МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Средства защиты от разрушающих программных компонентов
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Средства защиты от разрушающих программных компонентов» является формирование у будущих специалистов теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач.

Задачи изучения дисциплины. Формирование у студентов теоретических знаний в области средств защиты от разрушающих программных компонентов, а также навыков практического применения полученных знаний. Изучение таких разделов как стохастическая компьютерная вирусология, стохастические разрушающие программные воздействия, симбиотические и распределенные разрушающие программные воздействия, скрытые каналы передачи данных, перспективные методы противодействия вредоносным программам.

Дисциплина направлена на формирование профессиональных (ПК-1) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в часть БЛОКА 1 «Дисциплины (модули)», формируемую участниками образовательных отношений подготовки студентов по специальности 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Безопасность операционных систем», «Безопасность сетей ЭВМ», «Программно-аппаратные средства защиты информации».

Является основой для изучения следующих дисциплин: «Администрирование информационных систем и служб», «Интеллектуальные системы информационной безопасности». Приобретенные знания, могут быть использованы при подготовке и защите выпускной квалификационной работы, при прохождении преддипломной практики, а также в профессиональной деятельности.

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением знаний в области информационной безопасности.

Курс является фундаментом для ориентации студентов в сфере разработки систем информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия, самостоятельная работа студента (108 ак.ч.).

Дисциплина изучается на 5 курсе в 9 семестре. Форма промежуточной аттестации – зачет.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Средства защиты от разрушающих программных компонентов» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен разрабатывать системы защиты информации автоматизированных систем	ПК-1	ПК-1.2 Выполняет проектирование и реализацию системы защиты информации автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 5 зачётных единицы, 180 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		9
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	108	108
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	12	12
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	24	24
Реферат (индивидуальное задание)	12	12
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	18	18
Работа в библиотеке	18	18
Подготовка к зачету	15	15
Промежуточная аттестация – зачет (З)	З	З
Общая трудоемкость дисциплины		
ак.ч.	180	180
з.е.	5	5

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на такие темы:

– тема 1 (Введение. Стохастическая компьютерная вирусология);

– тема 2 (Стохастические разрушающие программные воздействия);

– тема 3 (Симбиотические и распределенные разрушающие программные воздействия);

– тема 4 (Скрытые каналы передачи данных);

– тема 5 (Перспективные методы противодействия вредоносным программам).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Введение. Стохастическая компьютерная вирусология	Введение. Предмет и задачи курса. Разрушающие программные воздействия (РПВ). Классификации. История появления. Структура комплекса программных средств антивирусной защиты. Критерии эффективности программных средств антивирусной защиты. Недостатки существующих средств защиты от РПВ. Перспективные методы защиты от РПВ. Стохастические методы, использующиеся в атаках на компьютерные системы.	10	-	-	Средства защиты компьютера от вирусов. Работа с антивирусными пакетами. Внешняя защита от разрушающих программных воздействий. Работа с программой XSpider.	4 4
2	Стохастические разрушающие программные воздействия	Простой и улучшенный криптотроян. Анонимная кража информации. Криптосчетчик. Конфиденциальное получение информации. Недоказуемое и отрицаемое шифрование. Загрузчик РПВ.	8	-	-	Разработка сигнатурного анализатора файлов с использованием различных хеш-функций	8

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Симбиотические и распределенные разрушающие программные воздействия	Информационный шантаж. Распределенные вычисления. Безопасный выкуп.	6	-	-	Изучение протокола конфиденциального получения информации (private information retrieval) и его модификаций.	6
4	Скрытые каналы передачи данных	История исследования скрытых каналов, современный взгляд на скрытые каналы. Характеристики скрытых каналов. Потайные и побочные скрытые каналы. Скрытые каналы в системах обработки информации. Методы организации локальных скрытых каналов. Методы организации сетевых скрытых каналов.	6	-	-	Моделирование поведения вредоносного программного обеспечения типа «Кейлогер».	8
5	Перспективные методы противодействия вредоносным программам	Иммунологический подход к антивирусной защите. Архитектура компьютерной иммунной системы. Автономность надежной системы защиты.	6	-	-	Анализ трафика протоколов транспортного и сетевого уровней в целях выявления скрытых каналов передачи информации.	6
Всего аудиторных часов		36		-		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ПК-1	Зачет	Комплект контролирующих материалов для зачета

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– реферат – всего 10 баллов;

– расчетно-графическая работа (РГР) – всего 20 баллов;

– лабораторные работы – всего 70 баллов.

Зачет проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Зачет по дисциплине «Средства защиты от разрушающих программных компонентов» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время зачетной недели студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.6), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Расчетно-графическая работа (РГР)

Изучение и реализация протокола конфиденциального получения информации (PIR).

Расчетно-графическая работа №1.

Тема: Организации всех этапов решения прикладных задач с использованием криптографических методов защиты от разрушающих программных воздействий.

Расчетно-графическая работа №2.

Тема: Организации всех этапов решения прикладных задач с использованием математических методов защиты от разрушающих программных воздействий.

6.4 Темы для рефератов (презентаций) – индивидуальное задание

1) Характеристика методов анализа программных реализаций.
2) Особенности анализа кода, выполняющегося в режиме ядра операционной системы.
3) Постановка задачи анализа программных реализаций.
4) Метод экспериментов.
5) Статический метод.
6) Динамический метод.
7) Принципы функционирования отладчиков.
8) Факторы, ограничивающие возможности отладчиков.
9) Метод маяков поиска функций защиты в машинном коде.
10) Метод Step-Trace поиска функций защиты в машинном коде.
11) Анализ потоков данных.
12) Особенности анализа оверлейного кода, параллельного кода.
13) Анализ машинного кода в среде, управляемой сообщениями.
14) Методы защиты программ от дизассемблирования и отладки.

15) Модели взаимодействия программной закладки с атакуемой компьютерной системой.

16) Предпосылки к внедрению и методы внедрения программных закладок.

17) Основные принципы построения политики безопасности, повышающей защищенность от программных закладок.

18) Жизненный цикл компьютерных вирусов.

19) Особенности функционирования компьютерных вирусов.

20) Особенности противодействия вирусам того или иного класса.

6.5 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Введение. Стохастическая компьютерная вирусология)

1) Какие задачи решает курс «Средства защиты от разрушающих программных компонентов»?

2) Какие разрушающие программные воздействия (РПВ) Вам известны?

3) По какой структуре построены комплексы программных средств антивирусной защиты?

4) По каким критериям оценивается эффективность программных средств антивирусной защиты?

5) В чем заключаются недостатки существующих средств защиты от РПВ?

Тема 2 (Стохастические разрушающие программные воздействия)

1) Чем отличаются простой криптотроян от улучшенного?

2) В чем заключается анонимная кража информации?

3) Что из себя представляет криптосчетчик?

4) В чем состоит отличие недоказуемого и отрицаемого шифрования?

5) Что такое загрузчик РПВ.?

Тема 3 (Симбиотические и распределенные разрушающие программные воздействия)

1) Что из себя представляют симбиотические программные воздействия?

2) Что из себя представляют распределенные разрушающие программные воздействия?

3) Что такое информационный шантаж?

4) Для чего могут быть использованы распределенные вычисления?

5) Что такое безопасный выкуп?

Тема 4 (Скрытые каналы передачи данных)

1) Что из себя представляют скрытые каналы?
2) Какие бывают скрытые каналы?
3) Чем отличаются потайные и побочные скрытые каналы?
4) Какие методы организации локальных скрытых каналов Вам известны?
5) Какие методы организации сетевых скрытых каналов Вам известны?

Тема 5 (Перспективные методы противодействия вредоносным программам)

1) В чем заключается иммунологический подход к антивирусной защите?
2) Какие основные свойства иммунной системы Вы знаете?
3) Как представлена архитектура компьютерной иммунной системы?
4) Как обеспечивается автономность надежной системы защиты?
5) Какие технологии эмуляции, на данный момент, находят наибольшее применение?

6.6 Вопросы для подготовки к зачету

1) Чем полиморфные вирусы отличаются от самошифрующихся?
2) Какой метод используется для обнаружения КВ в момент их активизации?
3) Какой метод используется для обнаружения последствий вирусной активности?
4) Какие методы используются для обнаружения КВ до момента их активизации?
5) Какие существуют типы программных средств антивирусной защиты?
6) Что такое вирусная сигнатура?
7) Что такое эвристический признак КВ?
8) Что такое ошибка 1-го рода при работе программных средств антивирусной защиты?
9) Что такое ошибка 2-го рода при работе программных средств антивирусной защиты?
10) Что такое ошибка 3-го рода при работе программных средств антивирусной защиты?
11) Что такое клептографическая атака на криптоалгоритм?
12) Какие криптоалгоритмы могут являться объектом клептографической атаки?

13) Какой пример Вы можете привести клептографической атаки на криптоалгоритм RSA?

14) Как можно защититься от клептографической атаки?

15) Как можно описать клептографическую атаку на криптосистему ЭльГамаля?

16) Как можно описать возможную клептографическую атаку на генератор ПСЧ?

17) Как вы понимаете термин «клептография»?

18) Что такое недоказуемое шифрование?

19) Что такое криптовычисления?

20) Каким образом можно получить запись из базы данных таким образом, чтобы не раскрывать, какая именно запись была получена?

21) Что такое отрицаемое шифрование?

22) Какие программы называют симбиотическими?

23) Каким образом можно использовать сетевые РПВ для проведения распределенных вычислений?

24) Какие методы противодействия автоматической рассылке сообщений вы знаете?

25) В чем различие между принципами недоказуемого и отрицаемого шифрования?

26) Какие свойства естественной иммунной системы присущи существующим средствам антивирусной защиты?

27) Каковы преимущества и недостатки распределенной сетевой системы защиты по сравнению с локальной?

28) Что является главным препятствием к развитию автономных систем защиты информации?

29) Какая из существующих технологий эмуляции в наибольшей мере подходит для исследования поведения вредоносного кода?

30) В чем суть технологии аппаратной виртуализации? Известны ли вам приложения, применяющие данную технологию?

31) Что такое скрытый канал по памяти?

32) Что такое скрытый канал по времени?

33) Какие основные характеристики скрытых каналов используются при их описании?

34) Какое влияние оказывает синхронизация на емкость канала?

35) Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: IP и ICMP?

36) Каким образом можно организовать скрытые каналы на базе стека протоколов TCP/IP: TCP и UDP?

37) Каким образом можно использовать протоколы уровня приложений HTTP и DNS для организации скрытых каналов?

38) Укажите методы противодействия угрозе организации скрытых каналов?

39) В чем состоят главные отличия компилятора от транслятора?

40) Перечислите преимущества трансляторов?

41) Какие интерпретируемые языки вы знаете?

42) Какие возможности предоставляет утилита awk?

43) Почему присутствие команды «rm» является одним из наиболее характерных признаков скрипт-вируса?

44) Какими свойствами должен обладать скрипт-файл, чтобы быть классифицированным как вирус?

45) Что такое уязвимость программного кода?

46) К каким последствиям может привести существование уязвимости в программном коде?

47) Каковы основные причины появления уязвимости в программном коде?

48) В чем суть уязвимости, вызванной переполнением буфера на стеке?

49) К каким последствиям может привести существование уязвимости класса «переполнение кучи»?

50) К каким последствиям может привести существование уязвимостей класса «целочисленное переполнение»?

51) В чем суть уязвимости внедрения команд?

52) К каким последствиям может привести существование уязвимости внедрения SQL-кода?

6.7 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр")/Ю.Н. Сычев. ─ Москва: ИНФРА-М, 2023 . ─ 199 с. : ил. + табл. ─ (Высшее образование: Бакалавриат) . ─ ISBN 978-5-16-014976-9. ил. – 15 экз. + [Электронный ресурс]: https://bookmix.ru/book.phtml?id=3950541 – Режим доступа: для авторизованных пользователей (Дата обращения 26.08.2024).

Дополнительная литература

1. Вавренюк А.Б. Разрушающие программные воздействия: Учебнометодическое пособие/А.Б. Вавренюк, Н.П. Васильев, Е.В. Вельмякина, Д.В. Гуров, М.А. Иванов, И.В. Матвейчиков, Н.А. Мацук, Д.М. Михайлов, Л.И. Шустова; под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011. — 328 с. [Электронный ресурс]: https://dl.libcats.org/genesis/792000/b01732bdd8b0a73317bcda100f5aa225/_as/[A.B._Vavrenyuk,_N.P._Vasilev,_E.V._Velmyakina,_D.(libcats.org).pdf (дата обращения: 26.08.2024).

2. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с. - . [Электронный ресурс]: https://books.ifmo.ru/file/pdf/2372.pdf (дата обращения: 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education.— Текст : электронный.

2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/ .— Текст : электронный.

3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x .— Текст : электронный.

4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red .– Текст : электронный.

5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: http://www.iprbookshop.ru/ . —Текст : электронный.

6. Сайт кафедры ИСИБ http://scs.dstu.education .

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 9.

Таблица 9 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (скамья учебная –20 шт., стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций: *Компьютерные классы (22 посадочных места),* оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	ауд. *207* корп. *4* ауд. *217* корп. *3* ауд. *211* корп. *4*

Лист согласования РПД

Разработал:
ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)

(подпись) Р.Н. Погорелов
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Протокол № 1 заседания кафедры от 27.08. 2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)

(подпись) В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра

(подпись) О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

<table>
<tr><td colspan="2">Номер изменения, дата внесения изменения, номер страницы для внесения изменений</td></tr>
<tr><td>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>