МИНПРОСВЕЩЕНИЯ РОССИИ
ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ТЕХНОЛОГИИ И ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКОГО ОБРАЗОВАНИЯ
КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ЭКОНОМИКИ И ДИЗАЙНА

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01 Модуль «Предметно-деятельностный»

Б1.В.01.01 Технологии и системы защиты информации

Направление подготовки *44.03.04 Профессиональное обучение*
Профиль подготовки *Информационные технологии*
Квалификация *Бакалавр*
Формы обучения: *очная; заочная*
Сроки обучения: *очно – 4; заочно – 4,5 года*

Форма обучения	Курс	Семестр	Количество часов					Форма итоговой аттестации (экз./зачет)
			Трудоемкость	Лекции	Лабораторные работы	Промежуточный контроль	СРС	
Очная	3	5	108	27	27		54	зачет
Заочная	3	5	108	6	6	3	93	зачет

Махачкала, 2021

Нурмагомедова Н.Х. Рабочая программа дисциплины «Технологии и системы защиты информации». – Махачкала: ДГПУ, 2021. – 22 с.

Рецензенты: Рагимханова Г.С. к.ф.-м.н., доцент кафедры информатики и ВТ ДГПУ

Эсетов Ф.А., к.п.н., доцент, зав. каф. информатики и ВТ

Программа утверждена на заседаниях:

кафедры информационных технологий, экономики и дизайна
протокол № 9 от «22» апреля 2021 г.

Зав. кафедрой Г.П. Раджабалиев;

ученого совета факультета Т и ППО
протокол № 9 от «28» апреля 2021 г.

Председатель совета Ф.Н. Алипханова;

учебно-методического совета ДГПУ
протокол № 4от «31» мая 2021 г.

Председатель УМС И.А.Дибиров

© ДГПУ, 2021
© Нурмагомедова Н.Х., 2021

I. Цель и задачи дисциплины

Целью дисциплины является формирование глубоких знаний и опыта у студентов по защите компьютерной информации, необходимого для успешной профессиональной деятельности в будущем.

Задачи дисциплины:

- усвоение студентами постановку и структуризацию проблем защиты информации, которые должны быть практически разрешены путем применения тех или иных технологий защиты информации;
- обучение практическим навыкам инсталляции программного обеспечения защиты информации.

II. Место дисциплины в структуре ОПОП

Дисциплина «Технологии и системы защиты информации» входит в вариативную часть учебного плана по направлению Профессиональное обучение, обязательной для изучения.

Для изучения дисциплины необходимы компетенции, сформированные у студентов в результате освоения дисциплин:

- математика;
- информатика;
- компьютерные технологии;
- информационные технологии.
- физические основы ЭВМ;

Знание материалов дисциплины необходимо при выполнении заданий научно-исследовательской, курсовой и выпускной квалификационной работ, учебной и производственной практик.

III. Требования к результатам освоения дисциплины

Процесс изучения дисциплины «Технологии и системы защиты информации» направлен на формирование следующих компетенций или их составляющих:

ПК-7. Готов применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов

Знает:

З-ПК-7.1.Основные понятия и методы теоретической информатики, его приложений, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов.

Умеет:

У-ПК-7.1.Применять основные понятия, методы теоретической информатики для анализа и синтеза информационных систем и процессов.

У-ПК-7.2.Решать задачи анализа и синтеза информационных систем и процессов с применением методов фундаментальной и прикладной математики.

Владеет:

В-ПК-7.1.Основными способами, методами анализа и синтеза информационных систем и процессов.

В-ПК-7.1.Технологиями решения задач анализа и синтеза информационных систем и процессов с применением методов фундаментальной и прикладной математики.

ПК-9. Готов оказать компьютерно-техническую и информационно-технологическую поддержку образовательной деятельности обучающихся

Знает:

З-ПК-9.1.Основы и методы использования аппаратного и программного обеспечения ПК для *обеспечения компьютерно-технической и информационно-технологической поддержки в образовательной деятельности обучающихся.*

Умеет:

У-ПК-9.1.*Использовать знания основ соответствующих дисциплин для обеспечения* для *обеспечения компьютерно-техниче-*

ской и информационно-технологической поддержки образовательной деятельности обучающихся.

Владеет:

В-ПК-9.1.Основами и навыками *обеспечения компьютерно-техниче-*

ской и информационно-технологической поддержки образовательной деятельности обучающихся.

Таблица 1

IV. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	
	Очно	Заочно
Общая трудоемкость час	**108**	**108**
Трудоемкость в зачетных единицах	3	3
Аудиторные занятия (всего)	48	18
Лекции	18	6
Лабораторные работы (ЛР)	30	12
Промежуточный контроль		
Самостоятельная работа (всего)	60	90
Итоговая аттестация	зачет	зачет

V. Содержание дисциплины

Таблица 2

V.1. Содержание разделов дисциплины (по лекциям)

№ № п/п	Наименование разделов	Содержание разделов
Модуль 1. Основные понятия информационной безопасности		
1.	Введение. Проблема информационной безопасности (ИБ).	Современное состояние, перспектива и ретроспектива, информационные системы, средства, каналы, сети и среды
2.	Информация качество и количество	Количество, качество, и ценность информации,
3.	Угрозы безопасности информации в компьютерных системах	КС как объект защиты информации, Понятие угрозы ИБ в КС, классификация и общий анализ угроз ИБ в КС.
Модуль 2. Защита информации		
4.	Общая характеристика средств и методов защиты информации	Обобщенные модули систем защиты информации, основные принципы обеспечения ИБ в КС, общая характеристика средств и методов защиты информации.
5.	Защита компьютерных систем от случайных угроз и несанкционированного доступа	Повышение эксплуатационные надежности КС, минимизация ущерба от аварий и стихийных бедствий, общая характеристика средств защиты информации, идентификация и аутентификация пользователей и разграничения их доступ к ресурсам компьютера
6.	Средства защиты ин-	Физические. Программные и аппаратные. Организационные. Законо-

	формационных систем	дательные. Психологические.
Модуль 3. Компьютерные вирусы		
7.	Криптографические методы защита информации	Классификация криптографических средств, основные методы шифрования
8.	Компьютерные вирусы и средства антивирусной защиты	Классификация компьютерных вирусов, Методы и средств защиты от компьютерных вирусов.
9.	Технические средства защиты информации	Пассивные технические средства. Активные технические средства. Экранирование. Техника перехвата информации. Защита каналов. Способы обнаружения устройств перехвата информации

Таблица 3

V.2. Тематический план изучения дисциплины

№№ п/п	Разделы дисциплины	Виды учебной работы и их трудоемкость (час)												Формируемые компетенции
		Лекции из них **Практическая подготовка**				**Лабораторные занятия** из них **Практическая подготовка**				Промежуточный контроль		Самостоятельная работа		
		Очно		Заочно		Очно		Заочно		Очно	Заочно	Очно	Заочно	
Модуль 1. Основные понятия информационной безопасности														
1.1	Лекция 1.Введение. Проблема информационной безопасности (ИБ).	2	2	1	1	2		1	1			5	10	ПКО-2; ПКО-4
1.2	Лекция 2. Информация качество и количество	2	1			2	2					5	10	
1.3	Лекция 3. Угрозы безопасности информации в компьютерных системах	2	2			2	1		2			5	10	
	Промежуточный контроль										1			
Модуль 2. . Защита информации														
2.1	Лекция 4. Общая характеристика средств и методов защиты информации	2		1	1	2	2					5	11	ПКО-2; ПКО-4
2.2	Лекция 5. Защита компьютерных систем от случайных угроз и несанкционированного доступа	2	1			2		1	1			8	10	
2.3	Лекция 6. Средства защиты информационных систем	2				1	2					7	11	
	Промежуточный контроль										1			
Модуль 3. Компьютерные вирусы														
3.1	Лекция 7. Криптографические методы защита информации	2	2	1	1	2	2					6	10	ПКО-2; ПКО-4
3.2	Лекция 8. Компьютерные вирусы и средства антивирусной защиты	2	1			2	2					6	11	
3.3	Лекция 9. Технические средства защиты информации	2	2				1					7	10	
	Промежуточный контроль										1			

	Итоговая аттестация	зач	зач							
	ИТОГО	27	6	27	6		3	54	93	

Таблица 4

V.3. Лабораторный практикум

№№ п/п	Раздел дисциплины	Тема	Цель	Учебно-методические материалы	Результат
Модуль 1. Основные понятия информационной безопасности					
1.1	Введение. Проблема информационной безопасности.	1.Разновидности компьютерных вирусов	Изучение принципов работы с разновидностями компьютерных вирусов	Лабораторный практикум «Технологии и системы защиты информации»	Изучены принципы лечения от разнообразных вирусов
1.2	Информация качество и количество	2.Системы контроля целостности	Приобретение навыков контроля целостности информации	Лабораторный практикум «Технологии и системы защиты информации»	Приобретены навыки контроля целостности информации
1.3	Угрозы безопасности информации в компьютерных системах	3.Системы отражения атак. Брандмауэр 4.Борьба с потенциально опасными программами 5.Безопасность в Интернет. Спам и антиспам	Изучение принципа работы хакеров	Лабораторный практикум «Технологии и системы защиты информации»	Изучен принцип работы хакеров
Модуль 2.. Защита информации					
2.1	Общая характеристика средств и методов защиты информации	6.Ограничение и контроль доступа 7.Анонимность в Интернете	Освоение принципов работы в Интернете	Лабораторный практикум «Технологии и системы защиты информации»	Освоены принципы работы в Интернете
2.2	Защита компьютерных систем от случайных угроз и несанкционированного доступа	8.Угрозы безопасности информации в компьютерных системах	Исследование угроз ИБ в КС		Исследованы угрозы безопасности информации в компьютерных системах
2.3	Средства защиты информационных систем	9. Физические и аппаратные средства защиты информации 10.Организационные и законодательные средства защиты информации	Изучение различных средств защиты информации		Изучены и анализированы различные средства защиты информации
Модуль 3. Компьютерные вирусы					

3.1	Криптографические методы защита информации	11.Шифрование информации	Изучение методов шифрования информации	Лабораторный практикум «Технологии и системы защиты информации»	Изучены методы шифрования информации
3.2	Компьютерные вирусы и средства антивирусной защиты	12.Восстановление информации 13.Антивирусные программы	Изучение методов и средств защиты информации от компьютерных вирусов		Изучены методы и средства защиты от компьютерных вирусов
3.3	Технические средства защиты информации	14.Пассивные средства защиты информации 15.Активные средства защиты информации	Изучение технических средств защиты информации		Изучены технические средства защиты информации

V.4. Самостоятельная работа студентов

V.4.1. Основные направления самостоятельной работы:

– Изучение литературы и лекционного материала;

– Подготовка к лабораторным работам, завершение их, оформление отчета и его защита;

– Написание рефератов.

Темы рефератов

1. Интеллектуальные компьютерные технологии защиты информации
2. Организационно-административное обеспечение информационной безопасности
3. Выработка официальной политики предприятия в области информационной безопасности
4. Современные методы защиты информации
5. Основы теории защиты информации
6. Инженерно-техническая защита информации
7. Голосовая защита информации
8. Биометрические системы защиты информации
9. Защита информации с использованием паролей
10. Защита информации в муниципальных информационных системах
11. Электронная цифровая подпись
12. Перехват информации
13. Подмена авторства информации
14. Маскировка под зарегистрированного пользователя и присвоение его полномочий
15. Модификация информации
16. Использование недостатков операционных систем
17. Копирование носителей информации и файлов с преодолением мер защиты
18. Незаконное подключение к аппаратуре и линиям связи;

V.4.2. Вопросы для самостоятельного изучения

Модуль 1. Основные понятия информационной безопасности

1.1. Основные составляющие информационной безопасности; категории информационной безопасности; абстрактные модели защиты информации.

1.2. Сервисы безопасности; законодательный уровень информационной безопасности.

1.3. Обзор российского законодательства в области информационной безопасности; информационная безопасность предприятия.

Модуль 2. . Защита информации

2.1. Преступления в сфере защиты информации; технологии защиты персональных данных; Безопасность современных сетевых технологий.

2.2. Методы защиты от вредоносного ПО; прикладные средства обеспечения информационной безопасности.

− 2.2. Средства защиты информационных систем: Способы обнаружения устройств негласного съема информации; Оптический (визуальный) канал утечки информации

Модуль 3. Компьютерные вирусы

3.1. Криптография и криптоанализ в России; цифровая подпись; классификация криптоалгоритмов; поточное шифрование. Скремблеры.

3.2. Методы комплексного обеспечения компьютерной безопасности; признаки классификации компьютерных вирусов; методы и средства обнаружения компьютерных вирусов.

− 3.3. Специальные средства для экспресс-копирования информации (или ее уничтожения) с магнитных носителей. Способы уничтожения информации. Оптический (визуальный) канал утечки информации

Таблица 5

V.4.3. Задания для самостоятельного выполнения

№№ п/п	Раздел дисциплины	Количество часов	Задания	Литература	Форма отчетности и контроля
Модуль 1. Основные понятия информационной безопасности					
1.1	Введение. Проблема информационной безопасности.	6	1. Изучить литературу 1,5, 9, 16, 17 2. Написать реферат (1, 2) 3. Изучить самостоятельно вопросы 1.1 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 1 Оформить отчет к л/р № 1 5. Защитить л/р № 1	1, 5, 9, 12, 16, 17	Отчет по л/р №1 и его защита, презентация рефератов 1, 2
1.2	Информация качество и количество	4	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (3, 4) 3. Изучить самостоятельно вопросы 1.2 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 2 Оформить отчет к л/р № 2 5. Защитить л/р № 2	1, 2, 4, 5, 8, 13, 16, 17	Отчет по л/р №2 и его защита, презентация рефератов 3, 4
1.3	Угрозы безопасности информации в компьютерных системах	8	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (5, 6) 3. Изучить самостоятельно вопросы 1.3 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 3-5 Оформить отчет к л/р № 3-5 5. Защитить л/р № 3-5	1, 2, 4, 5, 8, 13, 16, 17	Отчет по л/р №3-5 и их защита, презентация рефератов 5, 6
Модуль 2. . Защита информации					
2.1	Общая характеристика средств и методов защиты информации	6	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (7,8) 3. Изучить самостоятельно вопросы 2.1 раздела *V.4.2.* 4. Изучить методические реко-	1, 2, 4, 5, 8, 13, 14, 15, 16	Отчет по л/р №6-7 и их защита, презентация рефератов 7,8

			мендации к л/р № 6-7 Оформить отчет к л/р № 6-7 5. Защитить л/р № 6-7		
2.2	Защита компьютерных систем от случайных угроз и несанкционированного доступа	6	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (9,10) 3. Изучить самостоятельно вопросы 2.2 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 8 Оформить отчет к л/р № 8 5. Защитить л/р № 8	1, 2, 4, 5, 8, 13, 14, 15, 16, 17	Отчет по л/р №8 и его защита, презентация рефератов 9,10
2.3	Средства защиты информационных систем	6	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (11,12) 3. Изучить самостоятельно вопросы 2.3 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 9,10 Оформить отчет к л/р № 9,10 5. Защитить л/р № 9,10		Отчет по л/р №9,10 и их защита, презентация рефератов 11,12
Модуль 3. Компьютерные вирусы					
3.1	Криптографические методы защита информации	4	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (13,14) 3. Изучить самостоятельно вопросы 3.1 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 11 Оформить отчет к л/р № 11 5. Защитить л/р № 11	1, 2, 4, 5, 7, 8, 10, 11, 12, 13, 16, 17	Отчет по л/р №11 и его защита, презентация рефератов 13,14
3.2	Компьютерные вирусы и средства антивирусной защиты	8	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (15,16) 3. Изучить самостоятельно вопросы 3.2 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 12,13 Оформить отчет к л/р № 12,13 5. Защитить л/р № 12,13	1, 2, 3, 4, 5, 6, 8, 13, 16, 17	Отчет по л/р №12,13 и их защита, презентация рефератов 15,16
3.3	Технические средства защиты информации	6	1. Изучить литературу 1,2, 4, 5, 8, 13, 16, 17 2. Написать реферат (17,18) 3. Изучить самостоятельно вопросы 3.3 раздела *V.4.2.* 4. Изучить методические рекомендации к л/р № 14,15 Оформить отчет к л/р № 14,15 5. Защитить л/р № 14,15		Отчет по л/р №14,15 и их защита, презентация рефератов 17,18

VI. Образовательная технология

В преподавании дисциплины «Технологии и системы защиты информации» используются следующие образовательные технологии:

– лекции и лабораторные занятия, на которых выполняются задания, практикуются доклады, реферирование предложенной преподавателем литературы; проводятся дискуссии, тестирование.

– самостоятельная работа студентов, включающая усвоение теоретического материала, подготовка к лабораторным занятиям, выполнение творческих заданий, написание рефератов, тезисов, статей, работа с электронным учебно-методическим комплексом, под-

готовка к текущему контролю знаний к промежуточным аттестациям, итоговой аттестации;

– текущий и промежуточный контроль знаний, включая собеседование, консультации и тестирование по отдельным темам дисциплины, по модулю программы;

– НИРС, включающая занятия студентов в студенческом научном обществе, участие в конференциях, олимпиадах, изучения литературы и ее реферирование;

– консультирование студентов по вопросам учебной информации, написания тезисов, статей, докладов.

VII. Оценочные средства контроля текущей успеваемости и промежуточной аттестации студентов

VII.1. Модуль 1. Основные понятия информационной безопасности

Тест 1

1. Что понимается под информационной безопасностью:

a) защита душевного здоровья телезрителей

b) защита от нанесения неприемлемого ущерба субъектам информационных отношений

c) обеспечение информационной независимости России

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности:

a) Доступность

b) Масштабируемость

c) Целостность

d) Конфиденциальность

3. Что из перечисленного относится к числу основных аспектов информационной безопасности:

a) подлинность - аутентичность субъектов и объектов

b) целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения

c) стерильность - отсутствие не декларированных возможностей

4. Сложность обеспечения информационной безопасности является следствием:

a) комплексного характера данной проблемы, требующей для своего решения привлечения специалистов разного профиля

b) наличия многочисленных высококвалифицированных злоумышленников

c) развития глобальных сетей

5. Уголовный кодекс РФ не предусматривает наказания за:

a) увлечение компьютерными играми в рабочее время

b) неправомерный доступ к компьютерной информации

c) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

6. Согласно Закону "Об информации, информатизации и защите информации", риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на:

a) владельце этой системы

b) собственнике документов

c) потребителе информации

7. Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:

a) деятельность по технической защите конфиденциальной информации
b) образовательную деятельность в области защиты информации
c) предоставление услуг в области шифрования информации

8. В следующих странах сохранилось жесткое государственное регулирование разработки и распространения криптосредств на внутреннем рынке:

a) Китай
b) Россия
c) Франция

9. Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:

a) средства выявления злоумышленной активности
b) средства обеспечения отказоустойчивости
c) средства контроля эффективности защиты информации

10. Закон "Об информации, информатизации и защите информации" на первое место ставит:

a) сохранение конфиденциальности информации
b) поддержание целостности информации
c) обеспечение доступности информационных услуг

11. Атака, которая позволяет изучить логику работы сети:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;
b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

12. Атака позволяющая перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой ОС:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;
b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

13. Атака эффективно реализующаяся в системах, где применяются нестойкие алгоритмы идентификации/аутентификации хостов, пользователей:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;
b) ложный объект распределенной вычислительной сети;
c) анализ сетевого трафика;
d) отказ в обслуживании;
e) удаленный контроль над станцией в сети.

14. Атака, которая заключается в навязывании ложного маршрута из-за недостатков в алгоритмах маршрутизации:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

15. Атака, которая использует недостатки алгоритмов удаленного поиска (SAP(NetWare), и DNS (Internet)…):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

16. Атака, которая позволяет воздействовать на перехваченную информацию (проводить селекцию потока информации):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

17. Атака, которая позволяет воздействовать на перехваченную информацию (модифицировать информацию):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

18. Атака, которая позволяет воздействовать на перехваченную информацию (подменять информацию):

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

19. Атака, результатом осуществления которой может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

20. Атака, которая может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

21. Атака, которая заключается в передаче с одного адреса такого количества запросов на подключение к атакуемому хосту, какое максимально может "вместить" трафик:

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

22. Атака, которая заключается в запуске на атакуемом компьютере программы "сетевого шпиона":

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

23. Атака, которая заключается в запуске на атакуемом компьютере программы "сетевого шпиона":

a) подмена доверенного объекта или субъекта распределенной вычислительной сети;

b) ложный объект распределенной вычислительной сети;

c) анализ сетевого трафика;

d) отказ в обслуживании;

e) удаленный контроль над станцией в сети.

Модуль 2. Защита информации

Тест 2

1. Совершенный этап защиты информации называется:
   a) информационным
   b) начальным
   c) развитым*
   d) комплексным.

2. Процесс защиты информации в АС измеряется периодом:
   a) 20 – 25 лет
   b) 30 – 35 лет
   c) 35 – 40 лет*
   d) 40 – 45 лет

3. Используемые средства защиты информации в АСОД на начальном этапе:

a) материальные
b) морально-этические
c) неформальные
d) формальные*

4. Если информация искажена умышленно, то ее называют:
a) некачественной
b) субъективной
c) дезинформацией*

5. Защита информации в АСОД считается комплексной, если:
a) реализуется одна цель защиты и используется один вид защиты
b) реализуется более одной цели защиты и используется более одного вида защиты
c) реализуются все цели защиты и используются все виды защиты*
d) реализуется более одной цели защиты, но не все и используется более одного вида
защиты, но не все

6. Если доступ к информации ограничивается, то такая информация является:
a) качественной
b) достоверной
c) конфиденциальной*
d) ценной

7. Основной объем информации, составляющий базис организации или учреждения:
a) постоянная информация
b) медленно меняющаяся информация*
c) техническая информация
d) быстро меняющаяся информация

8. При информационном обеспечении деятельности предприятия с точки зрения защиты информации предметом наиболее пристального внимания должна быть:
a) регулирование входных и выходных потоков информации
b) управление входными потоками информации
c) формирование и совершенствование информационного кадастра
d) информационный кадастр и информационные технологии*

9. Традиционные меры защиты информации твердых копий:
a) программные средства
b) криптографические
c) соблюдение режима секретности*
d) каровое обеспечение

10. Если носители информации являются электромагнитные волны, то такая информация относится к:
a) электронной
b) телекоммуникационной*
c) документальной
d) речевой

11. Специализация функций АС, где особое значение имеет защита авторского права:

a) планирование и управление
b) образование и культура
c) транспорт и связь
d) научая и проектная деятельность*

12. К какой из составляющих системы защиты информации относятся средства пожарной сигнализации и пожаротушения:
a) организационной
b) программной
c) технической*
d) информационно-лингвистической

13. К какому виду угроз для АС относятся радиоактивное излучение и осадки:
a) природные*
b) технические
c) созданные людьми преднамеренно
d) созданные людьми непреднамеренно

14. При выполнении курсовой или дипломной работы студент может быть допущен к сведениям, имеющим гриф секретности:
a) секретно*
b) совершенно секретно
c) особой важности
d) для служебного пользования

15. Орган управления государственной системой защиты информации:
a) федеральное агентство правительственной связи и информации
b) федеральная служба контрразведки
c) гостехкомиссия России*
d) федеральная служба безопасности

16. Какой из способов подключения к Интернету обеспечивает наибольшие возможности для доступа к информационным ресурсам:
a) по телефонному каналу, который коммутируется
b) постоянное соединение по оптоволоконному каналу*
c) постоянное соединение по выделенному телефонному каналу
d) терминальное соединение по телефонному каналу, который коммутируется

17. Требование о возмещении убытков в связи с разглашением информации ограниченного доступа не может быть удовлетворено в случае:
a) несоблюдения пропускного режима
b) непринятие мер по соблюдению конфиденциальности*
c) отсутствия пожарной сигнализации
d) отсутствия инженерных сооружений

18. Разрешать и ограничивать доступ к информации, определять порядок и условия доступа вправе:
a) президент РФ
b) гостехкомиссия России
c) оператор информационной системы
d) обладатель информации*

19. Основанием для отказа гражданину в допуске к государственной тайне могут являться:

a) уклонение от воинской службы
b) принадлежность к общественным объединениям
c) имущественное и должностное понижение
d) уклонение от проверочных мероприятий*

20. Степени секретности сведений и их грифы, составляющих государственную тайну:

a) особо секретно, совершенно секретно, секретно
b) очень секретно, неприкосновенно, секретно
c) совершенно секретно, тайно, секретно
d) особой важности, совершенно секретно, секретно*

21. Какую функцию выполняет периферийное устройство:

a) управления работой ЭВМ по заданной программе
b) оперативного сохранения информации
c) ввода и вывода информации*
d) никаких функций не выполняет

22. Средства защиты информации без участия человека называются:

a) законодательные
b) организационные
c) неформальные
d) формальные*

23. К какому виду относится информация, если она представлена на диске:

a) телекоммуникационная
b) документальная*
c) электронная
d) магнитная

Модуль 3. Компьютерные вирусы

Тест 3

1. По среде обитания классические вирусы разделяются на:

a) загрузочные;
b) компаньоны;
c) паразитические;
d) ссылки;
e) перезаписывающие.

2. По среде обитания классические вирусы разделяются на:

a) ссылки;
b) компаньоны;
c) паразитические;
d) макровирусы;
e) перезаписывающие.

3. По среде обитания классические вирусы разделяются на:

a) ссылки;
b) компаньоны;
c) скриптовые;
d) паразитические;

e) перезаписывающие.

4. По способу заражения классические вирусы разделяются на:
a) файловые;
b) загрузочные;
c) макровирусы;
d) скриптовые;
e) перезаписывающие.

5. По способу заражения классические вирусы разделяются на:
a) файловые;
b) паразитические;
c) макровирусы;
d) скриптовые;
e) загрузочные.

6. По способу заражения классические вирусы разделяются на:
a) компаньоны;
b) файловые;
c) макровирусы;
d) скриптовые;
e) загрузочные.

7. По способу заражения классические вирусы разделяются на:
a) скриптовые;
b) файловые;
c) макровирусы;
d) ссылки;
e) загрузочные.

8. Сетевой червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе:
a) IM-Worm;
b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

9. Сетевые черви используют способ распространения – рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL на файл, расположенный на каком-либо веб-сервере:
a) IM-Worm;
b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

10. Сетевые черви распространяются двумя способами по IRC-каналам. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ – отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть:
a) IM-Worm;
b) IRC-Worm;
c) Net-Worm;

d) P2P-Worm;
e) Email-Worm.

11. Сетевой червь ищет удаленные компьютеры и копирует себя в каталоги, открытые на чтение и запись, при этом червь или перебирает доступные сетевые каталоги, используя функции операционной системы, и/или случайным образом ищет компьютеры в глобальной сети, подключаются к ним и пытаются открыть их диски на полный доступ:
a) IM-Worm;
b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

12. Сетевые черви ищут в сети компьютеры, на которых используется программное обеспечение, содержащее уязвимости. Для заражения уязвимых компьютеров червь посылает специально оформленный сетевой пакет или запрос, в результате чего код червя проникает на компьютер-жертву:
a) IM-Worm;
b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

13. Для внедрения в сеть сетевому червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальном компьютере. Всю остальную работу по распространению вируса сеть берет на себя – при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для скачивания файла с зараженного компьютера:
a) IM-Worm;
b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

14. Сетевой червь имитирует сетевой протокол конкретной файлообменной системы и на поисковые запросы отвечает положительно – при этом червь предлагает для скачивания свою копию:
a) IM-Worm;
b) IRC-Worm;
c) Net-Worm;
d) P2P-Worm;
e) Email-Worm.

15. Троянские утилиты удаленного администрирования:
a) Trojan-PSW;
b) Trojan-Clicker;
c) Backdoor;
d) Trojan-Downloader;
e) Trojan-Dropper.

16. Троянские программы для воровства паролей:
a) Trojan-PSW;
b) Trojan-Clicker;

c) Backdoor;
d) Trojan-Downloader;
e) Trojan-Dropper.

17. Троянские программы для доставки вредоносных программ:
a) Trojan-PSW;
b) Trojan-Clicker;
c) Trojan-Proxy;
d) Trojan-Downloader;
e) Trojan-Dropper.

18. Троянские программы, скрытно осуществляющие анонимный доступ к различным Интернет-ресурсам, обычно используются для рассылки спама:
a) Trojan-PSW;
b) Trojan-Spy;
c) Trojan-Proxy;
d) Trojan-Downloader;
e) Trojan-Dropper.

19. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
a) черный пиар;
b) фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

20. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
a) черный пиар;
b) фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

21. Спам, написанный от имени реальных или вымышленных лиц, обычно граждан стран с нестабильной экономической ситуацией, воспринимаемых публикой как рассадник коррупции:
a) черный пиар;
b) фишинг;
c) нигерийские письма;
d) источник слухов;
e) пустые письма.

22. Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:
a) детектор;
b) доктор;
c) сканер;
d) ревизор;
e) сторож.

23. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
a) детектор;

b) доктор;
c) сканер;
d) ревизор;
e) сторож.

VII.4. Методика балльно-рейтингового оценивания успеваемости студентов

Контроль и оценка учебных достижений студентов по дисциплине «Технологии и системы защиты информации» проводится по балльно-рейтинговой системе с использованием кредитно-зачетных единиц. Итоговые баллы по результатам изучения дисциплинарных модулей и всего курса основывается на интегральной оценке всех видов учебной (аудиторной, внеаудиторной, самостоятельной).

Текущий контроль по курсу «Технологии и системы защиты информации» включает:

− *лекционные занятия (2 часа)*: неявка на занятия – 0; посещение занятий – 2 балла; за активное участие в лекции – 3 балла (максимальное количество баллов за модуль – 3 занятий × 5 балла = 15 баллов);

− *лабораторные занятия (2 часа):* неявка на занятия – 0; посещение занятий – 2 балла; за выполнение лабораторной работы – 2 балла; за защиту выполненной работы – 3 балла (максимальное количество баллов за модуль – 5 занятий × (2+2+3) балла = 35 баллов).

Максимальное количество баллов по результатам текущей работы и промежуточного контроля по дисциплинарному модулю (без учета бонусов) – 100 баллов (текущая работа – 50 баллов, промежуточный контроль (тестирование) – 50 баллов).

Дополнительные баллы (бонусы):

- инициативное решение учебных задач на занятиях – 1 балл;
- оригинальное решение задачи – 2 балла;
- решение большего количества задач, чем предусмотрено в модуле – 4 балла;

Дополнительные баллы по результатам участия студентов в научно-исследовательской работе по дисциплине:

- реферат – 1 балл;
- научный доклад – 2 балла;
- публикация в печати – 4 балла;
- участие в работе научного кружка – 4 балла.
- доклады на научно-практической конференции:
  институтской – 2 балла;
  университетской – 3 балла;
  республиканской – 4 балла;
  Российской – 5 баллов;
  международной – 6 баллов.
- участие в олимпиаде:
  институтской – 1 балл;
  университетской – 2 балла;
  республиканской – 4 балла;
  Российской – 6 баллов;
  международной – 8 баллов.
- получение патента, свидетельства на охрану интеллектуальной собственности – 20 баллов.

Минимальное количество баллов, необходимое для получения положительной оценки по данной дисциплине определено – 51 баллов.

После завершения изучения дисциплинарного модуля студенту предоставляется одна неделя для добора баллов.

Экзамены и зачеты как отдельные виды учебной нагрузки не предусматриваются, но проводятся как одна из форм добора баллов.

Шкала диапазонов итоговой оценки определяется в соответствии с таблицей 9

Таблица 9

Шкала диапазонов итоговой оценки

БРС	Итоговая оценка
85 –100	5 (Отлично)
65 – 84	4 (Хорошо)
51 – 64	3 (удовлетворит.)
0 – 50	2 (Неудовлет.)
51 – 100	Зачет*

VIII. Информационное обеспечение дисциплины

а) Основная литература

1. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. – М: "Издательство "ФЛИНТА", 2011. – 224

2. Аверченков В.И. Рытов М.Ю. Организационная защита информации. – М: "ФЛИНТА", 2011. – 184 с.

3. Алексеев П.П., Козлов Д.А., Прокди Р.Г. Антивирусы. Настраиваем защиту компьютера от вирусов. – М: "Наука и Техника", 2008. – 80 с.

4. Бирюков А.А. Информационная безопасность: защита и нападение. М: "ДМК Пресс", 2012. – 474 с.

5. Богомолова О.Б. Усенков Д.Ю. Защита компьютера от вредоносных воздействий : практикум. – М: "Бином. Лаборатория знаний", 2012. – 175 с.

6. Гатченко Н.А. Исаев А.С. Яковлев А.Д. Криптографическая защита информации. Учебное пособие. - СПбНИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2012. – 142 с.

7. Гатчин Ю.А. Климова Е.В. Основы информационной безопасности. – СПбНИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2009. – 84 с.

8. Голиков А.М. Защита информации в инфокоммуникационных системах и сетях. – Томск: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. - 374

9. Гошко С.В. Технологии борьбы с компьютерными вирусами. Практическое пособие. – М: "СОЛОН-Пресс», 2009. – 352 с.

10. Информационная безопасность и защита информации: Учеб. Пособие для студ. высш. учеб. заведений/ В.П.Мельников, С.А.Клейменов, А.М.Петраков, 3-е изд., стер. – М.: Издательский центр «Академия», 2012.

11. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие. – СПбНИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2012. – 416 с.

12. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М: "ДМК Пресс", 2012. – 592 с.

б) Дополнительная литература

13. Безопасность сетей. Полное руководство./Р.Брэгг, Родс-Оусли, К.Страсберг; пер. с анг. – М. Издательство «ЭКО – М», 2010.

14. Информационная безопасность и защита информации: Учебное пособие/ Степанов Е.А. и др. – М.: Инфра, 2012.

15. Пазизин С.В. Основы защиты информации в компьютерных системах. – М.: ТВП/ОпиПМ, 2013.

16. Основы защиты информации: Учеб. Пособие для студ. высш. учеб. заведений/ А.И.Куприянов, А.В.Сахаров, В.А.Шевцов. – М.: Издательский центр «Академия», 2006.

17. Семененко В.А. Информационная безопасность: Учеб. пособие. 3-е изд., стереот. – М.:МГИУ, 2012.

.IX. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

18. Единая коллекция цифровых образовательных ресурсов. // http://school-collection.edu.ru/.

19. Информационные образовательные ресурсы. //http://www.ed.gov.ru/edusupp/ informedu /3585.

20. Учительская газета. // http://www.ug.ru/.

21. Федеральный центр информационно-образовательных ресурсов. // http://fcior.edu.ru/.

X. Методические указания для обучающихся по освоению дисциплины

При реализации программы дисциплины «Технологии и системы защиты информации» используются различные образовательные технологии – аудиторные занятия включают лекции и лабораторные занятия. Для контроля усвоения студентом данного курса используются контрольные работы и домашние задания. Самостоятельная работа студентов предполагает проработку лекционного и учебно-методического материала, включая рекомендуемую литературы для подготовки контрольным работам, а также выполнение домашних заданий.

Оценочные средства для текущего контроля успеваемости и усвоения дисциплины предполагают промежуточный контроль при подготовке к лабораторным работам по контрольным вопросам, контроль в виде самостоятельных работ при выполнении домашних заданий.

При изучении лекционного курса следует вести подробный конспект лекций, позволяющий самостоятельно проследить логику изложения учебного материала. Следует аккуратно вычерчивать графики, рисунки, схемы и таблицы, что способствует зрительному восприятию и более полному запоминанию материала. При недопонимании учебного материала нужно пытаться правильно сформулировать вопросы к лектору и не стесняться задавать их. Наиболее глубокие знания будут получены студентом только тогда, когда им усвоена структура учебной дисциплины, своевременно и полно понята суть проблемы и пути её решения.

На лабораторных занятиях нужно внимательно ознакомиться с теоретической частью работы, изучить ход проведения работы, порядок обработки полученных результатов. Особое внимание следует уделить систематизации материала для формулировки вывода по результатам лабораторного эксперимента, который способствует формированию базовых понятий изучаемой дисциплины.

Самостоятельная работа студента должна начинаться с изучения конспекта, соответствующих разделов рекомендуемой литературы и теоретической части лабораторных работ. Затем следует ответить на контрольные вопросы, предлагаемые для лучшего усвоения учебного материала.

IX. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

В учебном процессе используются следующие информационные технологии:

– компьютерная техника и средства связи (компьютер, проектор, экран, видеокамера и др.);

– методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов и др.);

– перечень интернет-сервисов и электронных ресурсов (поисковые сервисы Google, Yandex, электронная почта, электронные учебные и учебно-методические материалы);

– методические материалы (Электронный УМК): Раджабалиев Г.П., Нурмагомедова Н.Х..: «Технология защиты информации».

– перечень программного обеспечения: MS WindowsXP, Kaspersky, Internet Security, Safe'n'Sec Outpost Firewall, COMODO Firewall, RegRun, Prevx1, AnVir Task Manager

– мультимедийные средства представления лекционного и лабораторно-практического презентационного материала;

– доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочей программе, через личный кабинет студента и преподавателя;

– доступ в Интернет, наличие компьютерных программ общего назначения.

XII. Материально-техническое обеспечение дисциплины

- Инструментальные средства, реализующие возможности Интернет и мультимедиа технологий.
- Электронные средства образовательного назначения, в том числе на CD-ROM.
- Компьютерный класс с выходом в Интернет.
- Электронная доска.