Автономная некоммерческая организация высшего образования
«Открытый университет экономики, управления и права»
(АНО ВО ОУЭП)

УТВЕРЖДАЮ:

Сведения об электронной подписи
Подписано: Фокина Валерия Николаевна
Должность: ректор
Пользователь: vfokina

«20» января 2021г.

РАБОЧАЯ ПРОГРАММА

по дисциплине

Наименование дисциплины Б1.О.04 «Защита информации в ИС»
Образовательная программа направления подготовки 09.04.01 «Информатика и вычислительная техника», направленность (профиль): Информационные системы

Рассмотрено к утверждению на заседании
кафедры информатики
(протокол № 15-01 от 15.01.2021 г.)

Квалификация - магистр

Разработчик:
Артюшенко В.М., д.тех.н., проф.

Москва 2021

1. Цели и задачи дисциплины

Цель дисциплины - усвоение общей методологии, современных проблем и широкого круга специальных вопросов информационной безопасности информационных систем (ИС).

***Задачи дисциплины*:**

- раскрыть структуру и содержание круга современных проблем информационной безопасности ИС;
- охарактеризовать основные направления, средства и методы решения проблем обеспечения безопасности ИС;
- сформировать представления о научных основах решения проблем безопасности ИС;
- обеспечить формирование профессиональных навыков в области решения проблем безопасности ИС;
- выработка научного подхода к практике применения теоретических знаний в области защиты информации;
- повышение мотивации к процессу изучения научной дисциплины и научной деятельности.

2. Место дисциплины в структуре программы

Дисциплины «Защита информации в ИС» относится к обязательной части Блока 1.

3. Планируемые результаты обучения по дисциплине

Универсальную компетенцию:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Общепрофессиональные компетенции:

ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач;

ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;

Результаты освоения дисциплины, установленные индикаторы достижения компетенций

Наименование компетенции	Индикаторы достижения компетенции	Показатели (планируемые) результаты обучения
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает: принципы сбора, отбора и обобщения информации; основы теории систем и системного анализа	**Знать:** • основные технологии обеспечения безопасности ИС и соответствующие методы и средства;
	УК-1.2. Умеет: соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности	**Уметь:** • ставить и решать типовые задачи в области разработки и применения защищенных ИС;
	УК-1.3. Владеет: информационными источниками; навыками научного поиска, подготовки научных текстов	**Владеть:** • методами обработки результатов;
ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1. Знает: современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы, применяемые для решения профессиональных задач	**Знать:** • научные основы обеспечения безопасности ИС; • сущность и содержание типовых задач в области разработки и применения защищенных ИС;
	ОПК-2.2. Умеет: обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред и программно-технических платформ; разрабатывать оригинальные алгоритмы и программные средства для решения профессиональных задач	**Уметь:** • подбирать и использовать адекватные формы, методы и средства разработки и практического применения защищенных ИС;
	ОПК-2.3. Владеет: навыками разработки оригинальных	**Владеть:** • техническими средствами обеспечения

Наименование компетенции	Индикаторы достижения компетенции	Показатели (планируемые) результаты обучения
	алгоритмов и программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий для решения профессиональных задач	безопасности ИС.
ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ОПК-5.1. Знает: современное программное и аппаратное обеспечение информационных и автоматизированных систем	**Знать:** • основные направления и перспективы развития технологий защиты информации в ИС;
	ОПК-5.2. Умеет: модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач	**Уметь:** • оценивать эффективность применения ИС;
	ОПК-5.3. Владеет: навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	**Владеть:** • программными средствами обеспечения безопасности ИС.

Знания, умения и навыки, формируемые дисциплиной «Защита информации в ИС», являются необходимыми для изучения последующих дисциплин.

Междисциплинарные связи с дисциплинами

Компетенция	Этапы формирования компетенций, определяемые дисциплинами направления подготовки «Информатика и вычислительная техника»		
	начальный	последующий	итоговый
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Распределённая обработка информации в автоматизированных системах	Методы моделирования и исследования информационных систем	Выполнение и защита выпускной квалификационной работы
	Математические методы в ИВТ		
	Защита информации в ИС		
	Моделирование и анализ бизнес-процессов		
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения	Защита информации в ИС	Инструментальное обеспечение информационных систем	Выполнение и защита выпускной квалификационной работы
ОПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и	Распределённая обработка информации в автоматизированных системах	Производственная практика, технологическая (проектно-технологическая)	Корпоративные информационные системы
	Защита информации в ИС		Производственная практика, научно-исследовательская работа

Компетенция	Этапы формирования компетенций, определяемые дисциплинами направления подготовки «Информатика и вычислительная техника»		
	начальный	последующий	итоговый
автоматизированных систем	Технология баз данных и знаний		Выполнение и защита выпускной квалификационной работы
	Учебная практика, ознакомительная		
	Производственная практика, технологическая (проектно-технологическая)		

4. Объем дисциплины и виды учебной работы

Учебным планом предусматриваются следующие виды работы по дисциплине:

№ п/п	Виды учебных занятий	Всего часов по формам обучения, ак. ч			
		Очная		Заочная	
		всего	в том числе	всего	в том числе
1	**Контактная работа (объем работы обучающихся во взаимодействии с преподавателем) (всего)**			**20,2**	
	В том числе в форме практической подготовки				***2***
1.1	занятия лекционного типа (лекции)			4	
1.2	занятия семинарского типа (практические)*, в том числе:			12	
1.2.1	семинар-дискуссия, практические занятия				0 12
	в форме практической подготовки				*2*
1.2.2	занятия семинарского типа: лабораторные работы (лабораторные практикумы)				
1.2.3	курсовое проектирование (выполнение курсовой работы)			2	
1.3	контроль промежуточной аттестации и оценивание ее результатов, в том числе:			2,2	
1.3.1	консультации групповые				2
1.3.2	прохождение промежуточной аттестации				0,2
2	**Самостоятельная работа (всего)**			**189**	
2.1	работа в электронной информационно-образовательной среде с образовательными ресурсами учебной библиотеки, компьютерными средствами обучения для подготовки к текущей и промежуточной аттестации, к курсовому проектированию (выполнению курсовых работ)			189	
2.2	самостоятельная работа при подготовке к промежуточной аттестации			**6,8**	
3	Общая трудоемкость часы дисциплины зачетные единицы форма промежуточной аттестации			**216**	
				6	
		экзамен			

*_____

Семинар – семинар-дискуссия
ГТ - практическое занятие - глоссарный тренинг
ТТ - практическое занятие - тест-тренинг
ПЗТ - практическое занятие - позетовое тестирование
ЛС - практическое занятие - логическая схема
УД - семинар-обсуждение устного доклада

РФ – семинар-обсуждение реферата
Асессмент реферата - семинар-асессмент реферата
ВБ - вебинар
УЭ - семинар-обсуждение устного эссе
АЛТ - практическое занятие - алгоритмический тренинг

5. Содержание дисциплины

5.1. Содержание разделов и тем

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в информационную безопасность ИС	**Информация как объект защиты** Свойства, виды и формы представления информации. Информация и информационные ресурсы. Информация как объект права собственности. Информация как коммерческая тайна. Информация как рыночный продукт. Автоматизированные системы (АС) как объекты защиты информации. **ИС как объекты обработки и защиты информации** Классическая архитектура «клиент-сервер». Архитектура «клиент-сервер», основанная на Web-технологии. Технологии распределенной обработки информации. Доступ к базам данных. Управление информацией о ресурсах и пользователях ИС. Условия и режимы эксплуатации ИС. **Основные понятия и анализ угроз информационной безопасности** Основные понятия защиты информации и информационной безопасности (ИБ). Обзор и классификация угроз информации, обрабатываемой в ИС. Обзор способов реализации угроз безопасности информации. Несанкционированный доступ (НСД) к информации в ИС.
2	Обеспечение безопасности информации в ИС.	**Анализ существующих подходов к обеспечению безопасности информации** Законодательный, административный и процедурный уровни информационной безопасности. Основные понятия политики безопасности. Структура политики безопасности организации. Программно-технический уровень информационной безопасности. Сервисы безопасности. **Особенности защиты информации в ИС** Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС. Защита информации на уровне подсистемы управления ИС. Защита информации в каналах связи. Подтверждение подлинности информации, получаемой по коммуникационной подсети. Особенности защиты информации в базах данных. **Общие теоретические подходы к защите информации** Математические модели управления доступом к информации. Политика безопасности и модели доступа. Способы анализа моделей доступа. Модели нарушителей ИБ. Основы построения защиты информации. Модель элементарной защиты. Модель многозвенной защиты. Многоуровневая защита. **Международные и отечественные стандарты в сфере защиты информации** Роль стандартов ИБ. Международные стандарты ИБ. Стандарты для беспроводных сетей. Стандарты ИБ в Интернет. Отечественные стандарты в сфере защиты информации. **Сертификация и аттестация в области защиты информации** Назначение и общая характеристика. Проведение сертификационных испытаний. Аттестация объектов информатизации. Сертификация на региональном и международном уровнях. **Основы правового обеспечения защиты информации** Международный опыт правового обеспечения ИБ. Государственная система правового обеспечения ИБ. Содержание основных законов РФ в области ИБ. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.
3	Методы и средства технической защиты информации в ИС	**Виды и методы технической защиты информации** Пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры. **Технические каналы утечки информации** Общая характеристика технических каналов утечки информации и их

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		классификация. Каналы утечки речевой информации. Технические средства и методы получения информации по этим каналам. Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок. Технические средства и методы получения информации с использованием этих каналов. **Методы и средства защиты информации от утечки по техническим каналам** Основные методы, используемые при создании систем защиты информации. Заземление технических средств передачи информации. Использование сетевых фильтров. Экранирование помещений. Методы защиты от утечек по акустическим каналам. Защита средств связи и телекоммуникаций.
4	Технологии защиты данных в ИС.	**Современные методы защиты информации в ИС** Ограничение и разграничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Идентификация и установление подлинности объекта (субъекта). Криптографическое преобразование информации. Методы защиты информации от компьютерных вирусов. **Криптографические средства защиты информации** Основные принципы и классификация методов криптографического преобразования информации. Обзор методов шифрования. Выбор метода преобразования информации. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Электронная цифровая подпись (ЭЦП) и функции хэширования. Процедуры выработки ЭЦП. Защита электронного документооборота с использованием ЭЦП. **Технологии аутентификации** Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие одноразовые и многоразовые пароли и PIN-коды. Аутентификация, основанная на симметричных и асимметричных алгоритмах. Биометрическая аутентификация пользователей. **Технологии межсетевых экранов** Противодействие несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Установка и конфигурирование межсетевых экранов. Критерии оценки межсетевых экранов. Обзор современных межсетевых экранов. **Технологии защищенных виртуальных сетей** Способы создания защищенных виртуальных каналов. Туннелирование на канальном уровне. Защита виртуальных каналов на сетевом уровне. Построение защищенных виртуальных сетей на сеансовом уровне. Организация безопасного удаленного доступа. Обзор средств построения защищенных виртуальных сетей. Построение защищенных виртуальных сетей на базе маршрутизаторов, межсетевых экранов, специализированного программного обеспечения, специализированных аппаратных средств.
5	Технологии обнаружения вторжений в ИС.	**Анализ защищенности и обнаружения атак** Концепции адаптивного управления безопасностью. Технологии анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционных систем (ОС). Технологии обнаружения атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Методы реагирования. **Защита от вирусов в ИС** Компьютерные вирусы и проблемы антивирусной защиты. Основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты ИС. **Методы управления средствами сетевой безопасности ИС** Задачи управления системой сетевой безопасности. Архитекутура управления средствами сетевой безопасности. Функционирование системы управления средствами безопасности. Аудит и мониторинг безопасности. Стандарты, используемые при проведении аудита. Анализ рисков и управление рисками. Программные средства, используемые для анализа и управления рисками.
6	Построение и организация	**Построение комплексных систем защиты информации** Концепция создания защищенных ИС. Этапы создания комплексной системы

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
	функционирования комплексных систем защиты информации в ИС	защиты информации (КСЗИ). Моделирование КСЗИ. Выбор показателей эффективности и критериев оптимальности КСЗИ. Математическая постановка задачи разработки КСЗИ. Подходы к оценке эффективности КСЗИ. Создание организационной структуры КСЗИ. **Организация функционирования комплексных систем защиты информации** Пути и проблемы практической реализации концепции комплексной защиты информации. Применение КСЗИ. Техническая эксплуатация КСЗИ.

5.2 Занятия лекционного и семинарского типа

5.2.1 Темы лекций

Раздел 1 «Введение в информационную безопасность ИС»

1.Информация как объект защиты

2.Анализ угроз информационной безопасности

Раздел 2 «Обеспечение безопасности информации в ИС»

1.Особенности защиты информации в ИС

2.Сертификация и аттестация в области защиты информации

Раздел 3 «Методы и средства технической защиты информации в ИС»

1.Виды и методы технической защиты информации

2.Технические каналы утечки информации

Раздел 4 «Технологии защиты данных в ИС»

1.Современные методы защиты информации в ИС

2.Технологии защищенных виртуальных сетей

Раздел 5 «Технологии обнаружения вторжений в ИС»

1.Анализ защищенности и обнаружения атак

2.Управление средствами сетевой безопасности ИС

Раздел 6 «Построение и организация функционирования комплексных систем защиты информации в ИС»

1.Построение комплексных систем защиты информации (КСЗИ)

2.Техническая эксплуатация КСЗИ

5.2.2 Вопросы для обсуждения на семинарах и практических занятиях

Раздел 1 «Введение в информационную безопасность ИС»

1. Основные составляющие информационной безопасности.
2. ИС как объекты обработки и защиты информации.
3. Основные понятия защиты информации и информационной безопасности.
4. Технологии распределенной обработки информации.

Раздел 2 «Обеспечение безопасности информации в ИС»

1. Задачи, решаемые на законодательном, процедурном и административном уровнях информационной безопасности.
2. Особенности защиты информации в ИС.
3. Подтверждение подлинности информации, получаемой по коммуникационной подсети.
4. Модели защиты информации в ИС.
5. Роль стандартов информационной безопасности.
6. Организационное обеспечение информационной безопасности.
7. Сертификация и аттестация в области защиты информации.
8. Содержание основных законов РФ в области информационной безопасности.

Раздел 3 «Методы и средства технической защиты информации в ИС»

1. Каналы утечки речевой информации.
2. Механические системы защиты в задачах информационной безопасности ИС.
3. Системы оповещения. Системы опознавания.
4. Защита средств связи и телекоммуникаций.

Раздел 4 «Технологии защиты данных в ИС»

1. Методы криптографического преобразования данных.
2. Разграничение и контроль доступа к информации.
3. Симметричные и асимметричные алгоритмы шифрования.
4. Защита электронного документооборота с использованием электронной цифровой подписи.

Раздел 5 «Технологии обнаружения вторжений в ИС»

1. Функции межсетевых экранов.
2. Персональные и распределенные межсетевые экраны.
3. Основные понятия и функции виртуальных защищенных сетей.
4. Достоинства технологий виртуальных защищенных сетей.
5. Основные каналы распространения вирусов и других вредоносных программ.
6. Антивирусные программы и комплексы.
7. Анализ защищенности и обнаружения атак.

Раздел 6 «Построение и организация функционирования комплексных систем защиты информации в ИС»

1. Методы управления средствами сетевой безопасности ИС.
2. Программные средства, используемые для анализа и управления рисками.
3. Выбор показателей эффективности и критериев оптимальности комплексной системы защиты информации.

5.3 Определение соотношения объема занятий, проведенное путем непосредственного взаимодействия педагогического работника с обучающимися по заочной форме

Виды контактной работы	**Образовательные технологии**		**Контактная работа**	
	Объем занятий, проводимых путем непосредственного взаимодействия педагогического работника с обучающимися (ак.ч)	**Объем занятий с применением электронного обучения, дистанционных образовательных технологий (ак.ч)**	**(всего ак.ч.)**	**в том числе в форме практической подготовки (ак.ч.)**
1	2	3	4	5
Лекционного типа (лекции)	4	-	**4**	**-**
Семинарского типа (семинар)	-	-	-	-
Семинарского типа (практические занятия)	-	12	**12**	**-**
в том числе в форме практической подготовки	-	-	-	***2***
Семинарского типа (курсовое проектирование (работа))	2	-	**2**	**-**
Семинарского типа (лабораторные работы)	-	-	-	-
Промежуточная аттестация (экзамен)	2,2	-	**2,2**	**-**
Итого	8,2	12	**20,2**	***2***

Соотношение объема занятий, проводимых путем непосредственного взаимодействия педагогического работника с обучающимися по заочной форме – 41 %

6. Методические указания по освоению дисциплины

6.1 Учебно-методическое обеспечение дисциплины

Методические указания для преподавателя

Изучение дисциплины проводится в форме лекций, практических занятий, организации самостоятельной работы студентов, консультаций. Главное назначение лекции - обеспечить теоретическую основу обучения, развить интерес к учебной деятельности и конкретной учебной дисциплине, сформировать у студентов ориентиры для самостоятельной работы над курсом.

Основной целью практических занятий является обсуждение наиболее сложных теоретических вопросов курса, их методологическая и методическая проработка. Они проводятся в форме опроса, диспута, тестирования, обсуждения докладов и пр.

Самостоятельная работа с научной и учебной литературой, дополняется работой с тестирующими системами, тренинговыми программами, с информационными базами, образовательным ресурсов электронной информационно-образовательной среды и сети Интернет.

6.2 Методические материалы обучающимся по дисциплине, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Методические материалы доступны на сайте «Личная студия» в разделе «Методические указания и пособия».

1. Методические указания «Введение в технологию обучения».
2. Методические указания по проведению учебного занятия «Вебинар».
3. Методические указания по проведению занятия «Семинар - обсуждение устного эссе», «Семинар - обсуждение устного доклада».
4. Методические указания по проведению занятия «Семинар – асессмент реферата».
5. Методические указания по проведению занятия «Семинар – обсуждение реферата».
6. Методические указания по проведению учебного занятия с компьютерным средством обучения «Практическое занятие - тест-тренинг».
7. Методические указания по проведению учебного занятия с компьютерным средством обучения «Практическое занятие - глоссарный тренинг».
8. Методические указания по проведению занятия «Практическое занятие - позетовое тестирование».
9. Положение о реализации электронного обучения, дистанционных образовательных технологий.
10. Методические указания по проведению занятия «Практическое занятие - алгоритмический тренинг».

Указанные методические материалы для обучающихся доступны в Личной студии обучающегося, в разделе ресурсы.

6.3 Особенности реализации дисциплины в отношении лиц из числа инвалидов и лиц с ограниченными возможностями здоровья

Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия и переработки учебного материала.

Подбор и разработка учебных материалов должны производится с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

Выбор средств и методов обучения осуществляется самим преподавателям. При этом в образовательном процессе рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений студентов с ограниченными возможностями здоровья с преподавателями и другими студентами, создания комфортного психологического климата в студенческой группе.

Разработка учебных материалов и организация учебного процесса проводится с учетом нормативных документов и локальных актов образовательной организации.

В соответствии с нормативными документами инвалиды и лица с ограниченными возможностями здоровья по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь; инвалиды и лица с ограниченными возможностями здоровья по слуху имеют право на использование звукоусиливающей аппаратуры.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении государственной итоговой аттестации;

- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей(занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);

- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении аттестации с учетом их индивидуальных особенностей;

- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут.

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья организация обеспечивает выполнение следующих требований при проведении аттестации:

а) для слепых:

- задания и иные материалы для сдачи экзамена оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

- письменные задания выполняются обучающимися с использованием клавиатуры с азбукой Брайля, либо надиктовываются ассистенту;

б) для слабовидящих:

- задания и иные материалы для сдачи экзамена оформляются увеличенным шрифтом и\или использованием специализированным программным обеспечением Jaws;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- при необходимости обучающимся предоставляется увеличивающее устройство,допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- имеется в наличии информационная система "Исток" для слабослышащих коллективного пользования;

- по их желанию испытания проводятся в электронной или письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата:

- тестовые и тренинговые задания по текущей и промежуточной аттестации выполняются обучающимися на компьютере через сайт «Личная студия" с использованием электронного обучения, дистанционных технологий;

- для обучения лиц с нарушениями опорно-двигательного аппарата используется электронный образовательный ресурс, электронная информационно-образовательная среда;

- по их желанию испытания проводятся в устной форме.

О необходимости обеспечения специальных условий для проведения аттестации обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

6.4 Методические рекомендации по самостоятельной работе студентов

Цель самостоятельной работы - подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Реализация поставленной цели предполагает решение следующих задач:

- качественное освоение теоретического материала по изучаемой дисциплине, углубление и расширение теоретических знаний с целью их применения на уровне межпредметных связей;

- систематизация и закрепление полученных теоретических знаний и практических навыков;

- формирование умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;

- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;

- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;

- развитие научно-исследовательских навыков;

- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретенные знания, способности и навыки.

Самостоятельная работа является неотъемлемой частью образовательного процесса.

Самостоятельная работа предполагает инициативу самого обучающегося в процессе сбора и усвоения информации, приобретения новых знаний, умений и навыков и ответственность его за планирование, реализацию и оценку результатов учебной деятельности. Процесс освоения знаний при самостоятельной работе не обособлен от других форм обучения.

Самостоятельная работа должна:

- быть выполнена индивидуально (или являться частью коллективной работы). В случае, когда СР подготовлена в порядке выполнения группового задания, в работе делается соответствующая оговорка;
- представлять собой законченную разработку (этап разработки), в которой анализируются актуальные проблемы по определенной теме и ее отдельных аспектов;
- отражать необходимую и достаточную компетентность автора;
- иметь учебную, научную и/или практическую направленность;
- быть оформлена структурно и в логической последовательности: титульный лист, оглавление, основная часть, заключение, выводы, список литературы, приложения,
- содержать краткие и четкие формулировки, убедительную аргументацию, доказательность и обоснованность выводов;
- соответствовать этическим нормам (правила цитирования и парафраз; ссылки на использованные библиографические источники; исключение плагиата, дублирования собственного текста и использования чужих работ).

6.4.1 Формы самостоятельной работы обучающихся по разделам дисциплины

Раздел 4 «Технологии защиты данных в ИС»

Темы устного доклада

1. Задачи подсистемы управления идентификацией и доступом.
2. Перечислите основные атаки на протоколы аутентификации.
3. Опишите метод аутентификации на основе одноразовых паролей, его достоинства и недостатки.
4. Опишите метод аутентификации на основе многоразовых паролей, его достоинства и недостатки.
5. Опишите аппаратные средства аутентификации удаленных пользователей.
6. Опишите функциональность и характеристики смарт-карт и USB-токенов.
7. Особенности биометрической аутентификации пользователей.
8. Вредоносная программа. Основные типы вредоносных программ.
9. Укажите существенные отличия компьютерных вирусов от сетевых червей. Опишите основные особенности троянских программ.
10. Опишите основные подходы к обнаружению вредоносных программ.
11. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.
12. Дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ.
13. Опишите меры и средства защиты от спама.
14. Объясните суть фильтрации информационного потока межсетевым экраном.
15. Функции посредничества межсетевого экрана и программы-посредники. Функции, которые могут выполнять программы-посредники.
16. Опишите особенности функционирования экранирующего маршрутизатора (пакетного фильтра).
17. Назовите достоинства программно-аппаратного варианта исполнения межсетевых экранов.
18. Сформулируйте принципы формирования политики межсетевого взаимодействия, реализуемой системой межсетевых экранов.
19. Назовите основные схемы подключения межсетевых экранов. Опишите функционирование схемы с защищаемой закрытой и незащищаемой открытой подсетями.
20. Опишите тенденции дальнейшего развития межсетевых экранов.
21. Особенности использовании PIN-кода.
22. Дактилоскопические устройства аутентификации.
23. Системы аутентификации по голосу.
24. Системы аутентификации по узору радужной оболочки и сетчатки глаз.
25. Характеристика программного средства Kaspersky Internet Security.
26. Характеристика программного средства Dr.Web.
27. Характеристика программного средства Norton Internet Security.
28. Особенности функционирования персональных межсетевых экранов.
29. Особенности функционирования распределенных межсетевых экранов.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Рекомендуемая литература

Основная учебная и научная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html

Дополнительная литература

1. Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 с. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/74381.html
2. Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных : учебное пособие / С. Н. Никифоров, М. М. Ромаданов. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 108 с. — ISBN 978-5-9227-0783-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/80747.html
3. Никифоров С.Н. Защита информации. Защищенные сети [Электронный ресурс] : учебное пособие / С.Н. Никифоров. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 80 с. — 978-5-9227-0762-6. — Режим доступа: http://www.iprbookshop.ru/74382
4. Алексеев А.П. Многоуровневая защита информации [Электронный ресурс] / А.П. Алексеев. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 128 с. — 978-5-904029-72-2. — Режим доступа: http://www.iprbookshop.ru/75387

7.2. Ресурсы информационно-телекоммуникационной сети Интернет

- http://citforum.ru/
- http://www.rushelp.com/
- http://www.emanual.ru/
- http://www.gnpbu.ru/ - Научная педагогическая библиотека им. К.Д. Ушинского.

8. Материально-техническое обеспечение дисциплины, перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая программное обеспечение, современные профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине имеется следующее материально-техническое обеспечение:

- учебные аудитории для проведения учебных занятий, оборудованные учебной мебелью и оснащенные оборудованием и техническими средствами обучения с возможностью подключения к сети «Интернет»;

- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде.

Программное обеспечение:

Лицензионное программное обеспечение (в том числе, отечественного производства):

Операционная система Windows Professional 10

ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц

Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО)

Платформа проведения вебинаров (отечественное ПО)

Информационная технология. Онлайн тестирование цифровой платформы Ровеб (отечественное ПО)

Электронный информационный ресурс. Экспертный интеллектуальный информационный робот Аттестация асессоров (отечественное ПО)

Информационная технология. Аттестационный интеллектуальный информационный робот контроля оригинальности и профессионализма «ИИР КОП» (отечественное ПО)

Электронный информационный ресурс «Личная студия обучающегося» (отечественное ПО)

Свободно распространяемое программное обеспечение (в том числе отечественного производства):

Мой Офис Веб-редакторы https://edit.myoffice.ru (отечественное ПО)

ПО OpenOffice.Org Calc.

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.Org.Base

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.org.Impress

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.Org Writer

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО Open Office.org Draw

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами;

Современные профессиональные базы данных:

Реестр профессиональных стандартов https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/

Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» https://reestr.digital.gov.ru/

Общество с ограниченной ответственностью «Интерактивные обучающие технологии» https://htmlacademy.ru/tutorial/php/mysql

Web-технологии https://htmlweb.ru/php/mysql.php

Научная электронная библиотека. http://elibrary.ru

Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) –электронная библиотека по всем отраслям знаний http://www.iprbookshop.ru

Информационно-справочные системы:

- Справочно-правовая система «Гарант»;
- Справочно-правовая система «Консультант Плюс».