



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.19.10 ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ 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: 7 з.е.
в академических часах: 252 ак.ч.

Москва, 2024

Разработчики:

Доцент кафедры Информационно-измерительных систем, к.т.н.

Дубов С. С.

Преподаватель кафедры Информационно-измерительных систем

Носенко О. 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 способности решать задачи, связанные с организацией и функционированием службы информационной безопасности, разработкой организационно-распорядительных документов, регламентирующих деятельность по обеспечению информационной безопасности, управлением комплексом мер по защите информации, включая анализ угроз, моделирование систем защиты и проектирование структур службы защиты информации.

Задачи изучения дисциплины:

- освоение системного подхода к организации службы информационной безопасности, включая анализ угроз и моделирование систем защиты;
- понимание механизмов разработки организационно-распорядительных документов с учетом требований стандартов и нормативно-правовых актов;
- формирование умений применения комплексных мер защиты информации на основе анализа выявленных угроз.

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

Компетенции, индикаторы и результаты обучения

ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба

ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты

Знать:

ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности

Уметь:

ОПК-2.1.1/Ум1 Выявлять угрозы информационной безопасности применительно к объектам защиты

Владеть:

ОПК-2.1.1/Нв1 Навыками описания объекта информатизации как совокупности информационных, технических, программных и человеческих ресурсов, объединенных для реализации конкретного функционального процесса

ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели

Знать:

ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации

Уметь:

ОПК-2.1.2/Ум1 Определять меры необходимые для снижения рисков реализации угроз информационной безопасности

Владеть:

ОПК-2.1.2/Нв1 Методиками анализа и категорирования потенциальных угроз информационной безопасности (нарушение конфиденциальности, целостности, доступности) применительно к конкретным элементам объекта защиты

ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб

Знать:

ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации

Уметь:

ОПК-2.1.3/Ум1 Определять объект защиты и методы дестабилизирующего воздействия на него

Владеть:

ОПК-2.1.3/Нв1 Навыками построения сценариев реализации угроз, описывающих возможные пути проникновения и деструктивного воздействия на объект

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.10 «Организация системы обеспечения информационной безопасности» относится к обязательной части образовательной программы и изучается в семестре(ах): 3, 4.

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)
3 семестр	72	2	34	17	21	Зачет
4 семестр	180	5	42	42	60	Курсовая работа Экзамен (36)
Всего	252	7	76	59	81	36

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. Что такое информация. Информационная безопасность	18	8	4	6	ОПК-2.1. 1

Тема 1.1. Что такое информация. Информационная безопасность	18	8	4	6	
Раздел 2. Информационные процессы, связанные с защищаемой информацией	24	12	6	6	ОПК-2.1.1
Тема 2.1. Информационные процессы, связанные с защищаемой информацией	24	12	6	6	ОПК-2.1.2 ОПК-2.1.3
Раздел 3. Управления рисками	30	14	7	9	ОПК-2.1.1
Тема 3.1. Управления рисками	30	14	7	9	ОПК-2.1.2 ОПК-2.1.3
Раздел 4. Аудит информационной безопасности	48	14	14	20	ОПК-2.1.1
Тема 4.1. Аудит информационной безопасности	48	14	14	20	ОПК-2.1.2 ОПК-2.1.3
Раздел 5. Особенности построения модели угроз и модели нарушителя	48	14	14	20	ОПК-2.1.1
Тема 5.1. Особенности построения модели угроз и модели нарушителя	48	14	14	20	ОПК-2.1.2 ОПК-2.1.3
Раздел 6. Механизмы снижения вероятности реализации угроз информационной безопасности	48	14	14	20	ОПК-2.1.1
Тема 6.1. Механизмы снижения вероятности реализации угроз информационной безопасности	48	14	14	20	ОПК-2.1.2 ОПК-2.1.3
Итого	216	76	59	81	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Что такое информация. Информационная безопасность

Тема 1.1. Что такое информация. Информационная безопасность

Что такое информация. Информационная безопасность. Базовые определения. Защищаемая информация. Основания отнесения информации к защищаемой. Обучающийся изучает основные понятия информации и ИБ.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Информационные процессы, связанные с защищаемой информацией

Тема 2.1. Информационные процессы, связанные с защищаемой информацией

Как и кем информация производится, обрабатывается, где и как хранится, по каким каналам передается, кто и какой имеет к ней доступ. Как уничтожается. Информационные процессы, связанные с защищаемой информацией. Обучающийся анализирует процессы обработки защищаемой информации.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 3. Управления рисками

Тема 3.1. Управления рисками

Что такое риск. Какие есть подходы к оценке рисков. Какие есть механизмы управления рисками. Обучающийся готовит обзор методов управления рисками ИБ.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 4. Аудит информационной безопасности

Тема 4.1. Аудит информационной безопасности

Цель и задачи аудита. Виды аудита. Преимущества и недостатки разных видов аудита. Обучающийся изучает виды, этапы и стандарты аудита ИБ.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 5. Особенности построения модели угроз и модели нарушителя

Тема 5.1. Особенности построения модели угроз и модели нарушителя

Что такое модель угроз и модель нарушителя, зачем они нужны. Особенности построения модели угроз и модели нарушителя. Обучающийся составляет примеры моделей угроз и нарушителя для организации.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 6. Механизмы снижения вероятности реализации угроз информационной безопасности

Механизмы снижения вероятности реализации угроз. Классификация механизмов защиты. Основные методы. Оценка эффективности механизмов. Обучающийся анализирует контрмеры по снижению угроз информационной безопасности.

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, 3 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.

Промежуточная аттестация: Экзамен, 4 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, 4 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. Что такое информация. Информационная безопасность

Контролируемые ИДК: ОПК-2.1.1

Тема 1.1. Что такое информация. Информационная безопасность

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является основной целью информационной безопасности?

1. Обеспечение бесперебойного электропитания серверов
2. Защита интересов личности, общества и государства в информационной сфере
3. Создание максимально неудобных условий для пользователей
4. Установка самого дорогого программного обеспечения

2. Какие три основные свойства информации защищаются в рамках ИБ?

1. Актуальность, полнота, полезность
2. Скорость передачи, объем, стоимость
3. Понятность, лаконичность, своевременность
4. Конфиденциальность, целостность, доступность

3. Что такое «Модель угроз» в контексте ИБ?

1. Схема локальной вычислительной сети предприятия
2. Гипотетическая ситуация нападения хакеров
3. Штатное расписание отдела информационной безопасности
4. Документ, описывающий возможные угрозы и их источники

4. Для чего предназначен аудит информационной безопасности?

1. Для поиска и наказания сотрудников, нарушивших правила
2. Для независимой оценки текущего уровня защищенности компании
3. Для модернизации компьютерного оборудования
4. Для проверки бухгалтерской отчетности отдела ИТ

5. Что такое «идентификация» в системе контроля доступа?

1. Присвоение субъекту и объекту уникального признака (имени, номера)
2. Предоставление прав на выполнение операций
3. Проверка подлинности предъявленного идентификатора

4. Шифрование данных при передаче

Раздел 2. Информационные процессы, связанные с защищаемой информацией

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Тема 2.1. Информационные процессы, связанные с защищаемой информацией

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой метод аутентификации считается биометрическим?

1. Ответ на контрольный вопрос
2. Ввод логина и пароля
3. Сканирование отпечатка пальца
4. Использование USB-ключа

2. Что относится к организационным (административным) мерам защиты информации?

1. Подписание с сотрудником соглашения о неразглашении коммерческой тайны
2. Шифрование жесткого диска
3. Настройка антивируса на сервере
4. Установка межсетевого экрана

3. Как называется документ, определяющий правила работы с защищаемой информацией в организации?

1. Устав предприятия
2. Политика информационной безопасности
3. Должностная инструкция системного администратора
4. Паспорт информационной системы

4. Что такое межсетевой экран (брандмауэр)?

1. Средство контроля и фильтрации сетевого трафика
2. Устройство для резервного копирования данных
3. Программа для поиска вирусов на компьютере
4. Система обнаружения протечек воды в серверной

5. К какому виду угроз относится «социальная инженерия»?

1. Программная угроза (вирус-шифровальщик)
2. Техническая угроза (аппаратный сбой)
3. Угроза непреодолимой силы (форс-мажор)
4. Антропогенная угроза (воздействие человеческого фактора)

Раздел 3. Управления рисками

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Тема 3.1. Управления рисками

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является основанием для отнесения информации к защищаемой?

1. Информация размещена в сети Интернет
2. Желание собственника любой ценой скрыть информацию
3. Наличие в отношении информации законодательных требований или введение собственником режима коммерческой тайны
4. Высокая стоимость оборудования, на котором хранятся данные

2. Какая функция относится к задачам службы информационной безопасности?

1. Закупка расходных материалов для принтеров
2. Расследование инцидентов информационной безопасности
3. Проведение маркетинговых исследований

4. Уборка помещений серверной

3. Что такое VPN?

1. Протокол передачи голоса по IP-сети
2. Аппаратный ключ для защиты ПО
3. Виртуальная частная сеть для создания защищенных соединений
4. Вид компьютерного вируса

4. Какие данные относятся к категории персональных данных?

1. Любая информация, относящаяся к прямо или косвенно определенному физическому лицу
2. Информация о финансовых показателях компании
3. Техническая документация на продукцию предприятия
4. Сведения, составляющие государственную тайну

5. Какова основная цель резервного копирования данных?

1. Защита от кражи компьютера
2. Восстановление информации при ее утрате или повреждении
3. Освобождение места на жестком диске
4. Ускорение работы операционной системы

Раздел 4. Аудит информационной безопасности

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Тема 4.1. Аудит информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое «уязвимость» в контексте ИБ?

1. Недостаток или слабое место в системе, которое может быть использовано для реализации угрозы
2. Установка обновлений Windows
3. Нежелание сотрудников соблюдать инструкции
4. Хакер, атакующий систему

2. Какая ответственность предусмотрена УК РФ за неправомерный доступ к компьютерной информации?

1. Только материальная ответственность
2. Только дисциплинарное взыскание
3. Уголовная ответственность (штраф, исправительные работы, лишение свободы)
4. Административный штраф

3. Что такое электронная подпись?

1. Пароль для входа в электронную почту
2. Информация в электронной форме для идентификации лица, подписавшего документ
3. Сканированное изображение подписи человека
4. Название антивирусной программы

4. Для чего проводится аттестация объектов информатизации?

1. Для подключения к сети Интернет
2. Для определения рыночной стоимости компьютера
3. Для подтверждения соответствия системы защиты требованиям безопасности
4. Для инвентаризации основных средств

5. Что из перечисленного является методом предотвращения утечек информации (DLP-система)?

1. Настройка прав доступа к папкам
2. Лечение зараженных файлов от вирусов
3. Анализ исходящего трафика и копируемых на флешки данных
4. Создание резервных копий баз данных

Раздел 5. Особенности построения модели угроз и модели нарушителя

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Тема 5.1. Особенности построения модели угроз и модели нарушителя

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой из стандартов описывает требования к системе менеджмента информационной безопасности?

1. ГОСТ Р ИСО/МЭК 27001
2. ГОСТ Р 3410 (криптография)
3. ГОСТ Р ИСО 9001 (менеджмент качества)
4. ISO 14001 (экологический менеджмент)

2. Что понимается под «промышленным шпионажем»?

1. Незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну
2. Легальный сбор информации о конкурентах из открытых источников
3. Рейдерский захват предприятия
4. Маркетинговое исследование рынка

3. Что определяет «Модель нарушителя»?

1. Список сотрудников, имеющих доступ к секретным данным
2. Психологический портрет хакера в капюшоне
3. Вероятные пути проникновения злоумышленников
4. Предположения о возможностях, целях и типе злоумышленника

4. Какой вид физической защиты относится к инженерно-техническим средствам?

1. Инструктаж сотрудников о пропускном режиме
2. Наклейка «Посторонним вход воспрещен»
3. Договор с частным охранным предприятием
4. Охранный сигнализация на входе в серверную

5. Что является инцидентом информационной безопасности?

1. Плановая проверка системы защиты
2. Любое событие, которое может привести к нарушению ИБ
3. Единичный случай опоздания сотрудника на работу
4. Установка нового программного обеспечения

Раздел 6. Механизмы снижения вероятности реализации угроз информационной безопасности

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Тема 6.1. Механизмы снижения вероятности реализации угроз информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой метод шифрования является симметричным?

1. Хэширование пароля
2. Кодирование информации в Base64
3. Использование одного и того же ключа для шифрования и расшифровки
4. Использование открытого и закрытого ключа (например, RSA)

2. Какая информация может составлять коммерческую тайну?

1. Сведения о способах производства и технологиях, имеющих коммерческую ценность
2. Информация о численности работников и системе оплаты труда
3. Учредительные документы предприятия
4. Сведения о загрязнении окружающей среды

3. Что такое IDS (система обнаружения вторжений)?

1. Устройство для бесперебойного питания серверов
2. Система для блокировки рекламы в браузере
3. Программа для автоматического создания паролей
4. Программное или аппаратное средство, анализирующее трафик на предмет атак
4. Для чего необходимо лицензирование деятельности в области защиты информации?
 1. Для допуска организаций к работам, требующим высоких стандартов безопасности (например, гостайна)
 2. Для запрета на использование иностранного ПО
 3. Для статистического учета всех ИБ-специалистов в стране
 4. Для повышения налоговых сборов с ИТ-компаний
5. Кто несет персональную ответственность за организацию защиты информации с ограниченным доступом на предприятии?
 1. Руководитель организации
 2. Любой сотрудник, работающий с этой информацией
 3. Системный администратор
 4. Начальник службы безопасности

8. Оценочные материалы промежуточной аттестации

3 семестр, Зачет

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Вопросы/Задания:

1. Информация. Носители информации. Критерии отнесения информации к защищаемой.
2. Что такое информационная безопасность? Перечислите основные принципы организации защиты информации.
3. Порядок построения комплексной системы защиты информации.
4. Основание для отнесения информации к защищаемой.
5. Основные нормативные документы в сфере информационной безопасности.
6. Модель Угроз. Ее содержание и предназначение.
7. Модель нарушителя. Ее содержание и предназначение.
8. Угроза информационной безопасности. Определение. Свойства. Классификация.
9. Основные функции службы ИБ
10. Организационно-психологические меры защиты информации.
11. Микроклимат в коллективе и его влияние на ИБ организации.
12. Стимулирование сотрудников.

13. Предпосылки возникновения инцидента ИБ. Реакция на компьютерные инциденты.
14. Компьютерные инциденты.
15. Киберпреступления. Законодательство в России и за рубежом.
16. Конвенция о преступности в сфере компьютерной безопасности.
17. Стандарты ИБ. Содержание. Предназначение.
18. Классификация угроз безопасности.
19. Защита персональных данных.
20. Защита интеллектуальной собственности.
21. Уязвимость и ущербы в ИБ.
22. Структура и функции органов защиты информации предприятия.
23. Понятие «политика информационной безопасности». Цели, задачи и структурные уровни.
24. Роли и ответственность субъектов доступа.
25. Аттестация объектов информатизации. Цель, порядок проведения и участники процесса.
26. Лицензирование деятельности в области защиты информации. Органы лицензирования и виды лицензий.
27. Правовой режим коммерческой тайны. Меры по охране конфиденциальности информации, составляющей коммерческую тайну.
28. Законодательство Российской Федерации в области персональных данных. Права субъектов и обязанности операторов.
29. Трансграничная передача персональных данных.
30. Ответственность за правонарушения в сфере компьютерной информации.

4 семестр, Экзамен

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Вопросы/Задания:

1. Технические средства обеспечения физической безопасности.
2. Принципы организации защиты информации.

3. Действия службы ИБ в случае уличения сотрудника в воровстве.
4. Действия службы ИБ в случае уличения сотрудника в промышленном шпионаже.
5. Аудит информационной безопасности.
6. Основные документы отдела Защиты информации. Их содержание и предназначение.
7. Межсетевые экраны. Их разновидности и предназначение
8. Электронные ключи разновидности и сферы использования.
9. Классификация автоматизированных систем и требований по защите информации от несанкционированного доступа согласно руководящим документам ФСТЭК России.
10. Идентификация, аутентификация и авторизация. Определение, различие между понятиями и практическая реализация.
11. Биометрические методы аутентификации. Разновидности, преимущества и недостатки, области применения.
12. Парольная защита. Требования к сложности, методы хранения, управление парольной политикой.
13. Криптографические методы защиты информации: основные понятия (шифрование, электронная подпись, хэш-функция).
14. Понятие и организация виртуальных частных сетей (VPN) для обеспечения безопасной передачи данных по открытым каналам связи.
15. Обнаружение и предотвращение вторжений (IDS/IPS). Принципы работы и место в системе защиты.
16. Антивирусная защита: типы вредоносного ПО, методы обнаружения, организация антивирусной защиты в корпоративной сети.
17. Анализ защищенности и тестирование на проникновение. Цели, этапы, отличия от аудита.
18. Управление уязвимостями: процесс выявления, оценки и устранения уязвимостей программного обеспечения.
19. Резервное копирование и восстановление информации как мера обеспечения доступности и целостности данных. Виды резервного копирования.
20. Защита информации при использовании облачных сервисов.
21. Социальная инженерия как угроза информационной безопасности. Методы защиты от социальной инженерии.

22. Методы предотвращения утечек информации со стороны внутренних нарушителей.
23. Обеспечение физической безопасности объектов вычислительной техники и носителей информации.
24. Организация режима конфиденциального делопроизводства. Учет, хранение и обращение с документами, содержащими защищаемую информацию.
25. План непрерывности бизнеса и восстановления после чрезвычайных ситуаций.
26. Управление инцидентами информационной безопасности. Этапы выявления, реагирования и расследования.
27. Классификация и категорирование защищаемой информации. Маркировка материальных и электронных носителей.
28. Международные и национальные стандарты в области управления информационной безопасностью.
29. Принципы и методы риск-менеджмента в информационной безопасности.
30. Показатели эффективности системы защиты информации.

4 семестр, Курсовая работа

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Вопросы/Задания:

1. Анализ Закона № 5485-1 и практика применения Перечня сведений (Указ № 1203)
2. Проблемы разграничения сведений конфиденциального характера: сравнительный анализ Перечня (Указ № 188) и положений ФЗ «О коммерческой тайне» и «О персональных данных»
3. Реализация требований ФЗ «Об информации, информационных технологиях...» (№ 149-ФЗ) при организации защиты информации на предприятии
4. Влияние «закона о суверенном Рунете» (№ 156-ФЗ) на архитектуру и обеспечение информационной безопасности телекоммуникационных сетей в России
5. Правовой статус персональных данных: организация системы защиты в соответствии с требованиями ФЗ-152 в кредитно-финансовой сфере / медицинских учреждениях
6. Сравнительный анализ Доктрины информационной безопасности 2016 года и текущей Стратегии национальной безопасности: новые угрозы и приоритеты защиты
7. Разработка Положения о защите коммерческой тайны на предприятии (на примере IT-компании / производственного холдинга) в соответствии с ФЗ-98

8. Организация системы допуска к государственной тайне: анализ полномочий Межведомственной комиссии и практических процедур на режимном объекте

9. Роль и задачи Министерства внутренних дел в борьбе с преступлениями в сфере компьютерной информации (в контексте обеспечения ИБ)

10. Координация деятельности по защите информации: разграничение функций ФСТЭК и ФСБ России при создании объектов информатизации

11. Особенности организации защиты информации в Министерстве обороны / Службе внешней разведки (анализ открытых источников и общих принципов ведомственного документооборота)

12. Деятельность Совета Безопасности РФ как основного координатора государственной политики в области обеспечения информационной безопасности

13. Сравнительный анализ современных DLP-систем (на примере решений Solar Dozor, InfoWatch, ViPNet) и их роль в предотвращении утечек конфиденциальной информации

14. Применение SIEM-систем для обеспечения ситуационной централизованной безопасности в крупной организации: проблемы внедрения и настройки

15. Организация безопасного периметра корпоративной сети: сравнительный анализ поколений межсетевых экранов (NGFW) и их эффективность

16. Актуальность антивирусной защиты в эпоху «политики нулевого доверия»: сравнительный анализ антивирусных решений для корпоративного сектора

17. Инженерно-техническая защита информации: проектирование комплекса систем контроля доступа (СКУД) и видеонаблюдения для обеспечения физической безопасности серверной

18. Криптографические методы защиты: реализация электронной подписи (ЭП) и управление электронными ключами в системах электронного документооборота

19. Безопасность сетевой инфраструктуры: анализ уязвимостей активного сетевого оборудования (маршрутизаторы, коммутаторы) и методы их защиты

20. «Цифровой портрет организации» как объект защиты: анализ внешних и внутренних информационных рисков и методов их минимизации

21. Проблема защиты «цифрового портрета человека»: анализ угроз, связанных со сбором, хранением и обработкой биометрических и поведенческих данных

22. Обеспечение информационной безопасности при использовании систем видеоконференцсвязи (ВКС): сравнительный анализ решений по критериям безопасности и конфиденциальности

23. Угрозы безопасности VoIP-связи и методы их нейтрализации при организации корпоративных переговоров

24. Анализ требований рынка труда к специалистам по ИБ: компетенции выпускников профильных вузов и соответствие актуальным задачам бизнеса

25. Построение эффективной системы обучения сотрудников компании основам информационной безопасности как альтернатива техническим средствам защиты

26. Методология управления инцидентами информационной безопасности: разработка регламентов реагирования (на примере вирусных атак или атак на отказ в обслуживании)

27. Проведение аудита информационной безопасности на предприятии: анализ соответствия требованиям ФСТЭК и ФСБ России (практические аспекты)

28. Управление рисками информационной безопасности при передаче данных на аутсорсинг (облачные технологии, SaaS-провайдеры)

29. Обеспечение безопасности жизненного цикла веб-приложений (DevSecOps): внедрение средств контроля уязвимостей на этапах разработки

30. Анализ защищенности веб-ресурсов: обзор автоматизированных средств поиска уязвимостей (сканеров) и методология ручного тестирования (пентеста)

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. 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

3. Газизов А. Р. Организационное и правовое обеспечение информационной безопасности: учебное пособие: учебное пособие / А. Р. Газизов; под редакцией А. Р. Айдиняна. - Организационное и правовое обеспечение информационной безопасности - Ростов-на-Дону: Донской государственный технический университет, 2017. - 156 с. - 978-5-7890-1384-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/117813.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Тумбинская М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник: учебник / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург: Лань, 2022. - 344 с. - 978-5-8114-3940-9. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/207095.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш, М. В. Песков, В. В. Меденец. - Комплексное обеспечение информационной безопасности автоматизированных систем - Ставрополь: Северо-Кавказский федеральный университет, 2016. - 242 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/62945.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Ревнивых А. В. Информационная безопасность в организациях: учебное пособие: учебное пособие / А. В. Ревнивых. - Информационная безопасность в организациях - Москва: Ай Пи Ар Медиа, 2021. - 83 с. - 978-5-4497-1164-9. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/108227.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Ворожейкин В. Н. Технические средства и методы защиты информации – дополнительные главы: лабораторный практикум: лабораторный практикум / В. Н. Ворожейкин. - Технические средства и методы защиты информации – дополнительные главы - Самара: Самарский государственный технический университет, ЭБС АСВ, 2019. - 336 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/111432.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://www.iprbookshop.ru/> - IPR BOOKS
3. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
4. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
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)

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.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 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.