МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

20.03.2019 г.

протокол № 3

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

15 января 2020 г.

протокол № 5

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Методы и средства информационной безопасности
Направление подготовки	38.03.05 БИЗНЕС-ИНФОРМАТИКА
Профиль	Цифровой бизнес
Форма обучения	очная
Год набора	2020

Разработана:
Доцент,к.ф.м.н.
Тюлюкин Владимир Александрович

Ст. преподаватель,
Змеева Наталья Юрьевна

Екатеринбург
2020 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	**3**
1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ	**3**
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	**3**
3. ОБЪЕМ ДИСЦИПЛИНЫ	**3**
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП	**3**
5. ТЕМАТИЧЕСКИЙ ПЛАН	**4**
6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ	**5**
7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	**8**
8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	**14**
9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	**14**
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	**14**
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	**15**

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 38.03.05 БИЗНЕС-ИНФОРМАТИКА (уровень бакалавриата) (приказ Минобрнауки России от 11.08.2016 г. № 1002)
ПС	

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование у студентов теоретических и практических знаний в области информационной безопасности, принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности предприятия.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточный контроль	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 5						
Экзамен	144	56	28	28	52	4

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Общекультурные компетенции (ОК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	ИД-1.ОК-4 Знает необходимые для осуществления профессиональной деятельности правовые нормы, регулирующие экономические правоотношения Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности. Имеет навыки применения нормативной базы и решения экономических задач в области избранных видов профессиональной деятельности.

Общепрофессиональные компетенции (ОПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций

ОПК-1 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИД-1.ОПК-1 Знать: информационно-коммуникационные технологии, применяемые для решения стандартных задач профессиональной деятельности Уметь: использовать информационно-коммуникационные технологии, информационные ресурсы и библиографические базы данных в решении профессиональных задач; учитывать основные требования информационной безопасности при решении профессиональных задач. Иметь навыки решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры и с учетом основных требований информационной безопасности

Профессиональные компетенции (ПК)

Шифр и наименование компетенции	Индикаторы достижения компетенций
организационно-управленческая	
ПК-9 организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	ИД-1.ПК-9 Знать: - принципы обеспечения защиты информации, уровни информационной защиты, технические аспекты обеспечения защиты информации, основные направления работ по созданию системы информационной безопасности предприятия; - основные функции участников процесса обеспечения информационной безопасности предприятия; - методы организации эффективного взаимодействия с основными участниками процесса обеспечения информационной безопасности предприятия Уметь: - обеспечивать защиту информации и реализацию работ по созданию системы информационной безопасности предприятия; - обеспечивать эффективное взаимодействие между основными участниками процесса обеспечения информационной безопасности предприятия; - решать задачи, возникающие в ходе взаимодействия основных участников процесса обеспечения информационной безопасности предприятия Владеть навыками (трудовые действия) - навыками деловых коммуникаций в профессиональной сфере; - навыками решения задач обеспечения информационной безопасности предприятия

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 5		108					
Тема 1.	Предмет курса. Информационная безопасность в системе национальной безопасности РФ	6	2			4	

Тема 2.	Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.	8	2	2		4	
Тема 3.	Методы и средства обеспечения информационной безопасности. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей	40	6	16		18	
Тема 4.	Правовое регулирование защиты информации	12	4			8	
Тема 5.	Организационно методические методы защиты информации	12	2	2		8	
Тема 6.	Технические средства защиты информации	4	2			2	
Тема 7.	Криптографические методы защиты	14	2	4		8	
Тема 8.	Вопросы управления ИБ	12	8	4			

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1. Предмет курса. Информационная безопасность в системе национальной безопасности РФ	Контрольная работа №1 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации
Тема 2. Основные понятия теории информационной безопасности . Анализ угроз информационной безопасности.	Тест (Приложение 4)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Оценивается знание изученного материала.

Тема 3.Методы и средства обеспечения информационной безопасности . Стандарты информационной безопасности , критерии и классы оценки защищенности и компьютерных систем и сетей	Контрольная работа №2 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.
Тема 6. Технические средства защиты информации	Контрольная работа №3 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.
Тема 5. Организационно методические методы защиты информации	Контрольная работа №4 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.
Тема 7. Криптографические методы защиты	Контрольная работа №5 (Приложение 4)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Четкость и логичность формулировок, правильность выполнения и оформления работы, выполнение основных требований оформления документации.
Промежуточный контроль (Приложение 5)			

5 семестр (Эк)	Экзаменационные билеты (приложение 5)	В билете 2 теоретических вопроса и 1 практический	100 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущей и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущая аттестация. Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущей аттестации, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Предмет курса. Информационная безопасность в системе национальной безопасности РФ
Введение: предмет, содержание и задачи дисциплины, ее место среди других дисциплин учебного плана, формы отчетности, основная и дополнительная литература.
Место информационной безопасности в общей системе безопасности государства. Концепция информационной безопасности. Структура и основные положения нормативных правовых актов в области информационной безопасности. Государственные стандарты, используемые в области информационной безопасности.

Тема 2. Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.
Ценность информации. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита представления информации. Защита содержания информации. Основные виды атак на информационные АС. Классификация основных атак и вредоносных

Тема 3. Методы и средства обеспечения информационной безопасности. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей

Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Угрозы безопасности в компьютерных системах. Классификация способов несанкционированного доступа к информации в компьютерных системах. Модель поведения потенциального нарушителя. Алгоритм подготовки и реализации атаки нарушителем. Атака на политику безопасности. Атака на сменные элементы системы безопасности. Атака на протоколы информационного взаимодействия. Анализ способов нарушений информационной безопасности.

Противодействие несанкционированного доступа к информации в компьютерных системах. Требования к системе защиты информации. Принципы и правила организации защиты информации от несанкционированного доступа к информации в компьютерных системах. Этапы развития систем информационной безопасности. Средства защита информации в компьютерных системах. Система защиты информации на базе программно-аппаратного комплекса. Подсистемы защиты информации. Состав типового комплекса защиты от несанкционированного доступа к информации. Механизмы работы комплекса защиты от несанкционированного доступа к информации.

Многоуровневая модель защиты объектов информатизации. Способы защиты информации от утечки за счет ПЭМИН. Активные устройства защиты от утечки по каналам ПЭМИН.

Международные стандарты информационного обмена. Аппаратно-технические средства для организации технической защиты в сфере международного информационного обмена. Технологии защиты информации. Аппаратные межсетевые экраны. Рекомендации Microsoft по безопасному подключению почтового сервера к интернет. Безопасность браузеров. Схема подключения брандмауэров или файлволлов или межсетевого экрана. Брандмауэр Agnitum Outpost Firewall Pro. Защита локальный вычислительных сетей брандмауэром с одним сетевым интерфейсом. Средства защиты информации eToken, Symantec Antivirus for Ms Exchange, Symantec Antivirus client. Электронная цифровая подпись, порядок функционирования. Гипотетическая (гетерогенная) вычислительная сеть. Комплексный план технической защиты информации. Алгоритм создания системы информационной безопасности. Совершенствование организационных мероприятий, меры противодействия взлому защиты. Логическая архитектура информационно-вычислительного комплекса.

Защита информации в компьютерных системах от случайных угроз. Создание и управление учетными записями пользователей. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS. Аудит ресурсов и событий системы защиты. Настройка системных параметров безопасности. Настройка параметров безопасности подключения к Интернет. Повышение безопасности информации встроенными средствами. Шифрования операционной системы. Архивация и восстановление данных.

Понятия о видах вирусов. Классификация вирусов: по среде обитания; по способу заражения; по степени опасности деструктированных воздействий; по алгоритму функционирования. Механизм работы вирусов. Способы внедрения потенциально опасных программ. Методы обнаружения вирусов: сканирование; обнаружение изменений; эвристический анализ; использование резидентных сторожей; вакцинирование программ; аппаратно-программная защита. Антивирусные программы: Norton AntiVirus; McAfee; Dr. Web; Kaspersky Anti-Virus; Антивирус Касперского OEM. Профилактика заражения вирусами компьютерных систем. Сущность комплексного подхода

Тема 4. Правовое регулирование защиты информации

Система лицензирования на право проведения работ и оказания услуг в области защиты информации с ограниченным доступом. Нормативные документы, определяющие порядок лицензирования в области защиты конфиденциальной информации. Условия лицензирования деятельности по защите конфиденциальной информации. Общие принципы лицензирования в области защиты конфиденциальной информации. Лицензионные требования для получения лицензии на деятельность в области технической защиты конфиденциальной информации. Перечень документов, представляемых для получения лицензий в области защиты конфиденциальной информации. Система сертификации средств защиты информации. Структура средств защиты информации, подлежащих сертификации. Аттестация объектов информатизации на соответствие требованиям безопасности информации. Объекты, подлежащие аттестации. Перечень основных нормативных документов, определяющих порядок и объём аттестационных испытаний объектов информатизации. Общие требования по аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации. Порядок проведения аттестации объектов информатизации

Тема 5. Организационно методические методы защиты информации

Понятие государственной системы защиты информации. Принципы функционирования государственной системы защиты информации. Правовые основы деятельности государственной системы защиты информации. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Цели и задачи государственной системы защиты информации. Организационная и функциональная структура государственной системы защиты информации. Стандартизация в области обеспечения информационной безопасности. Пользование стандартами информационной безопасности.

Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима. Регламентация доступа персонала к информационным и вычислительным ресурсам. Организация работы с конфиденциальными документами. Требования и рекомендации по защите конфиденциальной информации. Учет, хранение, использование и уничтожение документов (носителей) с конфиденциальной информацией. Организация контроля за соблюдением исполнителями должностных инструкций. Правовое регулирование в сфере информационных отношений. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности. Пользование стандартами информационной безопасности. Международные и отечественные нормативные и руководящие документы, связанные с информационной безопасностью. Руководящие документы Гостехкомиссии РФ

Тема 6. Технические средства защиты информации

Общая характеристика и классификация технических каналов утечки информации (ТКУИ). Элементарная модель канала утечки информации. Основные и вспомогательные технические средства и системы. Контролируемая зона. Основные виды ТКУИ. Технические каналы утечки информации обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ): электромагнитные; электрические; параметрические. Технические каналы утечки акустической (речевой) информации: воздушные; вибрационные; акустоэлектрические; параметрические; оптико-электронный (лазерный). Технические каналы перехвата информации при ее передаче по каналам связи. Технические каналы утечки видовой информации.

Инженерно-технические средства и системы охраны объектов. Охранная сигнализация. Телевизионные системы видеоконтроля. Идентификация и аутентификация лиц, допускаемых на объект. Основные виды технических каналов и источников утечки информации. Противодействие наблюдению в оптическом диапазоне. Защита от прослушивания акустических сигналов. Средства борьбы с закладными подслушивающими устройствами. Защита речевой информации, передаваемой по каналам связи. Пассивные и активные методы защиты информации от утечки в результате электромагнитных излучений и наводок.

Комплексное обеспечение защиты информации от утечки по техническим каналам. Методика принятия решения на защиту от утечки информации в организации. Возможные виды квалификации злоумышленников. Оценка возможностей вероятных злоумышленников. Оценка своей организации как возможного источника информации для злоумышленников. Порядок организации защиты информации на этапе определения задач защиты. Порядок выбора целесообразных мер и средств защиты. Критерии оценки уровня защиты. Организационные способы защиты

Тема 7. Криптографические методы защиты

Введение в криптологию. Исторический обзор. Криптография и криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования. Ключи и алгоритмы шифрования. Методы шифрования с симметричным ключом. Методы замены (подстановки) и перестановки. Гаммирование. Шифрование, использующее генераторы (датчики) псевдослучайных последовательностей. Системы блочного шифрования на основе отечественного ГОСТа и стандарта DES (США). Системы несимметричного шифрования: с открытым ключом для шифрования и закрытым - для дешифрования. Односторонние функции. Криптографическая система RSA. Электронная цифровая подпись на основе криптографического преобразования. Особенности стандартизации и сертификации криптографических средств.

Тема 8. Вопросы управления ИБ

Вопросы управления ИБ

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности.

Анализ домашней компьютерной сети студента с точки зрения ценности информации, угроз и состояния систем защиты.

Тема 3. Методы и средства обеспечения информационной безопасности. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей

Противодействие несанкционированного доступа к информации в компьютерных системах. Требования к системе защиты информации. Принципы и правила организации защиты информации от несанкционированного доступа к информации в компьютерных системах. Этапы развития систем информационной безопасности. Средства защита информации в компьютерных системах. Система защиты информации на базе программно-аппаратного комплекса. Подсистемы защиты информации. Состав типового комплекса защиты от несанкционированного доступа к информации. Механизмы работы комплекса защиты от несанкционированного доступа к информации

Тема 5. Организационно методические методы защиты информации Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима. Регламентация доступа персонала к информационным и вычислительным ресурсам. Организация работы с конфиденциальными документами. Требования и рекомендации по защите конфиденциальной информации. Учет, хранение, использование и уничтожение документов (носителей) с конфиденциальной информацией.
Тема 7. Криптографические методы защиты Проверка криптостойкости шифров
Тема 8. Вопросы управления ИБ Изучение современных подходов к обеспечению безопасности коммерческой информации.

7.3. Содержание самостоятельной работы

Тема 1. Предмет курса. Информационная безопасность в системе национальной безопасности РФ Самоконтроль,
Тема 2. Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности. Изучить подсистемы безопасности в домашней информационной системе
Тема 3. Методы и средства обеспечения информационной безопасности. Стандарты информационной безопасности, критерии и классы оценки защищенности компьютерных систем и сетей контрольные работы
Тема 4. Правовое регулирование защиты информации Изучение нормативно методических документов
Тема 5. Организационно методические методы защиты информации Тест
Тема 6. Технические средства защиты информации Изучение стандартов
Тема 7. Криптографические методы защиты Контрольная работа

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
Материалы не предусмотрены

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ

http://lib.usue.ru/

Основная литература:

1. Партыка Т. Л., Попов И. И.. Информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2016. - 432 с. – Режим доступа: https://new.znanium.com/catalog/product/516806

1. Баранова Е.К., Бабаш А.В.. Информационная безопасность и защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИОР, 2016. - 322 с. – Режим доступа: https://new.znanium.com/catalog/product/495249

Дополнительная литература:

1. Ковалев Д. В., Богданова Е. А.. Информационная безопасность:учебное пособие. - Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2016. - 74 с.

2. Шаньгин В. Ф.. Информационная безопасность компьютерных систем и сетей:учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника". - Москва: Форум: ИНФРА-М, 2012. - 415 с.

4. Коноплева И. А., Богданов И. А.. Управление безопасностью и безопасность бизнеса:учебное пособие для студентов вузов, обучающихся по специальности " Прикладная информатика (по областям)". - Москва: ИНФРА-М, 2008. - 447 с.

5. Золотарев В. В., Данилова Е. А.. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс]:учебное пособие для студентов, обучающихся по специальностям "Комплексное обеспечение информационной безопасности автоматизированных систем", "Информационная безопасность телекоммуникационных систем", а также по магистерским программам направления "Информатика и вычислительная техника": в 3 частях. - Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2010. - 144 с. – Режим доступа: http://znanium.com/go.php?id=463037

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионное программное обеспечение:

Microsoft Windows 10 .Акт предоставления прав № Tr060590 от 19.09.2017. Срок действия лицензии 30.09.2020.

Microsoft Office 2016. Акт предоставления прав № Tr060590 от 19.09.2017. Срок действия лицензии 30.09.2020.

Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без органичения срока.

Embarcadero RAD Studio. Эл. лицензия, Информационное письмо. Срок действия лицензии 05.05.2020.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

-Справочно-правовая система Консультант +. Договор № 194-У-2019 от 09.01.2020. Срок действия лицензии до 31.12.2020

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.