



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
17 февраля 2023 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Б1.О.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 12.03.02 Оптотехника

Направленность(профиль) подготовки: Оптико-электронные приборы и системы

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2023

Срок получения образования: 4 года

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

Москва, 2023

Разработчики:

Старший преподаватель кафедры

Информационно-измерительных систем Бондарев И. Н.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 12.03.02 Опотехника, утвержденного приказом Минобрнауки от 19.02.0017 № 948

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Оптического приборостроения	Председатель ученого совета факультета	Торшина И. П.	Рассмотрено	01.12.2022, № 1

Содержание

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

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - приобретение обучающимися знаний в области информационной безопасности, характеризующихся созданием терминологического фундамента и ознакомлением с общими методами и подходами обеспечения информационной безопасности.

Задачи изучения дисциплины:

- рассмотрение основных методик и подходов обеспечения информационной безопасности в рамках современных автоматизированных систем;
- изучение принципов построения защищенных информационных систем и поддержания подсистемы защиты информации в актуальном состоянии;
- рассмотрение особенностей реализации общих методик защиты информации на различных платформах.

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

Компетенции, индикаторы и результаты обучения

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

УК-1.1 Анализирует задачу, выделяя ее базовые составляющие

Знать:

УК-1.1/Зн2 Основные области и специфика применения оптоэлектроники, оптических и оптико-электронных приборов и комплексов

Уметь:

УК-1.1/Ум1 Работать с научно-технической информацией

Владеть:

УК-1.1/Нв1 Системным анализом

УК-1.1/Нв3 Правилами и принципами анализа информации и текстов

УК-1.2 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов

Знать:

УК-1.2/Зн5 Методы проведения патентных исследований

Уметь:

УК-1.2/Ум1 Применять справочные материалы

УК-1.2/Ум5 Производить патентный поиск

УК-1.2/Ум6 Работать с научно-технической информацией.

Владеть:

УК-1.2/Нв1 Методами поиска информации в базах данных и интернет-ресурсах

УК-1.3 При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы, в том числе с применением философского понятийного аппарата

Знать:

УК-1.3/Зн3 Основы философского понятийного аппарата, применимые при анализе информации

Уметь:

УК-1.3/Ум3 Отличать факты от мнений, интерпретаций и оценок

УК-1.3/Ум4 Формировать собственные мнения и суждения

Владеть:

УК-1.3/Нв1 Методами поиска информации в базах данных и интернет-ресурсах

УК-1.4 Осуществляет поиск, сбор и обработку информации для решения поставленной задачи

Знать:

УК-1.4/Зн1 Критерии оценки результатов интеллектуальной деятельности

Уметь:

УК-1.4/Ум3 Применять справочные материалы, искать патентную и научно-техническую информацию

Владеть:

УК-1.4/Нв3 Методами поиска информации в базах данных и интернетресурсах

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.04 «Основы информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 1.

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

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лабораторные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
1 семестр	108	3	17	17	74	Зачет
Всего	108	3	17	17	74	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лабораторные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соответствующие результатам освоения программы
Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации	28	4	4	20	УК-1.1 УК-1.2 УК-1.3 УК-1.4

Тема 1.1. Национальная безопасность Российской Федерации	7	1	1	5	
Тема 1.2. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	7	1	1	5	
Тема 1.3. Основные понятия и общеметодологические принципы теории информационной безопасности	7	1	1	5	
Тема 1.4. Понятие и виды защищаемой информации	7	1	1	5	
Раздел 2. Информационная война, методы и средства ее ведения	22	3	3	16	УК-1.1 УК-1.2 УК-1.3 УК-1.4
Тема 2.1. Понятие и виды угроз информационной безопасности	7	1	1	5	
Тема 2.2. Информационная безопасность и информационное противоборство	8	1	1	6	
Тема 2.3. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны	7	1	1	5	
Раздел 3. Обеспечения информационной безопасности компьютерных систем	58	10	10	38	УК-1.1 УК-1.2 УК-1.3 УК-1.4
Тема 3.1. Методы и средства обеспечения информационной безопасности компьютерных систем	7	1	1	5	
Тема 3.2. Механизмы защиты информации в автоматизированных системах	10	2	2	6	
Тема 3.3. Формальные модели безопасности автоматизированных систем	10	2	2	6	
Тема 3.4. Особенности дискреционной и мандатной модели безопасности	7	1	1	5	
Тема 3.5. Методы и критерии оценки защищенности компьютерных систем	7	1	1	5	
Тема 3.6. Руководящие документы ФСТЭК России (Гостехкомиссии)	7	1	1	5	

Тема 3.7. Защита информации, обрабатываемой в автоматизированных системах от технических разведок	10	2	2	6
Итого	108	17	17	74

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Тема 1.1. Национальная безопасность Российской Федерации

Понятие национальной безопасности и ее значение для государства. Роль информационной безопасности как составляющей национальной безопасности. Основные угрозы национальной безопасности в информационной сфере. Виды безопасности в различных сферах жизнедеятельности личности, общества и государства.

Тема 1.2. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере

Государственная политика в области информационной безопасности. Основные направления и задачи обеспечения информационной безопасности на государственном уровне. Современные угрозы безопасности в информационной сфере: кибератаки, утечки информации, информационные войны. Проблемы региональной информационной безопасности.

Тема 1.3. Основные понятия и общеметодологические принципы теории информационной безопасности

Понятие информационной безопасности, объекты и субъекты защиты. Принципы конфиденциальности, целостности и доступности информации. Методологические основы анализа угроз и построения систем защиты. Основные понятия информационной безопасности.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.4. Понятие и виды защищаемой информации

Классификация информации по степени секретности: открытая, конфиденциальная, государственная тайна. Виды информации, требующей защиты: персональные данные, коммерческая тайна, государственная тайна. Виды защищаемой информации и защита интеллектуальной собственности.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Информационная война, методы и средства ее ведения

Тема 2.1. Понятие и виды угроз информационной безопасности

Определение информационных угроз. Виды угроз: несанкционированный доступ, утечка, искажение, уничтожение информации. Источники угроз: внешние и внутренние нарушители, технические и программные средства. Угрозы информационной безопасности Российской Федерации в различных сферах.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.2. Информационная безопасность и информационное противоборство

Понятие информационного противоборства как части информационной безопасности. Методы и средства информационного воздействия и защиты. Роль информационных технологий в современных конфликтах. Методы информационного противоборства и применение информационного оружия.

Текущий контроль

Вид (форма) контроля
Тестирование

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

Особенности защиты информации в условиях информационной войны. Меры по обеспечению устойчивости государственных информационных систем. Организационные и технические подходы к противодействию информационным атакам. Компьютерная система как объект информационной войны.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 3. Обеспечения информационной безопасности компьютерных систем

Тема 3.1. Методы и средства обеспечения информационной безопасности компьютерных систем

Технологии защиты информации: криптография, контроль доступа, антивирусные средства. Методы аутентификации и идентификации пользователей. Программно-аппаратные средства обеспечения информационной безопасности.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.2. Механизмы защиты информации в автоматизированных системах

Основные механизмы: разграничение доступа, шифрование, электронная цифровая подпись. Средства контроля целостности и конфиденциальности данных. Принципы построения защищенных автоматизированных систем. Механизмы защиты информации компьютерных систем.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.3. Формальные модели безопасности автоматизированных систем

Модели безопасности: дискреционная, мандатная, ролевые модели. Формализация правил доступа и управления правами пользователей. Применение моделей для оценки и построения систем безопасности.

Тема 3.4. Особенности дискреционной и мандатной модели безопасности

Дискреционная модель: управление доступом на основе прав владельца информации. Мандатная модель: управление доступом на основе уровней секретности и политик безопасности. Сравнительный анализ и области применения моделей.

Тема 3.5. Методы и критерии оценки защищенности компьютерных систем

Критерии оценки безопасности: конфиденциальность, целостность, доступность. Методы тестирования и аудита систем безопасности. Стандарты и классификация уровней защищенности.

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 3.6. Руководящие документы ФСТЭК России (Гостехкомиссии)

Основные нормативные акты и стандарты ФСТЭК по информационной безопасности. Требования к защите информации в государственных и коммерческих системах. Процедуры сертификации и аттестации средств защиты информации. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

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

Методы защиты от технической разведки: экранирование, помехозащита, контроль доступа. Организационные и технические меры предотвращения утечек информации. Особенности защиты в условиях современных технических угроз. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.

Текущий контроль
Вид (форма) контроля
Тестирование

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: 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.

7. Оценочные материалы текущего контроля

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Контролируемые ИДК: УК-1.1 УК-1.2 УК-1.3 УК-1.4

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: УК-1.1 УК-1.2 УК-1.3 УК-1.4

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) Гео 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: УК-1.1 УК-1.2 УК-1.3 УК-1.4

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

8. Оценочные материалы промежуточной аттестации

1 семестр, Зачет

Контролируемые ИДК: УК-1.1 УК-1.2 УК-1.3 УК-1.4

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 разновидности 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 асимметричное шифрование. Инфраструктура открытых ключей.

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Мызникова Т. А. Основы информационной безопасности: учебное пособие / Т. А. Мызникова. - Омск: ОмГУПС, 2017. - 82 с. - 978-5-949-41160-5. - Текст: электронный // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/book/129192> - Режим доступа: по подписке

Дополнительная литература

1. Башлы П. Н. Информационная безопасность и защита информации: учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Информационная безопасность и защита информации - Москва: Евразийский открытый институт, 2012. - 311 с. - 978-5-374-00301-7. - Текст: электронный // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/10677.html> - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. <https://student2.consultant.ru/cgi/online.cgi> - Правовой Сервер КонсультантПлюс

Ресурсы «Интернет»

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

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

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

1. Microsoft Office;

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими

рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.