МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита программ и данных

Кафедра Информатики и Информационных Технологий

Образовательная программа

10.03.01 Информационная безопасность

Профиль подготовки

Безопасность компьютерных систем

Уровень высшего образования

Бакалавриат

Форма обучения

очная

Статус дисциплины: *базовая*

Махачкала, 2018

Рабочая программа по дисциплине «Защита программ и данных» составлена в 2018 году в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) от 1 декабря 2016 г. №1515

Разработчик(и): кафедра ИиИТ ст.пр. Муртузалиева А.А.

Рабочая программа по дисциплине «Защита программ и данных» одобрена:
на заседании кафедры _____ от «___» _____20__г., протокол № __
Зав. кафедрой _____ Ахмедов С.А.

на заседании Методической комиссии факультета ИиИТ
от «___» _____20__г., протокол №___.
Председатель _____ Камилов К.Б.

Рабочая программа по дисциплине «Защита программ и данных» согласован с учебно-методическим управлением
«____» _____20 г. _____

Аннотация рабочей программы дисциплины

Дисциплина Б1.Б38 "Защита программ и данных" входит в *базовую* часть образовательной программы *бакалавриата* по направлению 10.03.01 Информационная безопасность

Дисциплина реализуется на факультете ИиИТ кафедрой ИиИТ.

Содержание дисциплины охватывает круг вопросов, связанных с основными принципами обеспечения безопасности программ и данных:

• экспертиза качества реализации программных и программно- аппаратных средств обеспечения информационной безопасности;

• исследование программного обеспечения на предмет наличия недокументированных возможностей;

• выявление уязвимостей программного обеспечения;

• выявление вредоносного программного обеспечения, оценка опасности обнаруженных вредоносных программ, планирование работ по локализации последствий и пресечению обнаруженной атаки.

Целью освоения дисциплины «Защита программ и данных» является детальное изучение студентами средств и методов анализа программных реализаций.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных - ОК-**5,** общепрофессиональных – ОПК-4, ОПК-**7,** профессиональных – ПК-2.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, лабораторные занятия, самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме – *контрольная работа, коллоквиум и пр.* и промежуточный контроль в форме - *зачета*.

Объем дисциплины 2 зачетные единицы.

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе								
	Всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		Всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	контроль		
7	72	38	20		18			34	зачет

1. Цели освоения дисциплины

Целью освоения дисциплины является знакомство с основными методами и средствами обеспечения защиты исполнимых файлов при разработке и использовании программного обеспечения, а также защиты массивов данных, представленных в электронном виде.

2.Место дисциплины в структуре ОПОП бакалавриата:

Данная дисциплина входит в базовую часть образовательной программы по направлению 10.03.01 -Информационная безопасность (уровень бакалавриата). Изучение вопросов защиты программ и данных основано на дисциплинах вида: «Информатика», «Математическая логика и теория алгоритмов», «Языки программирования»," Организационное и правовое обеспечение информационной безопасности " «Основы

информационной безопасности», "Криптографические методы защиты информации", "Языки ассемблера". Знания и практические навыки, полученные при изучении защиты программ и данных, обеспечивают освоение дисциплин вида: «Модели безопасности компьютерных систем», «Основы построения защищенных операционных систем», а также используются обучаемыми при разработке курсовых и дипломных работ.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины.

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знать: Представление о социальной значимости своей будущей профессии Понимание миссии ИТ-прогресса, требующей высокой мотивации к выполнению профессиональной деятельности Уметь: мотивировать выполнение профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, Владеть: нормами профессиональной этики.
ОПК-3	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знать: основы организации современных ЭВМ и их общие характеристики, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники; Уметь формулировать требования и принимать обоснованные решения по выбору аппаратно-программных средств для рационального решения задач, связанных с получением и преобразованием информации Владеть: практическими навыками по использованию средств вычислительной техники и программного обеспечения для организации обработки информации
ОПК-4	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: возможности сети Интернет для поиска и обработки данных и организации информационного обмена; Уметь: эффективно использовать возможности современных ПЭВМ, компьютерных сетей и программных средств для решения прикладных задач, возникающих в процессе обучения в вузе и в ходе будущей профессиональной деятельности

		Владеть: навыками работы со справочно-поисковыми системами в глобальной сети Интернет
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать: основные положения теории безопасности программ и данных; Уметь: проводить анализ безопасности программ и данных с помощью контрольно-испытательных и логико-аналитических методов, а также сравнивать логико-аналитические и контрольно испытательные методы; Владеет: - методами выявления уязвимости программного обеспечения
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знает: - основные принципы обеспечения безопасности программ и данных; основные модели поведения программного обеспечения Умеет : оценивать вероятность наличия разрушающего программного обеспечения на этапе испытаний программного обеспечения; оценивать надежность программного обеспечения для контроля его технологической безопасности;- обеспечивать целостность и достоверность используемого программного кода; осуществлять обоснованный выбор средств защиты программ и данных; Владеет методами выявления уязвимости программного обеспечения; основными методами выбора программного обеспечения безопасности компьютерных систем; основными способами защиты программного обеспечения от несанкционированного копирования

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 2 зачетные единицы, 72 академических часа.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)	Самостоятел ная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной

				Лекции	**Практические занятия**	**Лабораторные занятия**	**Контроль самост. раб.**		**аттестации *(по семестрам)***
	Модуль 1. ***(Основы информационной культуры и техническая база информационной технологии)***								
1	Введение в теорию обеспечения безопасности программ и данных	7		2				4	к/р , тестовый контроль, устный и письменный опросы
2	Методы и средства анализа безопасности программ и данных			4		4		6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
3	Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность			4		4		8	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
				10		8		18	
4	Расчет вероятности наличия разрушающих программных средств на этапе испытаний программного обеспечения и подходы к его исследованию			2		2		4	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
5	Методы обеспечения надежности программ для обеспечения их технологической безопасности			4		4		6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
6	Методы и средства обеспечения целостности и достоверности используемого программного кода			4		4		6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
	Итого по модулю 1:			10		10		16	
	ИТОГО			20		18		34	зачет

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине

Модуль 1

1.1 Введение в теорию обеспечения безопасности программного обеспечения и данных

Основные положения теории безопасности программ и данных. Угрозы безопасности программному обеспечению и данным. Теоретические основы дисциплины и терминология.

Основные принципы обеспечения безопасности программного обеспечения и данных. Технологическая и эксплутационная безопасность программ

1.2 Методы и средства анализа безопасности программного обеспечения и данных

Контрольно-испытательные методы анализа безопасности программ и данных. Логико-аналитические методы контроля безопасности программ и данных. Сравнительный анализ логико-аналитических и контрольно-испытательных методов анализа безопасности программ и данных

Выявление уязвимостей программ и данных. Выбор программного обеспечения безопасности компьютерных систем. Модели поведения программного обеспечения

1.3 Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность

Обобщенные способы анализа программных средств на предмет наличия (отсутствия) разрушающих программных средств.

Построение программно-аппаратных комплексов для контроля технологической безопасности программного обеспечения и данных.

Модуль 2

2.1Расчет вероятности наличия разрушающих программных средств на этапе испытаний программного обеспечения и подходы к его исследованию

Постановка задачи. Обоснование множества информационных характеристик. Алгоритмы приближенных вычислений вероятностных характеристик наличия в программном обеспечении разрушающих программных средств

Обоснование критериев принятия решений о наличии в программном обеспечении разрушающих программных средств. Подходы к исследованию безопасности сложных программных комплексов.

2.2 Методы обеспечения надежности программ для контроля их технологической безопасности

Исходные данные, определения и условия. Анализ существующих моделей надежности программного обеспечения.

Модель Нельсона. Оценка технологической безопасности программного обеспечения на базе модели Нельсона.

2.3 Методы и средства обеспечения целостности и достоверности используемого программного кода

Методы защиты программ и данных от несанкционированных изменений. Проверка целостности программ и данных.

Схема подписи с верификацией по запросу. Примеры применения схемы подписи с верификацией по запросу. Основные подходы к защите программного обеспечения от несанкционированного копирования.

4.3.2. Содержание лабораторно-практических занятий по дисциплине

Модуль 1

Раздел 1. Анализ программных реализаций, защита программ от анализа

1.1. Общие сведения

1.2. Метод экспериментов с черным ящиком

1.3. Статический метод
1.4. Динамический метод
1.4.1. Программные отладочные средства
1.4.2. Методика изучения программ динамическим методом
1.4.3. Пример применения динамического метода
1.5. Особенности анализа некоторых видов программ
1.5.1. Особенности анализа оверлейных программ
1.5.2. Особенности анализа графических программ Windows
1.5.3. Пример анализа графической программы Windows
1.5.4. Особенности анализа параллельного кода
1.5.5. Особенности анализа кода в режиме ядра Windows
1.6. Вспомогательные инструменты анализа программ
1.7. Защита программ от анализа
1.8. Вопросы для самопроверки

Модуль 2

Раздел 2. Программные закладки, пути их внедрения, средства и методы противодействия программным закладкам

2.1. Общие сведения
2.2. Субъектно-ориентированная модель компьютерной системы
2.3. Модели взаимодействия программной закладки с атакуемой системой
2.3.1. Модель «наблюдатель»
2.3.2. Модель «перехват»
2.3.3. Модель «искажение»
2.4. Предпосылки к внедрению программных закладок
2.4.1. Общие сведения
2.4.2. Переполнения буферов
2.4.3. Отсутствие необходимых проверок входных данных
2.4.4. Некорректный контекст безопасности
2.4.5. Устаревшие функции
2.4.6. Другие уязвимости
2.5. Методы внедрения программных закладок
2.6. Компьютерные вирусы как особый класс программных закладок
2.7. Средства и методы защиты от программных закладок 207
2.8. Организационные и административные меры антивирусной защиты
2.9. Выявление программных закладок в ручном режиме

5. **Образовательные технологии**

Рекомендуемые образовательные технологии: лекции, практические занятия, самостоятельная работа студентов.

В соответствии с требованиями ФГОС ВПО по направлению подготовки реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием

конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 30% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ООП). Занятия лекционного типа для соответствующих групп студентов не могут составлять более 60% аудиторных занятий (определяется соответствующим ФГОС)).

6. Учебно-методическое обеспечение самостоятельной работы студентов.
Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. Для реализации творческих способностей и более глубокого освоения дисциплины предусмотрены следующие виды самостоятельной работы: 1) текущая и 2) творческая проблемно - ориентированная.

Текущая самостоятельная работа, направленная на углубление и закрепление знаний студента, развитие практических умений включает: работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию; опережающую самостоятельную работу; выполнение домашних заданий; изучение тем, вынесенных на самостоятельную проработку; подготовку к лабораторным работам, к практическим занятиям; подготовку к контрольным работам, зачету, экзамену;

Для повышения результативности самостоятельной работы преподаватель разрабатывает учебно-методическое обеспечение, которое включает в себя средства обучения и средства контроля.
http://umk.dgu.ru/
http://edu.dgu.ru/
http://elib.dgu.ru/
http://moodle.dgu.ru/
http://eor.dgu.ru/Default/NProfileUMK/
http://cathedra.dgu.ru/

Творческая проблемно - ориентированная самостоятельная работа (ТСР) предусматривает: выполнение курсовой работы;- исследовательскую работу и участие в научных студенческих конференциях и олимпиадах; поиск, анализ, структурирование и презентацию информации; углубленное исследование вопросов по тематике лабораторных работ.

ПЕРЕЧЕНЬ ТЕМ ДОМАШНИХ РАБОТ

7 СЕМЕСТР

№ п/п	№ раздела дисциплины	Тема работы
1.	2-5	дизассемблеры.
2.	2-5	Программы отладчики
3.	2-5	оверлейные программы.
4.	2-5	системные отладчики
5.	2-5	программы-мониторы.
6.	2-5	формальные модели: • наблюдатель — по некоторому активизирующему событию закладка инициирует нетипичный для атакуемой системы информационный поток или моделирует сбойную ситуацию; • перехват — закладка производит сохранение всех или избранных фрагментов вводимой или выводимой информации в скрытую область локальной или удаленной внешней памяти либо в от- крытый канал связи; • искажение — закладка искажает информационные потоки атакуемой системы либо инициирует или подавляет возникающие при работе системы ошибки..
7.	2-5	средства динамического изменения полномочий

8.	2-5	стелс-технологии
9.	2-5	эксплойты.

Вопросы:

1. В чем заключается опасность программных закладок?
2. Какие программные закладки вы знаете?
3. Что такое информационный поток?
4. Как в рамках субъектно-ориентированной модели описывается операция порождения нового субъекта доступа?
5. Какими двумя причинами может вызываться НСД в рамках субъектно- ориентированной модели?
6. Что такое программная закладка?
7. Какие модели взаимодействия программной закладки с атакуемой системой вы знаете?
8. Как формально определяется модель «наблюдатель»?
9. Для чего чаще всего применяются программные закладки модели «наблюдатель»?
10. Каковы типичные недостатки программных закладок модели «наблюдатель»?
11. Как программные закладки модели «наблюдатель» обычно обеспечивают свою повторную активизацию после перезагрузки атакованной операционной системы?
12. Как выглядит общая схема взаимодействия клиентской и серверной частей программной закладки модели «наблюдатель»?
13. Какие преимущества дает программной закладке модели «наблюдатель» модульная архитектура?
14. Как формально определяется модель «перехват»?
15. Как устроены перехватчики паролей первого рода?
16. Как устроены перехватчики паролей второго рода?
17. Как устроены перехватчики паролей третьего рода?
18. Как устроены мониторы файловых систем?
19. Как устроены мониторы сети?
20. Как формально определяется модель «уборка мусора»?
21. Как формально определяется модель «искажение»?
22. Какие средства динамического изменения полномочий поддерживаются операционными системами семейства UNIX?
23. Какие средства динамического изменения полномочий поддерживаются операционными системами семейства Windows?\
24. Как несанкционированное порождение дочернего процесса системным процессом позволяет повысить полномочия пользователя?
25. Как несанкционированная модификация машинного кода монитора безопасности объектов позволяет повысить полномочия пользователя?
26. Какие сетевые атаки могут быть реализованы в рамках модели «искажение»?
27. Что такое стелс-технологии?
28. Что относится к основным функциям стелс-драйвера?
29. Можно ли внедрить программную закладку в адекватно защищен- ную компьютерную систему?
30. Какие типичные уязвимости защиты компьютерных систем вы знаете? 31. Что такое переполнение буфера?
32. Как переполнение буфера в стеке программы позволяет нарушителю передать управление на произвольный адрес в текущем адресном пространстве?
33. Как отлаживать в Microsoft Visual Studio консольную программу, за- пущенную в режиме перенаправления стандартного ввода?
34. Для первой учебной программы с переполнением буфера напишите эксплойт, выдающий на экран окно с заданным текстом и кнопкой ОК.

35. Для первой учебной программы с переполнением буфера напишите эксплойт, не привязанный к линейному адресу, по которому в оперативной памяти размещается переполняемый буфер.
36. Для первой учебной программы с переполнением буфера напишите эксплойт, использующий для завершения работы функцию завершения, указатель на которую содержится в таблице адресов импортов атакуемой программы.
37. Скомпилируйте первую учебную программу с переполнением буфера с опцией компилятора /GS. Убедитесь, что переполнение буфера невозможно поэксплуатировать.
38. Для второй учебной программы с переполнением буфера напишите эксплойт, выдающий на экран окно с заданным текстом и кнопкой OK.
39. Перепишите вторую учебную программу с переполнением буфера так, чтобы она использовала вместо функции HeapAlloc функцию LocalAlloc.
Напишите для этой программы эксплойт, аналогичный приведенному в тексте пособия.
40. Для третьей учебной программы с переполнением буфера напишите эксплойт, выдающий на экран окно с заданным текстом и кнопкой OK.
41. Для первой учебной программы с переполнением буфера напишите экс- плойт, не приводящий к досрочному завершению атакованной программы.
42. Для второй учебной программы с переполнением буфера напишите эксплойт, не приводящий к досрочному завершению атакованной программы. 43. Для третьей учебной программы с переполнением буфера напишите эксплойт, не приводящий к досрочному завершению атакованной программы. 44. Как устроен механизм DEP?
45. В чем заключалась уязвимость GetAdmin в Windows NT?
46. Как проверить, нет ли в текущем ядре операционной системы уязвимостей, подобных GetAdmin?
47. В чем заключалась уязвимость %00 в Internet Explorer 5?
48. В чем заключалась уязвимость AdminTrap в Windows NT?
49. Чем опасно наличие на рабочем столе пользователя окон, обслуживаемых системными процессами?
50. В чем заключалась уязвимость сервера NetDDE в Windows 2000?
51. В чем заключалась уязвимость графического формата WMF в Windows, исправленная в январе 2006 г.?
52. В чем заключается уязвимость program.exe?
53. Как можно проверить, есть ли в операционной системе программы, подверженные уязвимости program.exe?
54. Как в рамках субъектно-ориентированной модели формально описывается внедрение программной закладки в атакованную систему?
55. По каким признакам классифицируются методы внедрения программных закладок?
56. В чем заключается метод маскировки программной закладки под прикладное программное обеспечение?
57. В чем состоит основной недостаток метода маскировки программной закладки под прикладное программное обеспечение?
58. В чем заключается метод маскировки программной закладки под системное программное обеспечение?
59. Каково основное достоинство метода маскировки программной закладки под системное программное обеспечение?
60. Как в Windows установить новый сервис?
61. Что нужно добавить в прикладную программу Windows, чтобы она могла запускаться в режиме сервиса?
62. Как сделать самоинсталлирующийся сервис для Windows?
63. В чем заключается метод внедрения программной закладки путем подмены системного программного обеспечения?

64. Почему в Windows 2000 и более поздних версиях внедрение программной закладки путем подмены системного программного обеспечения практически невозможно?
65. В чем заключается прямое ассоциирование?
66. В чем состоит суть косвенного ассоциирования?
67. Что такое компьютерный вирус?
68. Является ли задача выявления компьютерного вируса алгоритмически разрешимой в общем случае?
69. Когда появились первые компьютерные вирусы?
70. Какой компьютерный вирус причинил наибольший ущерб за всю историю вычислительной техники?
71. Какой компьютерный вирус вызвал наиболее масштабную эпидемию за всю историю вычислительной техники?
72. Почему написать вирус для Windows сложнее, чем для MS-DOS?
73. Почему первые макровирусы так широко распространились?
74. Существуют ли психотропные компьютерные вирусы, способные убить человека?
75. Почему люди пишут компьютерные вирусы?
76. Каким требованиям должен удовлетворять эффективно размножающийся компьютерный вирус?
77. Что означает требование универсальности, предъявляемое к компьютерным вирусам?
78. Почему компьютерный вирус не должен повторно заражать одни и те же объекты?
79. Каким требованиям должен удовлетворять компьютерный вирус, эффективно размножающийся в защищенных компьютерных системах?
80. Каким требованиям должен удовлетворять эффективно размножающийся сетевой вирус?
81. Что такое стелс-механизм компьютерного вируса?
82. Чем пассивное размножение компьютерного вируса отличается от активного?
83. К какому классу компьютерных вирусов относится вирус Морриса?
84. Сколько времени обычно требуется для заражения незащищенного компьютера, подключенного к Интернету?
85. Почему прогнозы аналитиков о грядущем «вирусном апокалипсисе» не оправдались?
86. Сколько времени прошло от опубликования уязвимости RPC DCOM Exploit до начала эпидемии вируса MSBlast?
87. Как размножался вирус MSBlast? 88. Какие вредоносные воздействия на зараженные системы осущест- влял вирус MSBlast?
89. Чем отличаются онлайн-вирусы от почтовых вирусов?
90. Каковы основные этапы жизненного цикла онлайн-вируса?
91. В чем состоят достоинства и недостатки онлайн-вирусов по сравне- нию с почтовыми вирусами?
92. Какие методы применяются онлайн-вирусами для получения досту- па к ресурсам компьютеров-жертв?
93. Какой методы получения доступа к ресурсам компьютеров-жертв применяются онлайн-вирусами наиболее часто?
94. Почему большинство онлайн-вирусов функционируют под управлением операционных систем семейства Windows?
95. Каковы основные этапы жизненного цикла почтового вируса?
96. Каким образом почтовые вирусы формируют тему и тело зараженного письма?
97. Как почтовые вирусы чаще всего прикрепляют свое тело к заражен- ному письму?
98. В чем заключается метод прикрепления тела почтового вируса к за- раженному письму, основанный на встроенных кодах HTML?
99. Как почтовые вирусы используют в ходе распространения уязвимости программного обеспечения атакуемых систем?
100. В чем состоит метод прикрепления тела почтового вируса к зараженному письму, основанный на встроенных в письмо ссылках?

101. На какие две группы делятся методы защиты от программных закладок?
102. Что такое принцип минимизации программного обеспечения?
103. Что такое принцип минимизации полномочий?
104. Что такое изолированная программная среда?
105. Какие требования предъявляются к программно-аппаратным средствам антивирусной защиты?
106. Что такое сигнатурное сканирование?
107. В чем заключаются достоинства и недостатки сигнатурного сканирования?
108. Что такое эвристическое сканирование?
109. Каковы достоинства и недостатки эвристического сканирования?
110. Как программные закладки могут защищаться от эвристического сканирования?
111. Как часто должно выполняться антивирусное сканирование?
112. Какие достоинства и недостатки имеет антивирусное сканирование «на лету»?
113. Что такое контроль целостности программного обеспечения?
114. Какие достоинства и недостатки имеет контроль целостности программного обеспечения?
115. Что такое контроль целостности конфигурации системы?
116. Какие ключи реестра Windows наиболее важны с точки зрения за- щиты от программных закладок?
117. Какие достоинства и недостатки имеет контроль целостности кон- фигурации системы?
118. Что такое антивирусный мониторинг?
119. Что такое программные ловушки?
120. Можно ли обеспечить эффективную антивирусную защиту одними лишь программно-аппаратными средствами?
121. Что относится к основным мероприятиям по организационному сопровождению антивирусной защиты?
122. О чем должны быть проинструктированы пользователи сети, оснащенной комплексной системой антивирусной защиты?
123. Как проверяется адекватность поведения лиц, ответственных за обеспечение антивирусной защиты сети, в случае успешных вирусных атак?
124. Как организуется защита от программных закладок ранее неизвестных типов?
125. В чем заключаются инспекции состояния антивирусной защиты?
126. Почему и как антивирусная защита может быть преодолена?
127. Какие мероприятия проводятся в случае обнаружения факта успешного внедрения программных закладок в защищаемую систему?
128. В каких случаях осуществляется выявление программных закладок в ручном режиме?
129. Каковы типичные признаки поражения системы программной закладкой? 130. Как просмотреть список процессов, выполняющихся в операционной системе в данный момент?
131. Как можно отличить вредоносный процесс от нормального?
132. Как с помощью утилиты Process Explorer быстро определить, какие процессы пользуются функциями заданной библиотеки?
133. Как с помощью утилиты Process Explorer быстро определить, какие процессы работают с заданным объектом операционной системы?
134. Почему при ручном обнаружении программных закладок не следует немедленно останавливать обнаруженные вредоносные процессы?
135. Как проще всего найти EXE-файл, посредством которого был по- рожден заданный процесс?
136. Какие свойства процесса позволяет получить утилита Process Explorer?
137. Какие свойства библиотеки позволяет получить утилита Process Explorer?
138. Какими способами можно запретить доступ к обнаруженному вредоносному файлу?

139. Чем правило «запрет запуска программного файла, имеющего за- данную хеш-функцию» отличается от правила «запрет запуска программно- го файла, имеющего заданное имя и расположенного в заданной директории»?
140. Как можно изменить права доступа к файлу, если этот файл не отображается Проводником Windows?
141. Как просмотреть список сервисов (служб) Windows?
142. Какие ключи реестра Windows наиболее часто используются программными закладками для организации автозапуска закладки после пере- загрузки операционной системы?
143. Каковы типичные признаки вредоносного EXE-файла?
144. Как определить, все ли обнаруженные вредоносные программы корректно удалены из системы?
145. Как можно обнаружить файл, скрытый с помощью стелс- технологии?

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знать: Представление о социальной значимости своей будущей профессии Понимание миссии ИТ-прогресса, требующей высокой мотивации к выполнению профессиональной деятельности Уметь: мотивировать выполнение профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, Владеть: нормами профессиональной этики.	Устный опрос. Письменный опрос. Реферат. Доклад. Практическая работа Лабораторная работа
ОПК-3	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знать: основы организации современных ЭВМ и их общие характеристики, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники;	Устный опрос. Письменный опрос. Реферат. Доклад. Практическая работа Лабораторная работа

		Уметь формулировать требования и принимать обоснованные решения по выбору аппаратно-программных средств для рационального решения задач, связанных с получением и преобразованием информации Владеть: практическими навыками по использованию средств вычислительной техники и программного обеспечения для организации обработки информации	
ОПК-4	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: возможности сети Интернет для поиска и обработки данных и организации информационного обмена; Уметь: эффективно использовать возможности современных ПЭВМ, компьютерных сетей и программных средств для решения прикладных задач, возникающих в процессе обучения в вузе и в ходе будущей профессиональной деятельности Владеть: навыками работы со справочно-поисковыми системами в глобальной сети Интернет	Устный опрос. Письменный опрос. Реферат. Доклад. Практическая работа Лабораторная работа
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать: основные положения теории безопасности программ и данных; Уметь: проводить анализ безопасности программ и данных с помощью контрольно-испытательных и логико-аналитических методов, а также сравнивать логико-аналитические и контрольно испытательные методы; Владеет: - методами выявления уязвимости программного обеспечения	Устный опрос. Письменный опрос. Реферат. Доклад. Практическая работа Лабораторная работа
ПК-2	способностью применять	Знает: - основные принципы обеспечения безопасности	Устный опрос. Письменный опрос.

	программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	программ и данных; основные модели поведения программного обеспечения Умеет : оценивать вероятность наличия разрушающего программного обеспечения на этапе испытаний программного обеспечения; оценивать надежность программного обеспечения для контроля его технологической безопасности;- обеспечивать целостность и достоверность используемого программного кода; осуществлять обоснованный выбор средств защиты программ и данных; Владеет методами выявления уязвимости программного обеспечения; основными методами выбора программного обеспечения безопасности компьютерных систем; основными способами защиты программного обеспечения от несанкционированного копирования	Реферат. Доклад. Практическая работа Лабораторная работа

1.6.Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В соответствии с учебным планом предусмотрен экзамен в третьем семестре.
Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине предполагают следующее распределение баллов.
Форма текущего контроля – выполнение семестровых заданий. В течение семестра студент выполняет задания, за каждой из которых получает соответствующие баллы. За выполнение задания студент получает определенное количество баллов. Однотипные задания собраны в разделы.
Форма промежуточного контроля – контрольные, коллоквиум.
Форма итогового контроля, определенная учебным планом, - зачет

7.2. Типовые контрольные задания

Программная закладка - это:
2) Виды негативных воздействий, которые способна оказать программа с потенциально опасными последствиями для программной среды, в которую она внедрена
3) Соотнесите виды программных закладок и их назначение:
4) Какой вид программных закладок наиболее часто используется для снятия защиты копирования:

5) Какой вид программных закладок наиболее часто применяются против операционных систем:
6) Соотнесите методы внедрения программных закладок:
7) Такие программные закладки как мониторы делятся на:
8) Соотнесите методы выявления программных закладок:
9) Соотнесите методы защиты программ от изучения
Вопросы:
10) Программы, которые переводят последовательность машинных кодов в листинг, близкий к исходному тексту программы на языке ассемблера называют ...
11) Программа, которая загружает в память другую программу и предоставляет пользователю возможность наблюдать за ходом выполнения этой программы, называют ...
12) Выберите наиболее распространенные отладчики
13) Виды дизассемблеров:
14) Выберите основные функции отладчиков
1) трассировка
15) Соотнесите этапы анализа программ динамическим методом
16) Выберите наиболее актуальный метод, используемый для восстановления алгоритма защиты
17) При сопряжении защитных механизмов динамические методы анализа программного кода направлены на:
18) Методы защиты программ от изучения:
19) Методы защиты от НСК 1) использование электронных ключей 2) использование ключевых дискет и компакт-дисков 3) привязка к уникальным характеристикам компьютера
20) Методы защита дискет от копирования 1) создание дорожек за пределами рабочей области 2) создание, отличного от стандартного, количества секторов на отдельной дорожке 3) форматирование с использованием фактора чередования и анализ времени доступа к секторам 4) специальное форматирование отдельных дорожек
21) Методы защиты от динамического анализа программ 1) блокировка специальных прерываний 2) анализ времени выполнения отдельных участков программы 3) использование прерываний от таймера 4) блокировка прерываний от клавиатуры
22) Методы противодействия средствам дизассемблирования 1) шифрование отдельных участков программ 2) усложнение структуры программы
23) Методы противодействие модификации программы 1) проверка контрольной суммы файла 2) проверка даты изменения файла
24) Методы защиты от подделки данных 1) криптографический
2) вычисление дополнительной контрольной суммы 3) сокрытие критических данных
25) Задача статического метода анализа программных реализаций
26) Методы защиты от дизассемблеров искажением кода 1) скрытые команды управления 2) перекрывающийся код 3) нестандартный формат загружаемого модуля
27) Отладчик. Основные отладочные средства 1) контрольные точки останова
2) трассировка программы
28) Какие отладчики позволяют наиболее полно проводить анализ работы программ в ОС Windows
29) Распространенные типы программ, осуществляющих разрушающие программные воздействия
30) Классы вирусов по способу заражения 1) резидентные 2) нерезидентные
31) Классы вирусов по среде обитания 1) файловые 2) загрузочные 3) файлово-загрузочные
32) Вирусы в MS-DOS. Места внедрения вирусов в программу 1) начало файла 2) середина файла 3) конец файла
33) Файловые вирусы Windows. Способ обращения к функциям WinApi 1) вычисление адреса загрузки функции
34) Что такое файловый червь

35) Способы маскировки вирусов в Windows 1) создание условий невидимости (steals-технология) 2) шифрование кода 3) полиморфизм
36) Маскировка вирусов в Windows. Принципы обеспечения невидимости (steals-вирусы) 1) перехват обращения ОС к инфицированным файлам 2) передача файлов для просмотра в неинфицированном виде
37) Стандартные программы защиты от вирусов. Основные типы
38) Анализ алгоритмов работы вирусов. Общие задачи исследования 1) способы размножения 2) характер вносимых повреждений 3) метод лечения оперативной памяти 4) метод лечения файлов
39) Классы вирусов по деструктивным возможностям 1) разрушающие различные объекты - программы, данные, системные области 2) неразрушающие
40) Восстановление зараженной вирусом программы при его размещении в конце .exe файла 1) восстановление точки входа в заголовке исполняемого файла

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) Основная литература:

1. Проскурин, Вадим Геннадьевич.
Защита программ и данных : учеб. пособие для студентов вузов / Проскурин, Вадим Геннадьевич. - 2-е изд., стер. - М. : Академия, 2012. - 198,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - ISBN 978-5-7695-9288-1 : 486-20.

2. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных : Учеб. пособие для вузов / П.Ю.Белкин, О.О.Михальский, А.С.Першаков, Д.И.Правиков и др. - М. : Радио и связь, 2000. - 168 с. : ил. - ISBN 5-256-01533-8 : 0-0.

3. Платонов, Владимир Владимирович.
Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обуч. по специальности 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информ. безопасности автоматизированных систем" / Платонов, Владимир Владимирович. - М. : Академия, 2006. - 238,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено УМО. - ISBN 5-7695-2706-4 : 170-50

б) Дополнительная литература:

1. Защита программного обеспечения / Под ред. Д.Гроувера; Пер. с англ. В.Г.Потемкина и др.; Под ред. В.Г.Потемкина. - М. : Мир, 1992. - 288 с. - 45-50.

2. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс]: учебно-методическое пособие/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 218 с.— Режим доступа: http://www.iprbookshop.ru/77317.html.— ЭБС «IPRbooks»

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

1. Электронно-библиотечной системе IPRbooks . Режим доступа: www.iprbookshop.ru
2. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: http://elibrary.ru/defaultx.asp (дата обращения: 01.09.2018). – Яз. рус., англ.
3. Moodle[Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та,

из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/(датаобращения: 22.08.2018).

4. Электронный каталог НБ ДГУ[Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru, свободный (дата обращения: 21.09.2018).
5. Сайт кафедры http://iit.dgu.ru/ (дата обращения 15.09.2018)
6. Национальный Открытый Университет «ИНТУИТ» – http://www.intuit.ru/(дата обращения 15.09.2018)
7. Интернет-энциклопедия «Википедия». – https://ru.wikipedia.org/(дата обращения 15.09.2018)

10. Методические указания для обучающихся по освоению дисциплины.

Лекционный курс. Лекция является основной формой обучения в высшем учебном заведении. В ходе лекционного курса проводится систематическое изложение современных научных материалов.

Студенту необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях. Конспекты лекций следует использовать при подготовке к зачету, контрольным тестам, коллоквиумам, при выполнении самостоятельных заданий.

Специальное руководство, облегчающее работу студента по изучению темы, выдается для пользования на каждом занятии.

Изучив глубоко содержание учебной дисциплины, целесообразно разработать матрицу наиболее предпочтительных методов обучения и форм самостоятельной работы студентов, адекватных видам лекционных и лабораторных занятий.

Необходимо предусмотреть развитие форм самостоятельной работы, выводя студентов к завершению изучения учебной дисциплины на ее высший уровень.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Учебная аудитория, оборудованная мультимедиа проектором. Компьютер под управлением операционной системы Windows 7, 8.0, 8.1, имеющий установленный пакет офисных программ MSOffice 2010, 2013 и Microsoft Visual Studio.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

а) Мультимедийная аудитория - для лекций;

б) Компьютерный класс, оборудованный для проведения практических работ средствами оргтехники, персональными компьютерами, объединенными в сеть с выходом в Интернет – для практических занятий.

Для проведения лекционных занятий требуется аудитория на курс, оборудованная интерактивной доской, мультимедийным проектором с экраном.

Для проведения практических занятий требуется аудитория на группу студентов, оборудованная интерактивной доской, мультимедийным проектором с экраном.

Для проведения практических занятий на ПЭВМ требуется компьютерный класс с установленной на ПЭВМ: 1. Microsoft Office 2. Microsoft Visual Studio.