



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.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.11 ВВЕДЕНИЕ В АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»**

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: 5 з.е.
в академических часах: 180 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Долгова П. В.

Рабочая программа дисциплины (модуля) составлена 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

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 - формирование у обучающихся профессиональных компетенций в области организации и проведения аудиторских проверок состояния защищенности автоматизированных систем, а также получение теоретических знаний и практических навыков по оценке соответствия объектов информатизации требованиям стандартов и нормативно-правовых актов в сфере обеспечения информационной безопасности

Задачи изучения дисциплины:

- изучить основные понятия, стандарты, законодательные акты и нормативно-правовую базу в области аудита информационной безопасности, а также классификацию видов аудита;
- сформировать умение применять методики сбора и анализа данных об объекте аудита, выявлять уязвимости и несоответствия в системах защиты информации, а также оценивать эффективность существующих организационных и технических мер защиты;
- научить студентов разрабатывать программу аудита, формировать отчетную документацию по результатам проверки и формулировать практические рекомендации по повышению уровня защищенности информационной системы организации.

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

Компетенции, индикаторы и результаты обучения

ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

ОПК-2.4.1 Знает требования, предъявляемые к защищенным объектам информатизации

Знать:

ОПК-2.4.1/Зн1 Основные термины и определения в области аудита информационной безопасности

ОПК-2.4.1/Зн2 Классификацию и содержание ключевых международных и национальных стандартов в сфере информационной безопасности

Уметь:

ОПК-2.4.1/Ум1 Анализировать организационную структуру и техническую документацию компании для планирования аудиторской проверки

ОПК-2.4.1/Ум2 Составлять анкеты и опросные листы для интервьюирования сотрудников в ходе сбора аудиторских доказательств

Владеть:

ОПК-2.4.1/Нв1 Навыками работы с нормативно-правовой документацией и стандартами для выявления требований, применимых к объекту аудита

ОПК-2.4.1/Нв2 Методикой проведения предварительного интервью с заказчиком и сотрудниками для определения границ аудита

ОПК-2.4.2 Проводит аудит защищенности объекта информатизации

Знать:

ОПК-2.4.2/Зн1 Принципы построения системы менеджмента информационной безопасности как объекта аудита

ОПК-2.4.2/Зн2 Этические нормы и профессиональные стандарты поведения аудитора

Уметь:

ОПК-2.4.2/Ум1 Применять простейшие инструменты для проверки соответствия политик безопасности и технических настроек на соответствие требованиям стандартов

ОПК-2.4.2/Ум2 Интерпретировать результаты аудита и формулировать выводы о текущем состоянии защищенности информационной системы

Владеть:

ОПК-2.4.2/Нв1 Базовыми навыками документирования процесса аудита

ОПК-2.4.2/Нв2 Техниккой подготовки финального отчета по итогам аудита, включающего раздел с практическими рекомендациями

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.11 «Введение в аудит информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 7.

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)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
7 семестр	180	5	34	34	85	Курсовая работа Экзамен (27)
Всего	180	5	34	34	85	27

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотношенные с результатами освоения программы
Раздел 1. Теоретические и организационно-правовые основы аудита ИБ	50	10	11	29	ОПК-2.4. 1
Тема 1.1. Понятие, цели и виды аудита информационной безопасности	24	5	5	14	

Тема 1.2. Нормативно-правовая база и стандарты в области аудита ИБ	26	5	6	15	
Раздел 2. Методология проведения аудиторской проверки	52	12	11	29	ОПК-2.4. 1
Тема 2.1. Этапы проведения аудита информационной безопасности	25	6	5	14	ОПК-2.4. 2
Тема 2.2. Анализ рисков как основа аудита ИБ	27	6	6	15	
Раздел 3. Оформление результатов и развитие аудита ИБ	51	12	12	27	ОПК-2.4. 2
Тема 3.1. Отчетная документация и разработка рекомендаций по итогам аудита	26	6	6	14	
Тема 3.2. Современные тенденции и инструментальные средства аудита	25	6	6	13	
Итого	153	34	34	85	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Теоретические и организационно-правовые основы аудита ИБ

Тема 1.1. Понятие, цели и виды аудита информационной безопасности

Сущность аудита ИБ как инструмента управления рисками. Отличие аудита от мониторинга и расследования инцидентов. Классификация видов аудита: внешний и внутренний, инициативный и обязательный, аудит на соответствие требованиям и аудит эффективности. Место аудита в системе менеджмента информационной безопасности

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.2. Нормативно-правовая база и стандарты в области аудита ИБ

Законодательство РФ в сфере защиты информации (Конституция РФ, ГК РФ, КоАП, УК РФ, ФЗ «О персональных данных», ФЗ «О безопасности критической информационной инфраструктуры РФ»). Международные и национальные стандарты: серия стандартов ISO/IEC 27000 (ISO 27001, ISO 27002, ISO 19011 — руководящие указания по аудиту систем менеджмента), стандарты Банка России, методические документы ФСТЭК и ФСБ России

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Методология проведения аудиторской проверки

Тема 2.1. Этапы проведения аудита информационной безопасности

Планирование аудита: определение целей, области, критериев и объема проверки. Формирование группы аудиторов. Разработка программы и плана аудита.

Сбор и верификация информации: интервьюирование персонала, анализ организационно-распорядительной документации, инструментальный анализ защищенности

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.2. Анализ рисков как основа аудита ИБ

Понятие актива, угрозы, уязвимости. Качественные и количественные методы оценки рисков. Идентификация активов и построение модели угроз и нарушителя. Оценка текущих мер защиты. Интерпретация результатов оценки рисков для формирования выводов аудита

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 3. Оформление результатов и развитие аудита ИБ

Тема 3.1. Отчетная документация и разработка рекомендаций по итогам аудита

Структура и содержание отчета по аудиту ИБ. Описание несоответствий, замечаний и наблюдений. Формулирование выводов о состоянии объекта аудита. Разработка практических рекомендаций по устранению выявленных недостатков и совершенствованию СЗИ. Понятие корректирующих и предупреждающих действий

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.2. Современные тенденции и инструментальные средства аудита

Автоматизация процесса аудита: классы SIEM-, GRC-систем, сканеры безопасности. Особенности аудита облачных сервисов, виртуальной инфраструктуры и мобильных платформ. Профессиональная этика аудитора в области ИБ. Независимость и объективность аудиторских проверок

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: Экзамен, 7 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» 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 при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

Промежуточная аттестация: Курсовая работа, 7 семестр.

Курсовая работа оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется за глубокий анализ темы, оригинальные выводы и рекомендации, высокое качество оформления и отсутствие ошибок, убедительную защиту работы с полным пониманием темы;
- зачтено с оценкой «хорошо» выставляется за полное выполнение задания с хорошим уровнем анализа, четкую структуру и логику изложения материала, соответствие оформления основным требованиям;
- зачтено с оценкой «удовлетворительно» выставляется за выполнение всех заданий с незначительными недостатками, наличие основных разделов, но недостаточная глубина анализа, оформление работы с небольшими ошибками;
- не зачтено («не удовлетворительно») – выставляется за отсутствие темы или неуместный выбор, неполное выполнение заданий (отсутствие ключевых разделов), плагиат или отсутствие оригинальности, низкое качество оформления (нарушение стандартов).

7. Оценочные материалы текущего контроля

Раздел 1. Теоретические и организационно-правовые основы аудита ИБ

Контролируемые ИДК: ОПК-2.4.1

Тема 1.1. Понятие, цели и виды аудита информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является основной целью аудита информационной безопасности?

1. Наказание сотрудников за нарушение политик безопасности.
2. Получение объективной оценки текущего состояния защищенности объекта и его соответствия требованиям.
3. Демонстрация работы системы видеонаблюдения руководству.
4. Принудительное обновление всего программного обеспечения.

2. К какому виду аудита относится проверка, проводимая собственными силами организации (штатными специалистами)?

1. Внешний аудит.
2. Обязательный аудит.
3. Внутренний аудит.
4. Сертификационный аудит.

3. Что из перечисленного является объектом аудита информационной безопасности?

1. Только аппаратное обеспечение (серверы, ПК).
2. Только программное обеспечение.
3. Информационная система в целом, включая персонал, документацию, ПО и технические средства.
4. Только финансовая отчетность предприятия.

4. Какой стандарт из серии ISO/IEC 27000 содержит требования к системе менеджмента информационной безопасности (СМИБ) и часто используется для сертификационного аудита?

1. ISO/IEC 27002.
2. ISO/IEC 27001.
3. ISO/IEC 27005.
4. ISO 9001.

5. На каком этапе аудита разрабатывается программа проверки?

1. На этапе планирования.
2. На этапе сбора данных.
3. На этапе подготовки отчета.
4. На этапе корректирующих действий.

Тема 1.2. Нормативно-правовая база и стандарты в области аудита ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как в терминологии аудита называются задокументированные свидетельства, подтверждающие факты, полученные в ходе проверки?

1. Мнения экспертов.
2. Предположения аудитора.
3. Объективные доказательства.
4. Обещания сотрудников.

2. Что из перечисленного является нормативным документом ФСТЭК России в области защиты информации?

1. Налоговый кодекс РФ.
2. Трудовой кодекс РФ.
3. Приказ ФСТЭК №17 «Об утверждении Требований о защите информации...».
4. ГОСТ Р ИСО 9001-2015.

3. Аудит на соответствие требованиям законодательства о персональных данных (152-ФЗ) — это пример:

1. Аудита эффективности.
2. Аудита финансовой отчетности.

3. Аудита на соответствие (compliance audit).

4. Технического аудита сетей связи.

4. Какой метод сбора информации подразумевает беседу аудитора с сотрудниками организации?

1. Анализ документов.

2. Интервьюирование.

3. Инструментальное сканирование портов.

4. Реверс-инжиниринг кода.

5. Что означает понятие «уязвимость» в контексте аудита ИБ?

1. Потенциальную причину инцидента, которую сложно обнаружить.

2. Слабое место в системе, которое может быть использовано для реализации угрозы.

3. Стоимость восстановления системы после сбоя.

4. Высококвалифицированного злоумышленника.

Раздел 2. Методология проведения аудиторской проверки

Контролируемые ИДК: ОПК-2.4.1 ОПК-2.4.2

Тема 2.1. Этапы проведения аудита информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Сканеры безопасности (например, Nessus, MaxPatrol) используются для:

1. Создания резервных копий данных.

2. Автоматического выявления технических уязвимостей в ПО и конфигурациях.

3. Обучения сотрудников правилам парольной защиты.

4. Шифрования жестких дисков.

2. Что должно содержаться в итоговом отчете по аудиту?

1. Только перечень обнаруженных вирусов.

2. Выводы о состоянии объекта и рекомендации по устранению недостатков.

3. Личные характеристики сотрудников IT-отдела.

4. План развития компании на 5 лет.

3. Какой принцип является ключевым для работы аудитора?

1. Лояльность к руководству компании.

2. Независимость и объективность.

3. Скорость проведения проверки.

4. Коммерческая выгода от проверки.

4. Что такое «актив» в процессе аудита информационной безопасности?

1. Денежные средства на счетах организации.

2. Всё, что имеет ценность для организации и нуждается в защите (информация, сервисы, оборудование).

3. Активная позиция сотрудников на совещаниях.

4. Антивирусное программное обеспечение.

5. Какой федеральный закон регулирует обработку и защиту персональных данных в РФ?

1. ФЗ № 149 «Об информации...».

2. ФЗ № 152 «О персональных данных».

3. ФЗ № 187 «О безопасности КИИ».

4. ФЗ № 63 «Об электронной подписи».

Тема 2.2. Анализ рисков как основа аудита ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В чем разница между аудитом и расследованием инцидента?

1. Это одно и то же.
2. Аудит — это поиск виновных, расследование — поиск уязвимостей.
3. Аудит — это плановая проверка состояния защищенности, расследование — реактивное мероприятие по факту произошедшего события.
4. Аудит проводится только полицией.

2. Оценка рисков в ходе аудита необходима для:

1. Определения точной даты следующей проверки.
2. Приоритезации рекомендаций по уровню критичности выявленных проблем.
3. Увеличения бюджета отдела ИБ.
4. Увольнения некомпетентных сотрудников.

3. К какому классу объектов информатизации предъявляются наиболее строгие требования в соответствии с законодательством о КИИ?

1. Информационные системы персональных данных (ИСПДн).
2. Автоматизированные системы управления технологическими процессами (АСУ ТП) на объектах критической инфраструктуры.
3. Обычные веб-сайты организаций.
4. Локальные вычислительные сети без выхода в интернет.

4. Какой стандарт содержит руководящие указания по проведению аудита систем менеджмента (включая СМИБ)?

1. ISO/IEC 27005.
2. ISO 31000.
3. ISO 19011.
4. ГОСТ Р 34.10-2012.

5. Что означает термин «несоответствие» в аудиторском отчете?

1. Выявленный факт нарушения нормативного требования или политики.
2. Предложение по улучшению работы.
3. Мнение аудитора, не подкрепленное фактами.
4. Отсутствие на рабочем месте проверяемого сотрудника.

Раздел 3. Оформление результатов и развитие аудита ИБ

Контролируемые ИДК: ОПК-2.4.2

Тема 3.1. Отчетная документация и разработка рекомендаций по итогам аудита

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что проверяется в первую очередь при аудите организационных мер защиты?

1. Версии BIOS на компьютерах.
2. Наличие приказов, инструкций и политик безопасности, утвержденных руководителем.
3. Температура в серверной комнате.
4. Наличие пожарной сигнализации.

2. Аудит информационной безопасности по требованию законодательства (например, для ГИС) является:

1. Добровольным.
2. Инициативным.
3. Обязательным.
4. Рекомендательным.

3. Что такое SIEM-системы в контексте аудита?

1. Системы для автоматизации сбора и корреляции событий безопасности (могут использоваться как источник данных для аудита).
2. Программы для видеонаблюдения.
3. Инструменты для тестирования на проникновение.
4. Системы шифрования баз данных.

4. Политика информационной безопасности относится к:

1. Техническим мерам защиты.
2. Физическим мерам защиты.
3. Организационным (административным) мерам защиты.
4. Криптографическим мерам защиты.

5. Если в ходе аудита выяснилось, что пароли записаны на стикерах, приклеенных к мониторам, это является:

1. Хорошей практикой для быстрого доступа.
2. Организационной уязвимостью (нарушением политики безопасности).
3. Требованием эргономики рабочего места.
4. Элементом двухфакторной аутентификации.

Тема 3.2. Современные тенденции и инструментальные средства аудита

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В чем заключается цель корректирующих действий по итогам аудита?

1. В наказании ответственных за нарушение.
2. В устранении выявленных несоответствий и причин их возникновения.
3. В публикации отчета в СМИ.
4. В смене руководства организации.

2. Что понимается под «ложным срабатыванием» при работе сканера уязвимостей?

1. Обнаружение реально существующей уязвимости.
2. Сбой в работе самого сканера, требующий перезагрузки.
3. Ситуация, когда сканер указывает на уязвимость, которой на самом деле нет.
4. Успешное отражение хакерской атаки.

3. Какие данные необходимо собрать для идентификации активов на первом этапе аудита?

1. Только IP-адреса серверов.
2. Инвентаризационные данные об оборудовании, ПО, информационных ресурсах и их владельцах.
3. Номера лицензий Windows.
4. Список сотрудников, имеющих доступ в интернет.

4. GRC-системы в области ИБ предназначены для:

1. Обнаружения хакерских атак в реальном времени.
2. Автоматизации управления compliance (соответствием), рисками и политиками (часто используются для автоматизации аудита).
3. Шифрования трафика.
4. Блокировки вредоносных сайтов.

5. Какой документ определяет цели, объем и границы аудиторской проверки?

1. Акт приема-передачи дел.
2. Должностная инструкция аудитора.
3. Программа аудита.
4. Трудовой договор.

8. Оценочные материалы промежуточной аттестации

7 семестр, Экзамен

Контролируемые ИДК: ОПК-2.4.1 ОПК-2.4.2

Вопросы/Задания:

1. Понятие, цели и задачи аудита информационной безопасности. Место аудита в системе управления информационной безопасностью организации.

2. Виды аудита информационной безопасности: классификация, особенности и критерии выделения (внешний/внутренний, инициативный/обязательный).
3. Основные отличия аудита от мониторинга событий, расследования инцидентов и тестирования на проникновение.
4. Нормативно-правовая база аудита информационной безопасности в Российской Федерации: обзор федеральных законов.
5. Федеральный закон № 152-ФЗ «О персональных данных» и его роль в проведении аудита защищенности информационных систем.
6. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»: основные требования и особенности аудита для объектов КИИ.
7. Система стандартов ISO/IEC 27000 как методологическая основа аудита информационной безопасности.
8. Характеристика и область применения стандарта ISO/IEC 27001: требования к СМИБ и сертификационный аудит.
9. Роль стандарта ISO 19011 в проведении аудита систем менеджмента, включая СМИБ.
10. Документы и методики регуляторов (ФСТЭК России, ФСБ России) в области технической защиты информации и аттестации объектов.
11. Этапы проведения аудита информационной безопасности: характеристика и содержание каждого этапа.
12. Планирование аудита: разработка программы и плана аудита, определение целей, области и критериев проверки.
13. Понятие объекта и субъекта аудита информационной безопасности. Требования к группе аудиторов.
14. Методы сбора информации в ходе аудита: анализ документации, интервьюирование, инструментальный контроль.
15. Классификация активов организации и построение модели угроз и нарушителя как начальный этап аудиторской проверки.
16. Понятие уязвимости, угрозы и риска. Роль анализа рисков в аудите информационной безопасности.
17. Качественные и количественные методы оценки рисков: сущность, достоинства и недостатки.
18. Инструментальные средства аудита: назначение и классификация (сканеры уязвимостей, анализаторы протоколов, SIEM, GRC).

19. Назначение и принципы работы сканеров безопасности (Nessus, MaxPatrol, XSpider). Интерпретация результатов сканирования.

20. Организационный аудит: проверка организационно-распорядительной документации (политики, инструкции, регламенты).

21. Аудит технических мер защиты: проверка корректности настроек межсетевых экранов, средств антивирусной защиты и систем обнаружения вторжений.

22. Аудит физической защиты объекта информатизации (контроль доступа, видеонаблюдение, охрана).

23. Критерии оценки эффективности реализованных мер защиты информации в ходе аудита.

24. Порядок документирования результатов аудита: рабочие записи, протоколы, ведомости уязвимостей.

25. Структура и содержание итогового отчета по аудиту информационной безопасности.

26. Правила описания несоответствий, замечаний и наблюдений в аудиторском отчете.

27. Разработка рекомендаций по результатам аудита: понятие корректирующих и предупреждающих действий.

28. Принципы независимости, объективности и профессиональной этики аудитора в области информационной безопасности.

29. Современные тенденции развития аудита ИБ: особенности аудита облачных сервисов, виртуальной инфраструктуры и мобильных платформ.

30. Аттестация объектов информатизации и лицензирование деятельности в области защиты информации как формы подтверждения соответствия.

7 семестр, Курсовая работа

Контролируемые ИДК: ОПК-2.4.1 ОПК-2.4.2

Вопросы/Задания:

1. Сравнительный анализ международных и национальных стандартов в области аудита информационной безопасности (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001, ISO 19011).

2. Методология проведения внутреннего аудита информационной безопасности на предприятии (на примере коммерческой организации).

3. Нормативно-правовое регулирование аудита защищенности персональных данных в соответствии с ФЗ-152 «О персональных данных».

4. Разработка программы аудита информационной безопасности для государственной информационной системы (ГИС).

5. Особенности аудита защищенности объектов критической информационной инфраструктуры (КИИ) в соответствии с Ф3-187.

6. Методы и инструменты сбора доказательной базы при проведении аудита информационной безопасности.

7. Роль и место оценки рисков в процессе аудита информационной безопасности: сравнительный анализ методик.

8. Разработка чек-листа (опросного листа) для проведения аудита организационных мер защиты информации.

9. Анализ типовых нарушений и уязвимостей, выявляемых в ходе аудита информационных систем малого и среднего бизнеса.

10. Инструментальные средства аудита: сравнительный анализ сканеров безопасности (MaxPatrol, Nessus, XSpider).

11. Методика аудита настроек межсетевых экранов и средств защиты периметра сети.

12. Аудит политик парольной защиты и аутентификации в корпоративных информационных системах.

13. Особенности аудита систем обнаружения вторжений (IDS/IPS) и оценки эффективности их работы.

14. Разработка программы аудита физической защиты объекта информатизации (контроль доступа, видеонаблюдение, охрана).

15. Методика аудита антивирусной защиты в распределенных корпоративных сетях.

16. Анализ соответствия системы защиты информации требованиям стандарта ISO/IEC 27002: практические аспекты.

17. Разработка структуры и содержания итогового отчета по аудиту информационной безопасности.

18. Методы документирования несоответствий и формирования корректирующих действий по результатам аудита.

19. Аудит информационной безопасности при обработке персональных данных в медицинских учреждениях.

20. Особенности проведения аудита защищенности автоматизированных систем управления технологическими процессами (АСУ ТП).

21. Сравнительный анализ подходов к аудиту облачных сервисов (IaaS, PaaS, SaaS) и традиционной инфраструктуры.

22. Роль GRC-систем в автоматизации процессов аудита и управления соответствием требованиям ИБ.

23. Правовые и этические аспекты деятельности аудитора в области информационной безопасности.

24. Разработка методики аудита резервного копирования и восстановления данных в чрезвычайных ситуациях.

25. Аудит защищенности веб-приложений: методы, инструменты и критерии оценки.

26. Анализ типовых нарушений, выявляемых при проверке систем электронного документооборота.

27. Особенности аудита информационной безопасности в кредитно-финансовой сфере (стандарты Банка России).

28. Разработка плана корректирующих мероприятий по устранению недостатков, выявленных в ходе аудита ИБ.

29. Методика проведения аудита на этапе ввода информационной системы в эксплуатацию (первичный аудит).

30. Сравнительный анализ подходов к оценке эффективности затрат на обеспечение информационной безопасности по результатам аудита.

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Галатенко В. А. Основы информационной безопасности: учебное пособие: учебное пособие / В. А. Галатенко. - Основы информационной безопасности - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 266 с. - 978-5-4497-3316-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/142285.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Фаронов А. Е. Основы информационной безопасности при работе на компьютере: учебное пособие: учебное пособие / А. Е. Фаронов. - Основы информационной безопасности при работе на компьютере - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 154 с. - 978-5-4497-2418-2. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/133957.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Гулак М. Л. Аудит информационной безопасности. Прикладная статистика: учебное пособие: учебное пособие / М. Л. Гулак, М. Ю. Рытов, О. М. Голембиовская. - Аудит информационной безопасности. Прикладная статистика - Москва: Ай Пи Ар Медиа, 2020. - 121 с. - 978-5-4497-0713-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/97630.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. - Основы информационной безопасности - Москва: ЮНИТИ-ДАНА, 2023. - 287 с. - 978-5-238-02857-6. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/141624.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Овчинникова Е. А. Организационно-правовые основы информационной безопасности. Ч.1: учебное пособие: учебное пособие / Е. А. Овчинникова, Г. В. Попков; под редакцией С. Н. Новикова. - Организационно-правовые основы информационной безопасности. Ч.1 - Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. - 193 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/138773.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Овчинникова Е. А. Организационно-правовые основы информационной безопасности. Ч.2: учебное пособие: учебное пособие / Е. А. Овчинникова, Г. В. Попков; под редакцией С. Н. Новикова. - Организационно-правовые основы информационной безопасности. Ч.2 - Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. - 168 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/138774.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

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

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

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

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)

Не используется.

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.

Учебная аудитория

LED-экран - 1 шт.

Автоматизированное рабочее место (АРМ) - 1 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.