МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита программ и данных

Кафедра ИТиБКС факультета ИиИТ

Образовательная программа

10.03.01 Информационная безопасность

Профиль подготовки

Безопасность компьютерных

систем

Уровень высшего образования

бакалавриат

Форма обучения

Очная, очно-заочная

Статус дисциплины: входит в обязательную часть ОПОП

Махачкала, 2021

Рабочая программа дисциплины Защита программ и данных составлена в 2021 году в соответствии с требованиями ФГОС ВО - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность от 17 ноября 2020 г. №1427.

Разработчик: Ахмедова Написат Мурадовна, старший преподаватель кафедры информационных технологий и безопасности компьютерных систем.

Рабочая программа одобрена на заседании кафедры информационных технологий и безопасности компьютерных систем 28.06.2021г., протокол № 11.

Зав. кафедрой _____ Ахмедова З.Х.

Рабочая программа одобрена на заседании Методической комиссии факультета информатики и информационных технологий 29.06.2021г., протокол № 11.

Председатель методсовета факультета ИиИТ Бакмаев А.Ш.

Рабочая программа согласована с учебно-методическим управлением 09.07.2021г.,

Начальник УМУ _____ Гасангаджиева А.Г.

Аннотация рабочей программы дисциплины

Дисциплина ***Защита программ и данных*** входит в обязательную часть ОПОП *бакалавриата,* по направлению 10.03.01 Информационная безопасность.

Дисциплина реализуется на факультете ИиИТ кафедрой ИТиБКС.

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.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных – ОПК-1, ОПК-6, ОПК-9, профессиональных – ПК-2.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические 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, в том числе 72 академических часа по видам учебных занятий

Очная форма обучения

Семестр	Учебные занятия в том числе:								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
7	72	58	30		28			14	зачет

Очно-заочной форма обучения

Семестр	Учебные занятия в том числе:								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
7	72	28	14		14			44	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, детальное изучение студентами средств и методов анализа программных реализаций, а также защиты массивов данных, представленных в электронном виде.

2.Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Защита программ и данных входит в обязательную часть ОПОП *бакалавриата,* по направлению 10.03.01 Информационная безопасность

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 выпускных квалификационных работ.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения и процедура освоения).

Код и наименование компетенции из ОПОП	**Код и наименование индикатора достижения компетенций** *(в соответствии с ОПОП*	**Планируемые результаты обучения**	**Процедура освоения**
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИД1.ОПК-1.1.Знать. организационно – правовую основу информационной безопасности и средства ее обеспечения ИД2. ОПК-1.2.Уметь . использовать права и обязанности граждан государства в рамках правового пространства для обеспечения защиты информации Ид3.ОПК-1.3. Владеть навыками оперативного отслеживания нарушений прав пользователей телекоммуникационной системы и анализа информационных процессов в этих системах, способами моделирования информационных процессов в телекоммуникациях	Знает основы математики, физики, вычислительной техники и программирования. Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования. Имеет навыки теоретического и экспериментального исследования объектов профессиональной деятельности	Устный опрос, письменный опрос, практическая работа
ОПК-6 Способен при решении профессиональных	ИД1.ОПК-6.1. Знать: нормативно-правовые основы и документы по проблеме	Знать: нормативно-правовые основы и документы по проблеме организационного обеспечения	Устный опрос, письменный опрос, практическая работа

задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации ИД2.ОПК-6.2.. Уметь: использовать нормативно правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации ИД3.ОПК-6.3. Владеть: навыками работы с нормативно правовыми и организационно распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутри объектового режима.	информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации Уметь: использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации Должен владеть: навыками работы с нормативно правовыми и организационно распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутри объектового режима.	
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД 1 ОПК-9.1.Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности	Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Лабораторно-практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам

	защиты информации Ид 2 ОПК-9.2. Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации ИД 3 ОПК-9.3. Владеет методами и средствами криптографической и технической защиты информации	Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации Владеет методами и средствами криптографической и технической защиты информации	
ПК-2 Проведение работ по установке и техническому обслуживанию защищенных технических средств обработки информации	ПК 2.1. Порядок аттестации объектов информатизации на соответствие требованиям безопасности информации; ПК 2.2.Проводить техническое обслуживание защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно технической документацией ПК 2.3.Способом проведения специальных исследований на побочные электромагнитные излучения и наводки технических средств обработки информации;	Знает: Технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении; Умеет: проводить контроль защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; Владеет: Проведением контроля защищенности акустической речевой информации от утечки по техническим каналам	Лабораторно-практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 2 зачетных единиц, 72 академических часов.

4.2. Структура дисциплины.

4.2.1. Структура дисциплины в очной форме

№ п/п	Разделы и темы дисциплины по модулям	Семестр	Виды учебной работы, включая самостоятельную работу студентов (в часах)					Формы текущего контроля успеваемости и промежуточной аттестации
			Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.	Самостоятельная работа в т.ч. экзамен	
	Модуль 1.							
1	АНАЛИЗ	7	4	4				к/р , тестовый

	ПРОГРАММНЫХ РЕАЛИЗАЦИЙ, ЗАЩИТА ПРОГРАММ ОТ АНАЛИЗА							контроль, устный и письменный опросы
2	Метод экспериментов с «черным ящиком»	7	4	4			2	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
3	Статический метод	7	4	4			2	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
4	Динамический метод	7	4	2			2	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
	Итого по модулю 1:		16	14			6	
	Модуль 2.							
5	Особенности анализа некоторых видов программ	7	4	4			2	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
6	Защита программ от анализа	7	4	4			2	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
7	ПРОГРАММНЫЕ ЗАКЛАДКИ, ПУТИ ИХ ВНЕДРЕНИЯ, СРЕДСТВА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПРОГРАММНЫМ ЗАКЛАДКА	7	4	4			2	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
8	Средства и методы защиты от программных закладок	7	2	2			2	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
	Итого по модулю 2:		14	14			8	
	ИТОГО:		30	28			14	

4.2.2. Структура дисциплины в очно-заочной форме

№ п/п	Разделы и темы дисциплины по модулям	Семестр	Виды учебной работы, включая самостоятельную работу студентов (в часах)					Формы текущего контроля успеваемости и промежуточной аттестации
			Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.	Самостоятельная работа в т.ч. экзамен	
	Модуль 1.							
1	АНАЛИЗ ПРОГРАММНЫХ РЕАЛИЗАЦИЙ, ЗАЩИТА ПРОГРАММ ОТ АНАЛИЗА	7	2	2			4	к/р , тестовый контроль, устный и письменный опросы
2	Метод экспериментов с «черным ящиком»	7	2	2			6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
3	Статический метод	7	2	2			6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
4	Динамический метод	7	2				6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
	Итого по модулю 1:		8	6			22	
	Модуль 2.							
5	Особенности анализа некоторых видов программ	7	2	2			4	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
6	Защита программ от анализа	7	2	2			6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
7	ПРОГРАММНЫЕ ЗАКЛАДКИ, ПУТИ ИХ ВНЕДРЕНИЯ, СРЕДСТВА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ	7	2	2			6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады

	ПРОГРАММНЫМ ЗАКЛАДКА							по темам
8	Средства и методы защиты от программных закладок	7		2			6	практические задания, к/р , тестовый контроль, устный и письменный опросы, доклады по темам
	Итого по модулю 2:		6	8			22	
	ИТОГО:		14	14			44	

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

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1.

Тема 1. АНАЛИЗ ПРОГРАММНЫХ РЕАЛИЗАЦИЙ, ЗАЩИТА ПРОГРАММ ОТ АНАЛИЗА
Общие сведения. Факторы по анализу программных данных. Основные этапы анализа программ. Подходы к восстановлению алгоритмов.

Тема 2. Метод экспериментов с «черным ящиком»
Термин черный ящик. Два варианта задач. Трудности при реализации метода. Типовые примеры экспериментов, позволяющих быстро получить некоторые сведения об анализируемом программном продукте.

Тема 3. Статический метод
Принцип метола. Проблемы, возникающие при практической реализации алгоритмов дизассемблирования. Примеры дизасассемблеров.

Тема 4. Динамический метод
Программные отладочные средства. Методика изучения программ динамическим методом. Метод маяков. Метод Step-Trace первого этапа. Метод аппаратной точки останова. Метод Step-Trace второго этапа. Пример применения динамического метода

Модуль 2.

Тема 1. Особенности анализа некоторых видов программ
Особенности анализа оверлейных программ. Особенности анализа графических программ Windows. Пример анализа графической программы Windows. Особенности анализа параллельного кода. Вспомогательные инструменты анализа программ

Тема 2. Защита программ от анализа
Динамическое изменение кода программы. Искусственное усложнение структуры программы. Нестандартные обращения к функциям операционной системы. Искусственное усложнение алгоритмов обработки данных. Выявление факта выполнения программы под отладчиком.

Тема 3. ПРОГРАММНЫЕ ЗАКЛАДКИ, ПУТИ ИХ ВНЕДРЕНИЯ, СРЕДСТВА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПРОГРАММНЫМ ЗАКЛАДКА

Субъектно-ориентированная модель компьютерной системы. Модели взаимодействия программной закладки с атакуемой системой. Предпосылки к внедрению программных закладок.

Тема 4. Средства и методы защиты от программных закладок
Сканирование системы на предмет наличия известных программных закладок. Контроль целостности программного обеспечения. Контроль целостности конфигурации защищаемой системы. Антивирусный мониторинг информационных потоков
..

4.3.2. Содержание практических 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 эксплуатационная 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.

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

Модуль 2

2.1 Расчет 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.

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

5. **Образовательные технологии**

Предусмотрено сочетание традиционных видов учебной активности, таких как

конспектирование лекций и контроль усвоения теоретического материала в виде коллоквиумов, так и интерактивных технологий, таких как собеседования, ситуационные игры на выбор методов защиты информации на практических занятиях.

Подготовка студентами докладов по темам, не входящим в план лекций, а также выполнение расчетных работ, позволяют расширить научный кругозор студентов, повысить навык работы с учебной и научной отечественной и зарубежной литературой, развить языковые навыки, повысить математическую подготовку, укрепить междисциплинарные связи, повысить навык программирования.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

В соответствии с учебным планом предусмотрен зачет в седьмом семестре. Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине.

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.

Форма промежуточного контроля – контрольные, коллоквиум.

Форма итогового контроля, определенная учебным планом, - зачет.

Темы для самостоятельного изучения:

Наименование темы:	Примерная трудоемкость, а.ч.	
	очная	Очно-заочная
дизассемблеры	4	8
программы отладчики	2	8
оверлейные программы	2	4
программы-мониторы	2	8
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 ошибк	2	8
Средства динамического изменения полномочий	2	8
Итого СРС	14	44

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

7.1. Типовые контрольные задания

ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К ИТОГОВОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

. В чем заключается задача анализа программных реализаций? 2. Почему задача анализа программных реализаций является актуальной? 3. На какие этапы разбивается решение задачи анализа программных реализаций? 4. Какие методы применяются для решение задачи анализа программных реализаций? 5. Почему метод экспериментов с «черным ящиком» так называется? 79 6. В чем состоит суть метода экспериментов с «черным

ящиком»? 7. В чем заключаются достоинства и недостатки метода экспериментов с «черным ящиком»? 8. Какие типичные эксперименты применяются при анализе программ методом экспериментов с «черным ящиком»? 9. Как определить наличие марканта в схеме шифрования архиватора ARJ? 10. Как восстановить схему шифрования, реализуемую архиватором ARJ? 11. В чем заключается статический метод анализа программ? 12. Каковы достоинства и недостатки статического метода? 13. Какие проблемы возникают при дизассемблировании программных файлов? 14. Каковы типичные свойства «глупых» дизассемблеров? 15. Каковы типичные свойства «умных» дизассемблеров? 16. Какие проблемы возникают при изучении аналитиком листингов дизассемблира? 17. Как осуществляется передача параметров в функции программ, написанных на C/C++? 18. Как осуществляется возврат возвращаемого значения функциями программ, написанных на C/C++? 19. Что обозначается черным, темно-синим, светло-синим, зеленым и малиновым цветами в окне IDA View-A дизассемблера IDA? 20. Что такое «режим отображения кода в виде графа» дизассемблера IDA? 21. Что такое Hex-Rays? 22. В чем заключается главное достоинство Hex-Rays по сравнению с дизассемблерами? 23. В чем заключается основной недостаток Hex-Rays? 24. Как загрузить в дизассемблер IDA отладочную информацию в формате PDB? 25. Как пользователь дизассемблера IDA может редактировать листинг, выдаваемый этим дизассемблером? 26. В каких случаях статический метод анализа программных реализаций является наиболее эффективным? 27. Какие программные отладочные средства вы знаете? 28. Что такое флаг трассировки? 29. Что такое программные и аппаратные точки останова? 30. Какие основные функции обычно реализуются отладчиками? 31. В чем состоят достоинства и недостатки динамического метода анализа программных реализаций? 32. Какими основными факторами ограничиваются возможности отладчиков? 33. На какие основные этапы разбивается анализ программы динамическим методом? 34. Что такое метод маяков? 35. Какие участки анализируемой программы обычно используются в роли маяков? 80 36. Какими двумя способами можно устанавливать точки останова на маяки? 37. В чем заключаются достоинства и недостатки этих двух способов? 38. В чем состоит суть метода Step-Trace? 39. Почему при применении метода Step-Trace точки останова следует использовать с осторожностью? 40. Какие основные действия выполняются аналитиком на втором этапе анализа программы динамическим методом? 41. Что такое метод аппаратной точки останова? 42. Чем отличается применение метода Step-Trace на втором этапе анализа программы динамическим методом от применения этого же метода на первом этапе? 43. Что происходит на третьем этапе анализа программы динамическим методом? 44. Как открыть бинарный исполняемый файл отладчиком, встроенным в Microsoft Visual Studio? 45. Какими клавишами осуществляется управление отлаживаемой программой в отладчике, встроенном в Microsoft Visual Studio? 46. Какие окна отладчика, встроенного в Microsoft Visual Studio, целесообразно выводить на экран в ходе анализа программы, исходный текст которой неизвестен? 47. Как в отладчике, встроенном в Microsoft Visual Studio, установить аппаратную точку останова на обращения к заданному буферу с данными? 48. Что происходит в отладчике, встроенном в Microsoft Visual Studio, при срабатывании аппаратной точки останова? 49. Что отображается в окне Call Stack отладчика, встроенного в Microsoft Visual Studio? 50. Как можно повысить удобочитаемость информации, выдаваемой в окно Call Stack отладчиком, встроенным в Microsoft Visual Studio? 51. Почему метод аппаратной точки останова не всегда эффективен? 52. Что означают знаки вопроса, отображаемые в окне дампа памяти отладчика, встроенного в Microsoft Visual Studio? 53. Почему при разных запусках одной и той же программы некоторые буферы могут располагаться по разным адресам оперативной памяти? 54. Что обычно лежит по адресу оперативной памяти [ebp + 8]? 55. Что делает команда lea системы машинных команд процессоров семейства Intel x86? 56. Как утилита ipconfig отличает включенные сетевые адаптеры от выключенных? 57. Почему при анализе оверлейных программ могут теряться точки останова? 58. Как

предотвратить «уход» оверлейной программы из-под отладчика? 59. Сколько точек входа обычно имеет графическая программа Windows? 60. Почему классическая схема применения метода Step-Trace не годится для анализа графических программ Windows? 61. Как можно узнать адрес оконной функции заданного окна графической программы Windows? 81 62. В какое место оконной функции следует ставить точку останова? 63. Как можно узнать адрес диалоговой функции заданного диалогового окна графической программы Windows? 64. Как открыть исполняемый файл в редакторе ресурсов Microsoft Visual Studio? 65. Как отличить модальное диалоговое окно от немодального? 66. Какие системные функции Windows могут применяться для создания диалогового окна? 67. Почему точку останова удобнее ставить не в самое начало анализируемой функции, а после команды mov ebp, esp? 68. Что обычно делает диалоговая функция, получив сообщение WM_ INITDIALOG? 69. Как отличить в скомпилированной программе глобальные переменные от локальных? 70. Как средствами отладчика, встроенного в Microsoft Visual Studio, можно изменить содержимое того или иного участка адресного пространства отлаживаемого процесса? 71. Как проще всего узнать, к каким ключам и значениям реестра Windows обращается анализируемая программа? 72. Какие проблемы возникают при анализе динамическим методом параллельного кода? 73. Что такое системный отладчик?

ПЕРЕЧЕНЬ ТЕМ ДЛЯ РЕФЕРАТОВ

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 субъектноориентированной 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»? 185 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 защищенную 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, запущенную 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 ОК. 39. Перепишите вторую учебную программу с переполнением буфера так, чтобы она использовала вместо функции HeapAlloc функцию LocalAlloc. 186 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 ОК. 41. Для первой учебной программы с переполнением буфера напишите эксплойт, 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? 187 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 осуществлял вирус MSBlast? 89. Чем отличаются онлайн-вирусы от почтовых вирусов? 90. Каковы основные этапы жизненного цикла онлайн-вируса?

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств дисциплины включает в себя контрольные вопросы, задания контрольных работ, вопросы для промежуточной аттестации. Виды самостоятельной работы обучающихся. Изучение основной и дополнительной литературы по материалам курса. Выполнение заданий самостоятельной работы по курсу.

Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабора-торные занятия	Практические занятия	Само-стоя-тельная работа	Автоматизированное тести-рование	Другие виды учебной дея-тельности	Промежуточная аттестация	Итого
7	5		25	25	0	5	40	100

Программа оценивания учебной деятельности студента. Семестр 7

Лекции. Посещаемость, опрос, активность за семестр — от 0 до 5 баллов.

Лабораторные занятия. Выполнение одной лабораторной работы – 10б.

Практические занятия. Посещаемость, опрос, активность за семестр — от 0 до 15 баллов.

Самостоятельная работа. Контроль выполнения заданий самостоятельной работы в течение одного семестра — от 0 до 25 баллов;

Контрольная работа (от 0 до 10 баллов);

Автоматизированное тестирование. **Не предусмотрено.**

Другие виды учебной деятельности.

Написание реферата является одной из форм обучения студентов. Данная форма обучения направлена на организацию и повышение уровня самостоятельной работы студентов. Реферат, как форма обучения студентов - это краткий обзор максимального количества доступных публикаций по заданной теме, подготовка самого реферативного обзора и презентации по нему. При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируется уже сделанные выводы и в связи с небольшим объемом данной формы работы. Преподавателю предоставляется сам реферат в письменной форме (электронная версия в формате Microsoft Word) и презентация к нему (электронная версия в формате PowerPoint). Сдача реферата происходит в форме

защитыдоклада с использованием подготовленной презентации.
Критерии оценки рефератов:
Оценки на "отлично":
10 - тема раскрыта блестяще, презентация является целостным новым независимым дополнением высокого уровня к лекционному курсу
9 - тема раскрыта отлично, есть отдельные фрагменты, которые являются новыми независимыми смысловыми дополнениями к лекциям
8 - тема в основном раскрыта, качество материала высокое, но не является уникальным
Оценки на "хорошо"
7 - тема раскрыта не полностью, не хватает некоторой части. Качество материала хорошее.
6 - тема раскрыта не полностью, не хватает некоторой значимой части.
Удовлетворительно:
5 - раскрыта хотя бы примерно половина темы. Качество материала удовлетворительное.
4 - что-то по существу реферата сказано, но мало и фрагментарно. Качество материала на грани удовлетворительного.
Неудовлетворительно:
3 - понял, о чем надо рассказывать, но практически ничего не рассказал по теме реферата. Качество материала неудовлетворительное.
2 - понял название темы, ничего не рассказал либо рассказывал не о том. Материал фактически отсутствует.
1 - не понял название темы, не рассказывал. Материал фактически отсутствует и не по теме.
0 - реферат не сдавался.
Промежуточная аттестация. Методика оценивания знаний, обучающихся по дисциплине «Защита программ и данных» в ходе промежуточной аттестации:
25-40 баллов:
Ответ студента содержит:
глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
знание концептуально-понятийного аппарата всего курса;
знание монографической литературы по курсу,
также свидетельствует о способности:
самостоятельно критически оценивать основные положения курса;
увязывать теорию с практикой.
15-24 баллов:
Ответ студента свидетельствует:
о полном знании материала по программе;
о знании рекомендованной литературы,
а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.
1-14 баллов:
Ответ студента содержит:
поверхностные знания важнейших разделов программы и содержания лекционного курса;
затруднения с использованием научно-понятийного аппарата и терминологии курса;
стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.
Студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала ставится оценка 0 баллов.
Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за один семестр по дисциплине «Защита программ и данных» составляет 100

баллов.
Итоговой формой контроля знаний, умений и навыков по дисциплине является Экзамен. Зачет проводится в письменной форме. При соответствии ответа учащегося на зачете более чем 51 % критериев из этого списка выставляется оценка «зачтено».

8. Учебно-методическое обеспечение дисциплины.

а) адрес сайта курса
Сайт кафедры: http://iit.dgu.ru/ (дата обращения 15.06.2021)

б) 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). - 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 c.— Режим доступа: http://www.iprbookshop.ru/77317.html.— ЭБС «IPRbooks»

---

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

Примеры описания разных видов наименований учебной литературы:
1) eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: http://elibrary.ru/defaultx.asp (дата обращения: 01.04.2021). – Яз. рус., англ.
2) 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/ (дата обращения: 22.03.2021).
3) Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2021 – Режим доступа: http://elib.dgu.ru, свободный (дата обращения: 21.03.2021).

10. Методические указания для обучающихся по освоению дисциплины.

Практические занятия по дисциплине «Защита программ и данных» служат для

получения практических навыков по применению теоретических знаний, полученных студентами на лекциях, для решения конкретных задач в профессиональной сфере специалистов в области защиты информации.
Для более полного понимания целей, задач и практических результатов теории систем следует: 1) Ознакомиться с дополнительной литературой, особенно с трудами основоположников.
2) Выполнять самостоятельную работу
3) Попытаться в рамках практических занятий полностью выполнить все задания.

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, 8.1,10, имеющий установленный пакет офисных программ MSOffice и Ассемблер TASM, FASM.

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

f) 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, ПЭВМ с установленным ПО:. TASM, FASM

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

Для проведения лабораторных занятий на ПЭВМ требуется компьютерный класс с установленной на ПЭВМ:

1. Microsoft Office
2. Браузер с выходом в интернет.