеспечения ИБ.

6. Идентификация, аутентификация. Дайте определения терминам. Что такое факторы аутентификации? Примеры.

7. Авторизация и контроль доступа. Дайте определения терминам. Какие задачи решает контроль доступа?

8. Авторизация и контроль доступа. Что такое «Песочница»? Применение списков контроля доступа (ACL). Плюсы и минусы использования ACL.

9. Основные модели доступа. Схема и применение Дискреционного контроля доступа.

10. Основные модели доступа. Схема и применение Мандатного контроля доступа.

11. Основные модели доступа. Схема и применение Контроля доступа на основе ролей.

12. Многоуровневые модели доступа. Какие многоуровневые модели доступа Вы знаете? Какие цели они решают?

13. Виртуализация и контейнеризация: технологии изоляции и защиты данных. Инструменты.

14. Модель OSI. Что из себя представляет модель OSI? Назовите уровни модели OSI и как они применяются.

15. Дайте определение «Стек», «Стек протоколов TCP\IP». Разница между стеком TCP\IP и моделью OSI.

16. Алгоритм работы стека TCP\IP. Назовите уровни стека TCP\IP.

17. Угрозы сетевой безопасности. Дайте определение «Сетевые атаки». Классификация сетевых угроз.

18. Виды сетевых атак. Какие разновидность сетевых атак Вы знаете? Сниффинг, Спуффинг. Отказ в обслуживании (распределенный отказ в обслуживании).

19. Механизмы защиты информационных систем. Что такое «Пакетные фильтр», «Межсетевой экран», «WAF»? Плюсы и минусы. Защиту от каких угроз обеспечивают.

20. Механизмы защиты информационных систем. Системы IDS и IPS. Особенности работы. Способы применения.

21. Механизмы защиты информационных систем. SIEM и DLP. Использование и принцип работы.

22. Мониторинг информационных систем. Для чего нужен? Следствием какого механизма является мониторинг? Привлечение к ответственности. Методы привлечения к ответственности.

23. Управление инцидентами информационной безопасности: процесс и инструменты.

24. Процесс по управлению уязвимостями (vulnerability management). Сканер уязвимостей.

25. Тестирование на проникновение (Pentest). Инструменты.

26. Управление рисками информационной безопасности. Определение и назначение использования.

27. Введение аудита ИС. Способы введения аудита.

28. Определение SOC. Функции SOC. Инструменты. Уровни SOC.

29. Виды информационных систем. Определение «ИСПДн». Категории ПДн.

30. Виды информационных систем. Автоматизированные системы, Государственные информационные системы.

31. Маскирование конфиденциальной информации (данных). Принцип, способы, назначение применения. Инструменты.

32. ХЭШ. Определение «ХЭШ». Механизм работы ХЭШ функции. Коллизии в Хэш-функциях.

33. Основы криптографии. Определение, Понятия, Шифр Цезаря, Шифр Виженера.

34. Основы криптографии. Определение, Понятия, Шифр Вернама, роль и применение криптографии в кибербезопасности.

35. Симметричное и ассиметриченое шифрование. Инфраструктура открытых ключей.