ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА ЦИФРОВЫХ ТЕХНОЛОГИЙ

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ Е.С. Сахарчук
«17» 04 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Методы защиты и преобразование информации

образовательная программа направления подготовки 09.03.01 «Информатика и вычислительная техника»
шифр, наименование

Направленность (профиль)
Программное обеспечение вычислительной техники и информационных систем
Квалификация (степень) выпускника: бакалавр

Форма обучения очная

Курс 3 семестр 5,6

Москва 2022

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования направления (специальности) 09.03.01 «Информатика и вычислительная техника», утвержденного приказом Министерства образования и науки Российской Федерации № 929 от «19» сентября 2017 г. Зарегистрировано в Минюсте России «10» октября 2017 г. № 48489

Разработчики рабочей программы:

МГГЭУ, заведующий кафедрой цифровых технологий
место работы, занимаемая должность

_____ Митрофанов Е.П. 14.03 20 22 г
подпись Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Цифровых технологий
(протокол № 4 от «21» 03 20 22 г.)

на заседании Учебно-методического совета МГГЭУ
(протокол № 1 от «27» 04 20 22 г.)

СОГЛАСОВАНО:

Начальник учебно-методического управления
_____И.Г. Дмитриева
«27» 04 2022 г.

Начальник методического отдела
_____Д.Е. Гапеенок
«27» 04 2022 г.

Заведующий библиотекой
_____В.А. Ахтырская
«27» 04 2022 г.

Декан факультета ПМиИ
_____ Е.В.Петрунина
«27» 04 2022 г.

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цели и задачи освоения учебной дисциплины (модуля)

Цель: изучения дисциплины является подготовка студентов к освоению организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, ознакомление с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение способов применения методов защиты информации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

Задачи:

- определение места дисциплины в предметном блоке, ее взаимосвязи с другими дисциплинами учебного плана специальности;
- раскрытие специфики защиты компьютерных сетей как объекта научного исследования;
- определение основных этапов и базовых концептуальных подходов к созданию систем защиты компьютерных сетей в рамках исторического развития отечественной и зарубежной науки;
- знакомство со способами и особенностями создания систем защиты компьютерных сетей на различных уровнях взаимодействия с окружением;
- приобретение студентами навыков аналитического и эмпирического исследования систем компьютерной защиты сетей;
- выработка целостного представления о различных аспектах строения и функционирования систем компьютерной защиты сетей на всех ее уровнях;
- рост навыков в сфере создания систем компьютерной защиты сетей и умения применять полученные знания на практике.

1.2. Место дисциплины (модуля) в структуре образовательной программы направления подготовки

Учебная дисциплина «Методы защиты и преобразования информации» относится к вариативной части блока «Дисциплин (модулей)» Б1. Изучение учебной дисциплины «Методы защиты и преобразования информации» базируется на знаниях, умениях и навыках, полученных студентами при изучении дисциплин: «Информатика», «Архитектура компьютеров», «Вычислительные системы, сети и телекоммуникации».

Изучение учебной дисциплины необходимо для освоения таких дисциплин, как «Криптография», «Информационные технологии в инженерной деятельности», «Администрирование в информационных системах» и производственной практики «Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности».

1.3. Требования к результатам освоения учебной дисциплины (модуля)

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций:

Универсальные (УК), общепрофессиональные (ОПК), профессиональные (ПК) – в соответствии с ФГОС 3++.

Код компетенции	Содержание компетенции	Индикаторы достижения компетенции
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	Знает: основы математики, физики, вычислительной техники и программирования. Умеет: решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования. Владеет: навыками теоретического и экспериментального исследования объектов профессиональной деятельности
ОПК-5	Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	Знает: методы защиты программ от вирусов и вредоносных программ; о направлениях и перспективах развития защиты информации Умеет: применять методы защиты компьютерных сетей при проектировании АСОИУ в различных предметных областях. Владеет: навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Объем учебной дисциплины (модуля).

Объем дисциплины «Методы защиты и преобразование информации» составляет 5 зачетных единиц/ 180 часов:

Вид учебной работы	**Всего, часов**	**Очная форма**	**Очная форма**
		Курс, часов	**Курс, часов**
	Очная форма	3 курс, 5 семестр	3 курс, 6 семестр
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:		34	48
Лекции (Л)	24	10	14
В том числе, практическая подготовка (ЛПП)			
Практические занятия (ПЗ) ***(в том числе зачет)***	58	24	34
В том числе, практическая подготовка (ПЗПП)			
Лабораторные работы (ЛР)			
В том числе, практическая подготовка (ЛРПП)			
Самостоятельная работа обучающихся (СР)	62	38	24
В том числе, практическая подготовка (СРПП)			
Промежуточная аттестация (подготовка и сдача), всего:	36		36
Контрольная работа			
Курсовая работа			
Экзамен	36		36
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	180	72	108

2.2. Содержание разделов учебной дисциплины (модуля)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Защита информации. Основные понятия	Информационные ресурсы и документирование информации Безопасность информационных ресурсов. Государственные информационные ресурсы.	ОПК-1 ОПК-5

	и определения	Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования. Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.	
2.	Изучение источников, рисков и форм атак на информацию в АСОИУ, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в АСОИУ	Изучение источников, рисков и форм атак на информацию в АСОИУ, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в АСОИУ. Классификация угроз и меры по обеспечению сохранности информации в АСОИУ. Классификация рисков и основные задачи обеспечения безопасности информации в АСОИУ. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения АСОИУ и угрозы исходящие от использования «электронной почты».	ОПК-1 ОПК-5
3.	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в АСОИУ	Законодательная, нормативно-методическая и научная база систем защиты информации. Требования к содержанию нормативно-методических документов по защите информации. Российское законодательство по защите информационных технологий. Политика безопасности. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в АСОИУ.	ОПК-1 ОПК-5
4.	Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности	Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Доктрина информационной безопасности Российской Федерации. Классификация защищенности средств вычислительной техники. Международные стандарты по защите информации. Стандарты безопасности в Интернете.	ОПК-1 ОПК-5
5.	Криптографические модели. Симметричные и ассиметричных криптосистемы для	Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки.	ОПК-1 ОПК-5

	защиты компьютерной информации в АСОИУ	Блочные и поточные шифры. Методы генерации псевдослучайных последовательностей чисел.	
6.	Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем	Стандартные алгоритмы шифрования. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов. Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Безопасность и быстродействие криптосистемы RSA. Изучение американского стандарта шифрования данных DES. Основные режимы работы алгоритма DES. Отечественный стандарт шифрования данных.	ОПК-1 ОПК-5
7.	Методы идентификации и проверки подлинности пользователей компьютерных систем	Основные понятия и концепции идентификации и проверки подлинности пользователей компьютерных систем. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы цифровой подписи. Отечественный стандарт цифровой подписи. Биометрические средства идентификации пользователей.	ОПК-1 ОПК-5
8.	Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet	Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Internet.	ОПК-1 ОПК-5
9.	Защита информации в компьютерных сетях, антивирусная защита	Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации в Internet.	ОПК-1 ОПК-5
10.	Требования к системам информационной защиты АСОИУ. Организационные требования к	Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита	ОПК-1 ОПК-5

	системам информационной защиты АСОИУ.	информационной безопасности АСОИУ и предприятия в целом.	

2.3. Разделы дисциплины и виды занятий

Очная форма обучения

№ п/п	Наименование раздела (темы)	Аудиторная работа		Внеауд. работа	Объем в часах
		Л	ПЗ/ЛР	СР	Всего
		в том числе, ЛПП	в том числе, ПЗПП/ЛРПП	в том числе, СРПП	в том числе, ПП
5 семестр					
	РАЗДЕЛ 1. Защита информации. Основные понятия и определения				
	1. Информационные ресурсы и документирование информации Безопасность информационных ресурсов. Государственные информационные ресурсы. Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования. Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.	2	6	8	16
	Итого:	2	6	8	16
	В том числе ПП:				
	РАЗДЕЛ 2. Изучение источников, рисков и форм атак на информацию в АСОИУ, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в АСОИУ				
	1. Изучение источников, рисков и форм атак на	2	4	8	14

	информацию в АСОИУ, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в АСОИУ. Классификация угроз и меры по обеспечению сохранности информации в АСОИУ. Классификация рисков и основные задачи обеспечения безопасности информации в АСОИУ. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения АСОИУ и угрозы исходящие от использования «электронной почты».				
	Итого:	2	4	8	14
	В том числе ПП:				
	РАЗДЕЛ 3. Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в АСОИУ				
	1. Законодательная, нормативно-методическая и научная база систем защиты информации. Требования к содержанию нормативно-методических документов по защите информации. Российское законодательство по защите информационных технологий. Политика безопасности. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в АСОИУ.	2	*4*	8	14
	Итого:	2	*4*	8	14
	В том числе ПП:				
	РАЗДЕЛ 4. Международные и Государственные стандарты				

	информационной безопасности и их использование в практической деятельности				
	1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Доктрина информационной безопасности Российской Федерации. Классификация защищенности средств вычислительной техники. Международные стандарты по защите информации. Стандарты безопасности в Интернете.	2	4	6	12
	Итого:	2	*4*	6	12
	В том числе ПП:				
	РАЗДЕЛ 5. Криптографические модели. Симметричные и ассиметричных криптосистемы для защиты компьютерной информации в АСОИУ				
	1. Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Методы генерации псевдослучайных последовательностей чисел.	2	6	8	16
	Итого:	2	*6*	8	16
	В том числе ПП:				
6 семестр					
	РАЗДЕЛ 6. Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем				
	1. Стандартные алгоритмы шифрования. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов. Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Безопасность и	2	6	4	12

	быстродействие криптосистемы RSA. Изучение американского стандарта шифрования данных DES. Основные режимы работы алгоритма DES. Отечественный стандарт шифрования данных.				
	Итого:	2	*6*	4	12
	В том числе ПП:				
	РАЗДЕЛ 7. Методы идентификации и проверки подлинности пользователей компьютерных систем				
	1. Основные понятия и концепции идентификации и проверки подлинности пользователей компьютерных систем. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы цифровой подписи. Отечественный стандарт цифровой подписи. Биометрические средства идентификации пользователей.	2	6	4	12
	Итого:	2	*6*	4	12
	В том числе ПП:				
	РАЗДЕЛ 8. Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet				
	1. Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных	2	6	4	12

	корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Internet.				
	Итого:	2	*6*	4	12
	В том числе ПП:				
	РАЗДЕЛ 9. Защита информации в компьютерных сетях, антивирусная защита				
	1. Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации в Internet.	4	8	6	18
	Итого:	4	*8*	6	
	В том числе ПП:				
	РАЗДЕЛ 10. Требования к системам информационной защиты АСОИУ. Организационные требования к системам информационной защиты АСОИУ.				
	1. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита	4	8	6	18

	информационной безопасности АСОИУ и предприятия в целом.				
	Итого:	4	*8*	6	18
	В том числе ПП:				
	Всего:	24	58	62	144
	В том числе ПП:				

2.4. План самостоятельной работы обучающегося по дисциплине (модулю)

Очная форма обучения

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость (часов)	Формируемые компетенции	Формы контроля
1.	Защита информации. Основные понятия и определения	Самоподготовка Самостоятельное изучение разделов	8	ОПК-1 ОПК-5	Устный опрос, проверка задания
2.	Изучение источников, рисков и форм атак на информацию в АСОИУ, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в АСОИУ	Самоподготовка Самостоятельное изучение разделов	8	ОПК-1 ОПК-5	Устный опрос, проверка задания
3.	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в АСОИУ	Самоподготовка Самостоятельное изучение разделов	8	ОПК-1 ОПК-5	Устный опрос, проверка задания
4.	Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности	Самоподготовка Самостоятельное изучение разделов	6	ОПК-1 ОПК-5	Устный опрос, проверка задания
5.	Криптографические модели. Симметричные и ассиметричных криптосистемы для защиты компьютерной	Самоподготовка Самостоятельное изучение разделов	8	ОПК-1 ОПК-5	Устный опрос, проверка задания

	информации в АСОИУ				
6.	Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем	Самоподготовка Самостоятельное изучение разделов	4	ОПК-1 ОПК-5	Устный опрос, проверка задания
7.	Методы идентификации и проверки подлинности пользователей компьютерных систем	Самоподготовка Самостоятельное изучение разделов	4	ОПК-1 ОПК-5	Устный опрос, проверка задания
8.	Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet	Самоподготовка Самостоятельное изучение разделов	4	ОПК-1 ОПК-5	Устный опрос, проверка задания
9.	Защита информации в компьютерных сетях, антивирусная защита	Самоподготовка Самостоятельное изучение разделов	6	ОПК-1 ОПК-5	Устный опрос, проверка задания
10.	Требования к системам информационной защиты АСОИУ. Организационные требования к системам информационной защиты АСОИУ.	Самоподготовка Самостоятельное изучение разделов	6	ОПК-1 ОПК-5	Устный опрос, проверка задания
		Экзамен	36		Экзамен

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

При организации обучения студентов с инвалидностью и ОВЗ (ПОДА) обеспечиваются следующие необходимые условия:

- учебные занятия организуются исходя из психофизического развития и состояния здоровья лиц с ОВЗ совместно с другими обучающимися в общих группах, а также индивидуально, в соответствии с графиком индивидуальных занятий;

- при организации учебных занятий в общих группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе;

- в процессе образовательной деятельности применяются материально-техническое оснащение, специализированные технические средства приема-передачи учебной информации в доступных формах для студентов с различными нарушениями, электронные образовательные ресурсы в адаптированных формах.

- подбор и разработка учебных материалов преподавателями производится с учетом психофизического развития и состояния здоровья лиц с ОВЗ;

- используются элементы дистанционного обучения при работе со студентами, имеющими затруднения с моторикой;

- при необходимости студенты с инвалидностью и ОВЗ обеспечиваются текстами конспектов (при затруднении с конспектированием);

- при проверке усвоения материала используются методики, не требующие выполнения рукописных работ или изложения вслух (при затруднениях с письмом и речью).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

- инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);
- доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);
- доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно, др.).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа студентов представляет собой обязательный вид деятельности, обеспечивающий успешное освоение образовательной программы высшего образования в соответствии с требованиями ФГОС.

Самостоятельная работа в рамках образовательного процесса решает следующие задачи:

- закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий;
- приобретение дополнительных знаний и навыков по изучаемой дисциплине;
- формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;
- развитие навыков самоорганизации;
- формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;
- выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Основными принципами организации самостоятельной работы являются:

- принцип обратной связи, позволяющий осуществлять контроль и коррекцию действий студента;
- принцип развития интеллектуального потенциала студента (формирование алгоритмического, наглядно-образного, теоретического стилей мышления, умений принимать оптимальные или вариативные решения в сложной ситуации, умений обрабатывать информацию);

- принцип обеспечения целостности и непрерывности обучения (предоставление возможности последовательного выполнения заданий в пределах темы, дисциплины).

Основными видами самостоятельной работы по данной дисциплине являются подготовка к практическому занятию, подготовка к контрольной работе, подготовка к тесту, подготовка к экзамену.

Подготовка к практическому занятию требует поиска дополнительной информации по теме, которой будет посвящено занятие, что позволяет глубже разобраться в изучаемых вопросах и сформировать навык самостоятельного информационного поиска и анализа подобранного материала. При подготовке к практическим занятиям студенту рекомендуется придерживаться следующего порядка:

- внимательно изучить основные вопросы темы практического занятия, определить место темы занятия в общем содержании, ее связь с другими темами;
- найти и проработать соответствующие разделы в рекомендованных учебниках, нормативных документах и дополнительной литературе;
- после ознакомления с теоретическим материалом ответить на вопросы для самопроверки;
- продумать свое понимание сложившейся ситуации в изучаемой сфере, пути и способы решения проблемных вопросов;
- продумать развернутые ответы на предложенные вопросы темы, опираясь на лекционные материалы, расширяя и дополняя их данными из учебников, дополнительной литературы.

Подготовка к контрольной работе. Контрольная работа проводиться после изучения определенной темы (тем) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя:

- изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой;
- повторение учебного материала, полученного при подготовке к практическим занятиям и во время их проведения;
- изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний.

Подготовка к тестированию. Тестирование – это не только форма контроля, но и метод углубления, закрепления знаний обучающихся. Задача тестирования - добиться глубокого изучения отобранного материала, пробудить у обучающегося стремление к изучению дополнительной литературы. Подготовка включает в себя изучение рекомендованной литературы, лекционного материала, конспектирование дополнительных источников. Чтение и запоминание текста индивидуально. Желательно сначала прочитать текст целиком, потом выделить в нем главные мысли, разделить текст на части, составить план текста, выделить логическую связь между этими пунктами и потом еще раз перечитать и пересказать.

Подготовка к опросу включает в себя повторение пройденного материала по теме предстоящего опроса. Помимо основного материала студент должен изучить дополнительную рекомендованную литературу и информацию по теме, в том числе с использованием Интернет-ресурсов. Опрос предполагает устный ответ студента на один основной и несколько дополнительных вопросов преподавателя. Ответ студента должен представлять собой развёрнутое, связанное, логически выстроенное сообщение. При выставлении оценки преподаватель учитывает правильность ответа по содержанию, его последовательность, самостоятельность суждений и выводов, умение связывать теоретические положения с практикой, в том числе и с будущей профессиональной деятельностью.

Подготовка к экзамену. Подготовка к экзамену осуществляется на протяжении всего периода освоения учебной дисциплины, но непосредственную подготовку в период промежуточной аттестации целесообразно осуществлять в два этапа. На первом из разных источников подбирается весь материал, необходимый для развернутых ответов на все вопросы. При ознакомлении с каким-либо разделом учебника рекомендуется прочитать его целиком, стараясь уловить логику и основную мысль автора. При вторичном чтении лучше акцентировать внимание на основных, ключевых вопросах темы. Можно составить краткий конспект, что позволит изученный материал быстро освежить в памяти перед экзаменом. Конспектирующему следует выделять понятия, категории, законы, принципы, идеи выводы, факты и т. д. Затем выявляются связи и отношения между этими компонентами текста. Технологические приемы конспектирования: выписки цитат; пересказ своими словами; выделение идей и теорий; критические замечания; уточнения; собственные разъяснения; сравнивание позиций; реконструкция текста в виде создания таблиц, рисунков, схем; описание связей и отношений; введение дополнительной информации и др. Хороший конспект отличается краткостью - не более 1/8 первичного текста, целевой направленностью, научной корректностью, ясностью, четкостью, понятностью. Важно отметить сложные и непонятные места, чтобы на консультации задать вопрос преподавателю. На втором этапе по памяти восстанавливается содержание того, что записано в ответах на каждый вопрос.

Контроль самостоятельной работы студента осуществляется посредством текущего и промежуточного контроля. Текущий контроль осуществляется на практических занятиях в ходе проверки отдельных видов самостоятельной работы, выполненной студентами.

Промежуточный контроль самостоятельной работы осуществляется в ходе промежуточной аттестации обучающихся.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся – не предусмотрены.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.
Текущий контроль – устный опрос, проверка задания.
Промежуточная аттестация – зачет, экзамен.

6.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрено.

6.3. Курсовая работа

Не предусмотрено.

6.4. Вопросы к зачету

1. Понятие информационной безопасности. Характеристики информации с позиции безопасности.
2. Классификация угроз безопасности информации.

3. Классификация угроз безопасности распределенных вычислительных систем
4. Модель OSI.
5. Объясните понятие «политика безопасности организации».
6. Какие разделы должна содержать документально оформленная политика безопасности?
7. Какие проблемы решает верхний уровень политики безопасности?
8. Какие задачи решает средний уровень политики безопасности?
9. Каковы особенности нижнего уровня политики безопасности?
10. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
11. Назовите основные международные стандарты информационной безопасности.
12. Дайте краткую характеристику международного стандарта 17799 (BS 7799).
13. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности».
14. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
15. Назовите стандарты информационной безопасности для Internet.

6.5. Вопросы к экзамену

1. Понятие информационной безопасности. Характеристики информации с позиции безопасности.
2. Классификация угроз безопасности информации.
3. Классификация угроз безопасности распределенных вычислительных систем
4. Модель OSI.
5. Объясните понятие «политика безопасности организации».
6. Какие разделы должна содержать документально оформленная политика безопасности?
7. Какие проблемы решает верхний уровень политики безопасности?
8. Какие задачи решает средний уровень политики безопасности?
9. Каковы особенности нижнего уровня политики безопасности?
10. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
11. Назовите основные международные стандарты информационной безопасности.
12. Дайте краткую характеристику международного стандарта 17799 (BS 7799).
13. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности».
14. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
15. Назовите стандарты информационной безопасности для Internet.
16. Каковы назначение и особенности функционирования протокола SET.
17. Каковы назначение и функциональность протоколов SSL и IPSec.
18. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408. Назовите и охарактеризуйте три основные части этого стандарта.
19. Обобщенная схема криптосистемы шифрования
20. Классификация криптографических алгоритмов

21. Схема симметричной криптосистемы шифрования
22. Алгоритм шифрования DES и 3DES
23. Стандарт шифрования ГОСТ 28147-89
24. Стандарт шифрования AES
25. Режимы работы блочного симметричного алгоритма
26. Дайте определение однонаправленной функции. Каковы особенности однонаправленных функции.
27. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
28. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш-функция?
29. Дать определение понятия «идентификация», «аутентификация», «авторизация», «администрирование».
30. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
31. Опишите метод аутентификации на основе мно призовых паролей. Каковы его недостатки?
32. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
33. Сформулируйте принцип строгой аутентификации.
34. Объясните назначение PIN-кода и особенности его использования.
35. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используют для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

1. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3 - Текст : электронный. - URL: https://znanium.com/catalog/product/1018901
2. Введение в криптографию. Курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 240 с. — (Высшее образование: Бакалавриат). - Текст : электронный. - URL: https://znanium.com/catalog/product/1018899
3. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 592 с. — (Высшее образование: Бакалавриат). - Текст : электронный. - URL: https://znanium.com/catalog/product/996789
4. Моделирование системы защиты информации. Практикум : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2018. — 224 с. + Доп. материалы [Электронный ресурс; Режим доступа: http: //www.znanium.com]. — (Высшее образование: Бакалавриат). — DOI: https://doi.org/10.12737/18877 - Текст : электронный. - URL: https://znanium.com/catalog/product/916068

7.2. Дополнительная литература

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/444046

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433715

7.3. Программное обеспечение

Сетевой компьютерный класс, оснащенный современной техникой

1. Офисный программный пакет (например, Microsoft Office 2007 или более поздних версий).
2. Web-браузер Mozilla Firefox или Google Chrome
3. Экран для проектора

7.4. Электронные ресурсы

1. Национальный открытый университет ИНТУИТ [Электронный ресурс]. URL: http://www.intuit.ru
2. Хабрахабр [Электронный ресурс]. URL: http://habrahabr.ru/
3. Электронная библиотека «Знаниум»: https://znanium.com/
4. Электронная библиотека «Юрайт»: https://urait.ru/
5. Научная электронная библиотека «Elibrary.ru»: https://www.elibrary.ru/defaultx.asp

7.5. Методические указания и материалы по видам занятий

1. Автоматика и Телемеханика / Automation and Remote.
2. Автоматика, связь, информатика.
3. Безопасность информационных технологий.
4. Бизнес-информатика.
5. Вестник кибернетики (электронный журнал).
6. Вестник компьютерных и информационных технологий.
7. Вопросы защиты информации.
8. Вопросы кибербезопасности.
9. Геоинформатика/Geoinformatika.
10. Информатизация образования и науки.
11. Информатизация и связь.
12. Информатика и ее применения.
13. Информатика и образование.
14. Информатика и системы управления.
15. Информационное общество.
16. Информационное право.
17. Информационно-измерительные и управляющие системы.
18. Информационно-управляющие системы.
19. Информационные ресурсы России.
20. Информационные системы и технологии.
21. Информационные и телекоммуникационные технологии.
22. Информационные технологии.

23. Информационные технологии в проектировании и производстве.
24. Информационные технологии и вычислительные системы.
25. Информация и безопасность.
26. Информация и космос.
27. Компьютерная оптика.
28. Компьютерные инструменты в образовании.
29. Компьютерные исследования и моделирование.
30. Математическая биология и биоинформатика (электронное научное издание).

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Измененные пункты	Решение Учебно-методического совета