МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Димитровградский инженерно-технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(ДИТИ НИЯУ МИФИ)

УТВЕРЖДАЮ:
Заместитель руководителя
_____Т.И. Романовская

«____» _____2020г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Направление подготовки *09.03.01 Информатика и вычислительная техника*

Квалификация выпускника *Бакалавр*

Профиль *Программное обеспечение средств вычислительной техники и автоматизированных систем*

Форма обучения *очная*

Выпускающая кафедра *Кафедра информационных технологий*

Кафедра-разработчик рабочей программы *Кафедра информационных технологий*

Семестр	Трудоемкость час. (ЗЕТ)	Лекций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз., час./зачет)
7	72 (2)	17	17	17	21	зачет
Итого	**72 (2)**	**17**	**17**	**17**	**21**	

Димитровград
2020 г.

СОДЕРЖАНИЕ

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 3
2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО 3
3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ 5
4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 6
5 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 9
6 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ВХОДНОГО И ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ И ИТОГОВОЙ АТТЕСТАЦИИ (АННОТАЦИЯ) 9
7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 10
8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 10
9 ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ 12

1 ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины «Защита информации»:

- основных положений в области безопасности информации;
- сервисов обеспечения безопасности информации в автоматизированных системах;
- программно-аппаратных средств защиты информации;
- моделей разграничения доступа;
-организационных мер по защите информации;
- основных положений криптографии;
- алгоритмов шифрования;
- инфраструктуры открытых ключей;
- стадий и принципов построения автоматизированных систем в защищенном исполнении;
- распространенных угроз информационной безопасности;
- стандартов и положений в области защиты информации.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина *Защита информации* относится к *базовой* части блока *Б1 профессионального* модуля учебного плана.

Для изучения учебной дисциплины необходимы знания, умения и готовности, сформированные у обучающихся в результате освоения дисциплин вузовской образовательной программы по технологии программирования, структурам данных, управлению данными, моделированию систем, администрированию в информационных системах.

Знания, полученные при изучении дисциплины, помогут студентам в научно-исследовательской работе и дипломном проектировании, а также в дальнейшей профессиональной деятельности.

Таблица 2.1 – Перечень предшествующих и последующих дисциплин, формирующих общекультурные и профессиональные компетенции

Код	**Наименование компетенции**	**Предшествующие дисциплины**	**Последующие дисциплины (группы дисциплин)**
ДК-7	использовать ЭВМ для управления и обработки информации	Информатика Программирование Основы моделирования систем Программирование на Delphi	
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Физика Информатика Сети и телекоммуникации Дискретная математика Математическое программное обеспечение Исследование операций Математическая логика и теория алгоритмов Мультимедийные технологии Вычислительная мате-	Технология разработки программного обеспечения Производственная практика (преддипломная) Итоговая государственная аттестация

		матика Численные методы в автоматизированных системах Методы оптимизации Дискретные структуры Структуры и алгоритмы обработки данных Современные среды визуального программирования Компьютерное моделирование Имитационное моделирование Технологии программирования в сетях Производственная (технологическая)	
ПК-3	способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности;	Метрология, стандартизация и сертификация Основы научных исследований Компьютерная графика Теория вероятностей и математическая статистика Производственная (технологическая)	Производственная практика (преддипломная)

3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины «Защита информации» направлен на формирование элементов компетенций в соответствии с ОС НИЯУ МИФИ и ОП ВО по данному направлению подготовки.

Таблица 3.1 - Перечень планируемых результатов обучения по дисциплине

Планируемые результаты освоения ОП (компетенции), достижение которых обеспечивает дисциплина		Перечень планируемых результатов обучения по дисциплине
Код компетенции	Содержание компетенции	
ДК-7	использовать ЭВМ для управления и обработки информации	**знать:** программно-аппаратные средств защиты информации; **уметь:** разрабатывать и создавать типовые схемы защиты информации на основе современных средств защиты информации; **владеть:** методами выявления и анализа способов нарушения безопасности информации;
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	**знать:** правовые основы защиты компьютерной информации, организационные, технические и программные методы и средства защиты информации в АСОИУ и ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; иметь представление о направлениях развития и перспективах защиты информации; **уметь:** применять методы защиты компьютерной информации при проектировании и эксплуатации АСОИУ и ИС в различных предметных областях; **владеть:** установки и настройки программного обеспечения, применяемого для защиты АСОИУ и ИС от несанкционированного доступа, как из сетей общего пользования, так и внутренних сетей предприятия.
ПК-3	способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности;	**знать:** распространённые организационные мер по защите информации; **уметь:** пользоваться стандартами, нормативными правовыми актами из области безопасности информации при проектировании систем защиты. **владеть:** подходами при построении автоматизированных систем в защищенном исполнении.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Структура дисциплины

Таблица 4.1

Объём дисциплины по видам учебных занятий

Вид учебной работы	Всего, зачетных единиц (акад. часов)	Семестр
Общая трудоемкость дисциплины	**108 (3)**	**7**
Контактная работа с преподавателем:		
занятия лекционного типа	**17**	
занятия семинарского типа		
в том числе: семинары		
практические занятия		
практикумы		
лабораторные работы	**34**	
другие виды контактной работы		
в том числе: курсовое проектирование		
Самостоятельная работа обучающихся:**	**57**	
изучение теоретического курса		
расчетно-графические задания, задачи		
реферат, эссе		
курсовое проектирование		
Подготовка к экзамену		
Вид промежуточной аттестации	**зачет**	

Распределение учебной нагрузки по разделам дисциплины

Таблица 4.2

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, акад. часы					Формируемые компетенции
		Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего часов	
1	Раздел 1. Основы информационной безопасности.	4		6	12	22	ДК-7 ОПК-5 ПК-3
2	Раздел 2. Криптографические методы и средства информационной безопасности.	6		18	20	44	ДК-7 ОПК-5 ПК-3
3	Раздел 3. Методы защиты информации от несанкционированного доступа.	4		10	16	30	ДК-7 ОПК-5 ПК-3
4	Раздел 4. Информационная безопасность в компьютерных сетях.	3			9	12	ДК-7 ОПК-5 ПК-3

ИТОГО:	17		34	57	108	

4.2 Содержание дисциплины

Удельный вес проводимых в активных и интерактивных формах проведения аудиторных занятий по дисциплине составляет 30 %.

Лекционный курс

Таблица 4.3

№ лекции	Номер раздела	Тема лекции и перечень дидактических единиц	Трудоемкость, акад. часов	
			всего	в том числе с использованием интерактивных образовательных технологий
1	1	**Основные понятия и подходы информационной безопасности.** Угрозы информационной безопасности. Классификация нарушителей информационной безопасности. Каналы утечки информации. Основные понятия политики безопасности. Структура политики безопасности. Стандарты и спецификации информационной безопасности. Международные и отечественные стандарты информационной безопасности Критерии оценки надежности компьютерных систем. Требования к системам защиты информации.	2	2
2	1	**Подходы к защите информации в ОС.** Защита информации от несанкционированного доступа в ОС Windows. Управление доступом к объектам в ОС. Подсистема безопасности ОС Windows. Защита информации в ОС Linux. Аудит событий в ОС.	2	
3	2	**Криптографические методы.** Основные определения криптографии и стеганографии. Понятие криптоанализа. Классификация криптографических методов защиты информации. Понятие криптографического протокола. Симметричные алгоритмы. Ассиметричные алгоритмы. Подстановочные и перестановочные шифры. Алгоритмы шифрования.	2	2
4	2	**Симметричные криптосистемы.** Сеть Фейштеля. Алгоритм DES. Стандарт шифрования AES. Стандарт шифрования ГОСТ 28147-89. Алгоритм Blowfish.	2	2
5	2	**Асимметричные криптосистемы.** Системы с открытым ключом. Алгоритм шифрования RSA. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических кривых. Алгоритмы обмена ключами.	2	2
6	3	**Электронно-цифровая подпись.** Алгоритмы электронно-цифровой подписи. Однонаправленные хеш-функции. Хеш-функция MD4. Хеш-функция MD5. Хеш-функция SHA. Требования к хеш-функциям. Стойкость хеш-функций.	2	2
7	3	**Идентификация и проверка подлинности.** Способы несанкционированного доступа к информации. Идентификация и аутентификация пользователя. Алгоритма аутентифи-	2	2

		кации и идентификации пользователя. Проверка подлинности пользователей.		
8	4	**Безопасность сетевых технологий.** Способы несанкционированного доступа к информации в компьютерных сетях. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Режим функционирования межсетевых экранов и их основные компоненты. Применение межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов.	2	
9	4	**Средства обнаружения атак.** Методы анализа сетевой информации. Классификация систем обнаружения атак. Классификация и архитектура систем обнаружения атак.	1	
		Итого:	**17**	**12**

Практические занятия *учебным планом не предусмотрены*

Лабораторные работы

Таблица 4.4

№ занятия	Номер раздела	Наименование лабораторной работы и перечень дидактических единиц	Трудоемкость, акад. часов	
			всего	в том числе с использованием интерактивных образовательных технологий
Семестр 8				
1, 2	1	ЛР№1 Основы систем счисления	2	
3	1	Защита отчета	2	
4, 5	2	ЛР№2 Криптографические методы преобразования информации	2	
6	2	Защита отчета	2	
7, 8	2	ЛР№3 Симметричные криптографические алгоритмы	4	
9	2	Защита отчета	2	
10	2	Проверочная работа №1	2	
11	2	ЛР№4 Асимметричные криптографические алгоритмы	4	
12	2	Защита отчета	2	
13	3	ЛР№5 Алгоритм электронно-цифровой подписи	4	
14	3	Защита отчета	2	
15	3	Проверочная работа №2	2	
16	3	ЛР№6 Алгоритмы аутентификации	2	
17	3	Защита отчета	2	
		Итого:	**34**	

Самостоятельная работа студента

Таблица 4.5

Раздел дисципли-	№ п/п	Вид самостоятельной работы студента (СРС) и перечень дидактических единиц	Трудоемкость, часов

ны			
1	1.1	Изучение теоретического материала по разделу 1	6
	1.2	Оформление и защита отчетов по лабораторно работе №1.	6
2	2.1	Изучение теоретического материала по разделу 2	6
	2.2	Оформление и защита отчетов по лабораторным работам №2, 3, 4	12
	2.3	Подготовка к проверочной работе №1	6
3	3.1	Изучение теоретического материала по разделу 3	6
	3.2	Оформление и защита отчетов по лабораторным работам №5, 6	5
	3.3	Подготовка к проверочной работе №2	5
4	4.1	Изучение теоретического материала по разделу 4	5
		ИТОГО:	**57**

5 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе преподавания дисциплины «Защита информации» рекомендуется применять следующие методы обучения:

- словесные лекции;
- интерактивные лекции;
- практические работы;

Лекционный курс рекомендуется читать по утвержденной рабочей программе.

При закреплении полученных знаний на примерах и упражнениях, можно использовать такие виды обучения как объяснительно-иллюстративный (на примерах применения анализа), репродуктивный (если у студентов возникают вопросы по примерам) и исследовательский. Кроме того, положительно влияет на процесс закрепления пройденного материала проблемное изложение ситуаций и частично-поисковая форма их решения.

Кроме этого, на контрольных занятиях студентам по их желанию предлагается вместо стандартного варианта задания выполнить два или даже одно «трудное» задание. Для выполнения этих заданий знание основного материала необходимо, но далеко недостаточно.

Применение любой формы обучения предполагает также использование новейших IT-обучающих технологий.

6 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ВХОДНОГО И ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ И ИТОГОВОЙ АТТЕСТАЦИИ (АННОТАЦИЯ)

Входной контроль осуществляется в форме тестирования с целью определения базовых знаний студента и выявления разделов дисциплины, вызывающих наибольшие затруднения у студентов.

Контроль освоения дисциплины производится в соответствии с Положением о рейтинговой системе оценки знаний студентов ДИТИ НИЯУ МИФИ.

Текущий контроль студентов по дисциплине производится в дискретные временные интервалы в следующих формах:

- выполнение лабораторных работ;
- защита лабораторных работ;
- устные опросы;

Дополнительно оцениваются личностные качества студента: умение работать в коллективе, своевременная сдача тестов, выполнение и защита лабораторных работ, выполнение самостоятельной работы.

Промежуточный контроль студентов производится в форме тестирования:

Итоговый контроль по дисциплине проходит в форме устного опроса по экзаменационным билетам, включающим в себя ответ на теоретический вопрос, решение задач, выполнение практического задания на ПК.

Фонды оценочных средств, включают в себя типовые задания, тесты и методы контроля, позволяющие оценить результаты обучения по данной дисциплине, перечислены в Приложении.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 7.1 - Обеспечение дисциплины основной и дополнительной литературой по дисциплине

N п/п	Автор	Название	Место издания	Наименование издательства	Год издания	Количество экземпляров
Основная литература						
1	Барабанова М.И., Кияев В.И.	Информационные технологии: открытые системы, сети, безопасность в системах и сетях	СПб	СПбГУЭФ	2010	1
	Партыка Т.П., Попов И.И.	Информационная безопасность	М	ФОРУМ	2010	1
Дополнительная литература						
1	Галатенко В.А.	Основы информационной безопасности	М	ИНТУИТ	2006	1
2	Соколов А.В., Шаньгин В.Ф.	Защита информации в распределенных корпоративных сетях и системах	М	ДМК Пресс	2002	1
	Левин М.	Безопасность в сетях Internet и Intranet	М	Познавательная книга плюс	2001	1
	Ховард М., Лебланк Д.	Защищенный код	М	Русская Редакция	2005	1

7.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Электронная библиотечная система (ЭБС) Книгафонд *http://www.knigafund.ru/*
2. Центр информационно-библиотечного обеспечения учебно-научной деятельности НИЯУ МИФИ *http://www.library.mephi.ru/*
3. Научная электронная библиотека *http://elibrary.ru/defaultx.asp*
4. Электронно-библиотечная система «Лань» *http://elibrary.ru/defaultx.asp*

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Для проведения лекционных занятий используется:

• комплект электронных презентаций/слайдов;
• компьютерный класс, оснащенный презентационной техникой (проектор, интерактивная доска, компьютер).

2. *Для проведения лабораторных работ используется*:
• компьютерный класс, оснащенный презентационной техникой (проектор, интерактивная доска, компьютер);

9 ТЕХНОЛОГИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ

Технологическая карта рейтинговых баллов по дисциплине «Информационная безопасность»

Специальность 09.03.01 4 курс очное обучение (ЮнБ-11)

Максимальное количество баллов за работу в течение семестра: 60 баллов.

Итоговый контроль: 40 баллов

Семестр 7

Всего часов 108

в том числе:

1 лекции – 17 часов;

3 практические занятия – 34 часов;

3 подготовка к зачету – 57 часов.

Структура текущего и промежуточного контроля.

Информация о контр. точках	Текущий контроль(<=25) (ТК)									Промежуточный контроль (<=30) (ПК)		Форма итогового контроля
	$ТК_1$	$ТК_2$	$ТК_3$	$ТК_4$	$ТК_5$	$ТК_6$	$ТК_7$	$ТК_8$	$ТК_9$	$ПК_1$	$ПК_2$	
форма контроля	*Л//ЛЗ/ ЛР1*	*Л/ЛЗ/ ЛР2*	*Л/ЛЗ/ ЛР3*	*Л/ЛЗ*	*Л/ЛЗ/ ЛР4*	*Л/ЛЗ/ ЛР5*	*Л/ЛЗ*	*Л/ЛЗ/ ЛР6*	*Л/ЛЗ/ ЛР7*	$КР_1$	$КР_2$	*З*
неделя сдачи	2	4	6	8	10	12	14	16	18	8	14	
макс. балл	3	3	3	1	3	3	1	3	5	15	15	40

Структура баллов, начисляемых студентам по результатам текущего контроля (промежуточного контроля)

№ п/п	Наименование видов учебной работы и состояния учебной дисциплины студентов	Начисляемое количество баллов (долей баллов)	Максимальное количество баллов по данному виду учебной работы
1	Посещение лекций и лабораторных занятий	18 занятий по 0,5 балла	9
2	Выполнение лабораторных работ	6 лабораторных работ по 1 баллу 1 лабораторных работа по 2 балла	8
3	Защита лабораторных работ	6 лабораторных работ по 1 баллу 1 лабораторных работа по 2 балла	8
Максимальная сумма баллов по результатам текущего контроля			25

Ведущий преподаватель А. А. Аленин

(подпись И.О. Фамилия)

Сокращения: Л – лекция, ПЗ – практическое занятие, ПР – практическая работа, КР – контрольная работа.

Самостоятельная работа студента

Раздел дисциплины	№ п/п	Вид самостоятельной работы студента (СРС) и перечень дидактических единиц	Трудоемкость, часов
1	1.1	Изучение теоретического материала по разделу 1	6
	1.2	Оформление и защита отчетов по лабораторной работе №1.	6
2	2.1	Изучение теоретического материала по разделу 2	6
	2.2	Оформление и защита отчетов по лабораторным работам №2, 3, 4	12
	2.3	Подготовка к проверочной работе №1	6
3	3.1	Изучение теоретического материала по разделу 3	6
	3.2	Оформление и защита отчетов по лабораторным работам №5, 6	5
	3.3	Подготовка к проверочной работе №2	5
4	4.1	Изучение теоретического материала по разделу 4	5
		ИТОГО:	**57**

Ведущий преподаватель А.А. Аленин

(подпись И.О. Фамилия)

Сокращения: Л- лекция, ПЗ – практическое занятие, ДЗ домашнее задание, СР – самостоятельная работа, ПР – проверочная работа, ИЗ– типовой расчет, КР – контрольная работа

Приложение 1
к рабочей программе дисциплины
«Защита информации»

Аннотация рабочей программы

Дисциплина Б1.В.ДВ.12 Защита информации является частью профессионального модуля дисциплин подготовки студентов по направлению подготовки 09.03.01 Информатика и вычислительная техника. Дисциплина реализуется на информационно-технологическом факультете ДИТИ НИЯУ МИФИ кафедрой информационных технологий.

Дисциплина нацелена на формирование следующих компетенций выпускника:

ДК-7 – использовать ЭВМ для управления и обработки информации

ОПК-5 – способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-3 – способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности;

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации, организация мастер-классов представителей IT-компаний.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме выполнения, защиты лабораторных работ и устного опроса по изученной теме, промежуточный контроль в форме тестирования, написание реферата и итоговый контроль в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единиц, 108 часов. Программой дисциплины предусмотрены лекционные занятия в объеме 17 часов, лабораторные работы в объеме 34 часов и 57 часов самостоятельной работы студента.

Приложение 2
к рабочей программе дисциплины
«Защита информации»

Методические указания для самостоятельной работы обучающихся

При изучении дисциплины используется два вида самостоятельной работы студентов – аудиторная, под руководством преподавателя, и внеаудиторная. Тесная взаимосвязь этих видов работ предусматривает дифференциацию и эффективность результатов ее выполнения и зависит от организации, содержания, логики учебного процесса.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию. Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Основными видами самостоятельной работы студентов без участия преподавателей являются:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание рефератов;

– подготовка к лабораторным и контрольным работам, их оформление;

– подготовка лабораторных разработок;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-графических и курсовых работ (проектов) и т.д.

Для самостоятельного изучения и более глубокой проработки тем, которые не вошли в данный курс, студентам предлагается написать реферат. Реферат – творческая исследовательская работа, основанная, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования. Реферат должен быть написан на основе соответствующей литературы, которую студенты могут подобрать сами или с помощью преподавателя, и оформлен в соответствии с существующими стандартами. При написании реферата необходимо: изучить теоретическую литературу по предмету исследования, в развернутом виде представить историю и теорию вопроса, осветить основные положения темы реферата, указать разные точки зрения на предмет исследования, сделать выводы по теме исследования, обозначить перспективу изучения проблемы. Обязательно наличие библиографического списка, оформленного по ГОСТу и соответствующие ссылки внутри реферата.

Приложение 4
к рабочей программе дисциплины
«Защита информации»

Методические указания для студентов по освоению дисциплины

Трудоемкость освоения дисциплины составляет 108 часов, из них 51 час аудиторных занятий и 57 часов, отведенных на самостоятельную работу студента.

Вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторном занятии.
Самостоятельные задания	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.
Лабораторная работа	Методические указания по выполнению лабораторных работ по дисциплине «Защита информации»
Реферат	Реферат – творческая исследовательская работа, основанная, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования. При написании реферата необходимо: изучить теоретическую литературу по предмету исследования, в развернутом виде представить историю и теорию вопроса, осветить основные положения темы реферата, указать разные точки зрения на предмет исследования, сделать выводы по теме исследования, обозначить перспективу изучения проблемы. Реферат должен быть оформлен в соответствии с существующими стандартами.
Подготовка к зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и электронные источники.

Приложение 5
к рабочей программе дисциплины
«Защита информации»

ТЕХНОЛОГИИ И ФОРМЫ ПРЕПОДАВАНИЯ
Рекомендации по организации и технологиям обучения для преподавателя

I. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

Информационные технологии: использование электронных образовательных ресурсов при подготовке к лекциям, практическим и лабораторным занятиям.

Опережающая самостоятельная работа – изучение студентами нового материала до его изучения в ходе аудиторных занятий.

II. Виды и содержание учебных занятий

Раздел 1. Основы защиты компьютерной информации

Теоретические занятия (лекции) – 4 часа.

Лекция 1. Основные понятия и подходы информационной безопасности.

Угрозы информационной безопасности. Классификация нарушителей информационной безопасности. Каналы утечки информации. Основные понятия политики безопасности. Структура политики безопасности. Стандарты и спецификации информационной безопасности. Международные и отечественные стандарты информационной безопасности Критерии оценки надежности компьютерных систем. Требования к системам защиты информации.

Лекции 2. Подходы к защите информации в ОС.

Защита информации от несанкционированного доступа в ОС Windows. Управление доступом к объектам в ОС. Подсистема безопасности ОС Windows. Защита информации в ОС Linux. Аудит событий в ОС.

Лабораторные работы – 6 часов

Занятие 1, 2. ЛР№1 Основы систем счисления.

Занятие 3. Защита отчета.

Раздел 2. Криптографические методы и средства информационной безопасности.

Теоретические занятия (лекции) – 6 часов.

Лекции 3. Криптографические методы.

Основные определения криптографии и стеганографии. Понятие криптоанализа. Классификация криптографических методов защиты информации. Понятие криптографического протокола. Симметричные алгоритмы. Ассиметричные алгоритмы. Подстановочные и перестановочные шифры. Алгоритмы шифрования.

Лекция 4. Симметричные криптосистемы.

Сеть Фейштеля. Алгоритм DES. Стандарт шифрования AES. Стандарт шифрования ГОСТ 28147-89. Алгоритм Blowfish.

Лекция 5. Асимметричные криптосистемы.

Системы с открытым ключом. Алгоритм шифрования RSA. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических кривых. Алгоритмы обмена ключами.

Лабораторные работы – 18 часов.

Занятие 4, 5. ЛР№2 Криптографические методы преобразования информации.

Занятие 6. Защита отчета.

Занятие 7, 8. ЛР№3 Симметричные криптографические алгоритмы.

Занятие 9. Защита отчета.

Занятие 10. Проверочная работа №1.

Занятие 11. ЛР№4 Асимметричные криптографические алгоритмы.
Занятие 12. Защита отчета.

Раздел 3. Методы защиты информации от несанкционированного доступа.
Теоретические занятия (лекции) – 4 часов.

Лекции 6. Электронно-цифровая подпись.
Алгоритмы электронно-цифровой подписи. Однонаправленные хеш-функции. Хеш-функция MD4. Хеш-функция MD5. Хеш-функция SHA. Требования к хеш-функциям. Стойкость хеш-функций.

Лекция 7. Идентификация и проверка подлинности.
Способы несанкционированного доступа к информации. Идентификация и аутентификация пользователя. Алгоритма аутентификации и идентификации пользователя. Проверка подлинности пользователей.

Лабораторные работы – 10 часов.
Занятие 13. ЛР№5 Алгоритм электронно-цифровой подписи.
Занятие 14. Защита отчета
Занятие 15. Проверочная работа №2.
Занятие 16. ЛР№6 Алгоритмы аутентификации.
Занятие 17. Защита отчета.

Раздел 4. Информационная безопасность в компьютерных сетях.
Теоретические занятия (лекции) – 3 часов.

Лекции 8. Безопасность сетевых технологий.
Способы несанкционированного доступа к информации в компьютерных сетях. Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Режим функционирования межсетевых экранов и их основные компоненты. Применение межсетевых экранов. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов.

Лекция 9. Средства обнаружения атак.
Методы анализа сетевой информации. Классификация систем обнаружения атак. Классификация и архитектура систем обнаружения атак.