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

Моделирование угроз информационной безопасности
(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 «Моделирование угроз информационной безопасности» является формирование знания теоретических основ моделирования угроз информационной безопасности, изучение методологии системного обеспечения защиты информации, информационных ресурсов и информационных процессов, проведение на основе методов моделирования угроз безопасности вычислительных экспериментов.

Задачи изучения дисциплины. Приобретение студентами знаний, умений и практических навыков, необходимых для понимания обеспечения информационной безопасности открытых информационных систем. Научиться распознавать угрозы безопасности информации в информационной системе, производить тестирование безопасности информационных систем и моделирование атак на веб-приложения.

Дисциплина направлена на формирование общепрофессиональных (ОПК-3) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» 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: «Сети и системы передачи информации», «Безопасность сетей ЭВМ», «Безопасность систем баз данных».

Является основой для изучения следующих дисциплин: «Информационная безопасность открытых информационных систем», «Технология построения защищенных распределенных приложений».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением вычислительных систем.

Курс является фундаментом для ориентации студентов в сфере разработки информационных систем.

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 4 курсе в 8 семестре. Форма промежуточной аттестации – экзамен.

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

Процесс изучения дисциплины «Моделирование угроз информационной безопасности» 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 использовать математические методы необходимые для решения задач профессиональной деятельности	ОПК-3	ОПК-3.1 Осуществляет обоснованный выбор математических методов для решения типовых задач

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 экзамену.

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
		8
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	18	18
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	9	9
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	18	18
Работа в библиотеке	18	18
Подготовка к экзамену	36	36
Промежуточная аттестация – экзамен (Э)	Э	Э
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 3 темы:

– тема 1 (Угрозы безопасности информации в информационной системе);

– тема 2 (Тестирование безопасности информационных систем);

– тема 3 (Моделирование атак на веб-приложения).

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	Угрозы безопасности информации в информационной системе	Модель угроз информационной безопасности в информационных системах. Модель нарушителя информационной безопасности. Актуальные угрозы информации в информационных системах.	4	-	-	Модель угроз информационной безопасности Сбор информации о веб-приложении	4 4
2	Тестирование безопасности информационных систем	Сбор информации о тестируемой системе. Тестирование конфигурации и бизнес-логики. Тестирование политики пользовательской безопасности. Тестирование аутентификации/авторизации. Тестирование механизмов управления сессиями. Тестирование уязвимостей на стороне пользователя.	20	-	-	Анализ защищенности транспортного уровня Изучение защищенности механизма управления доступом Тестирование защищенности механизма управления сессиями	4 4 4

Окончание таблицы 3

1	2	3	4	5	6	7	8
3	Моделирование атак на веб-приложения	Sql-инъекции (SQL-injection). Описание, методы выявления, рекомендации по предупреждению. Межсайтовый скриптинг (XSS). Классификация, способы обнаружения, механизмы проведения. Межсайтовая подделка запросов (CSRF). Особенности реализации. Методы защиты. Удаленное внедрение кода (RCE). Методы удаленного внедрения кода в веб-приложения.	12	-	-	Моделирование атак типа SQL-injection Моделирование XSS атак Поиск уязвимостей к атакам CSRF Анализ уязвимостей к атакам RCE	4 4 4 4
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 5.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-3	Экзамен	Комплект контролирующих материалов для экзамена

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

– реферат – всего 10 баллов;

– лабораторные работы – всего 90 баллов.

Оценка по экзамену 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.

Экзамен по дисциплине «Моделирование угроз информационной безопасности» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 6.

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 Темы для рефератов (презентаций) – индивидуальное задание

1. Угрозы и их источники безопасности информационно - телекоммуникационным системам.
2. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах.
3. Основные задачи обеспечения безопасности информации в информационных системах.
4. Математические метода моделирования угроз.
5. Методы исследования угроз информационной безопасности автоматизированных систем.
6. Использования инструментальных средств для анализа защищенности объектов информатизации.
7. Требования нормативно-методических документов по защите информации. Классический подход. Официальный подход.
8. Организация контроля эффективности защиты объектов информатизации.
9. Формирование модели угроз информационной системе.
10. Определение актуальности угроз.
11. Математические способы анализа защищенности объектов информатизации и информационных систем.
12. Анализ защищенности информационных систем на основе моделирования угроз.
13. Критерии оценки эффективности защищенности информационных систем на основе моделирования угроз.
14. Требования к средствам контроля эффективности защиты информации.
15. Основные подходы к анализу защищенности объектов информатизации средствами контроля.
16. Общая математическая модель защиты информации.
17. Математическая модель Лотки-Вольтерры защиты информации в ИС.
18. Математическая модель Ланчестера защиты информации в ИС.
19. Построение формальной модели защиты ИС.
20. Графовая модель угроз, расчет параметров модели.

21. Требования к средствам контроля эффективности защиты информации.

22. Основные подходы к анализу защищенности объектов информатизации средствами контроля.

23. Организационное обеспечение информационной безопасности.

24. Системы защиты информации в ведущих зарубежных странах.

25. Моделирование систем защиты информации.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Угрозы безопасности информации в информационной системе)

1) Что такое угрозы безопасности информации в информационной системе?

2) В чем заключается процесс определения угроз ИБ в информационной системе?

3) Как оценить возможности нарушителей по реализации угроз безопасности информации?

4) Как оценить вероятности реализации угрозы безопасности информации?

5) Как оценить степени возможного ущерба от реализации угрозы безопасности информации?

Тема 2 (Тестирование безопасности информационных систем)

1) В чем заключается тестирование на проникновение?

2) В чем заключается разница между тестирование сетевого уровня и уровня приложений?

3) Каковы методы аудита при проведении пентеста?

4) Каким образом проводится сбор информации о веб-приложении?

5) Как проводится определение точек входа?

Тема 3 (Моделирование атак на веб-приложения)

1) Что из себя представляют SQL-инъекции?

2) Что такое XSS атаки?

3) Каковы последствия проведения XSS атак?

4) Что такое CSRF-атака?

6.5 Вопросы для подготовки к экзамену

1) Каковы характеристики технического канала утечки информации?

2) Каковы характеристики оптического прибора перехвата речевой информации?

3) Какие принципы выявления закладных устройств оптического перехвата информации Вы знаете?

4) Каковы основные способом борьбы с утечкой информации по оптическим каналам?

5) Какие мероприятия должны быть предусмотрены при построении системы защиты оптических каналов?

6) В чем заключаются сложности определения веб-сервера и фреймворка веб-приложения?

7) В чем заключаются сложности определения веб-приложений на сервере?

8) Как проводится поиск информации в мета-файлах и на веб-сервере?

9) Как производится тестирование конфигурации и инфраструктуры веб-приложения?

10) Что такое «Логирование»?

11) В чем заключаются угрозы от старых версий веб-приложения, скрытых файлов и резервных копий?

12) В чем заключается небезопасное использование методов протокола http?

13) Что из себя представляет механизм HSTS?

14) Что такое «Валидация»?

5) Что из себя представляют SQL-инъекции?

6) Что такое XSS атаки?

7) Каковы последствия проведения XSS атак?

15) Что такое CSRF-атака?

16) Какие методы и способы защиты от SQL-инъекций Вы знаете?

17) Что из себя представляют DOM-модели?

18) Какие методы и способы защиты от XSS атак Вы знаете?

19) Что из себя представляет CSRF-атака?

20) Какие разновидности CSRF-атак Вы знаете?

21) Какие методы и способы защиты от CSRF-атак Вы знаете?

22) Какие основные сетевые механизмы безопасности Вы знаете?

23) Какие компоненты и возможности конфигурации и сборки у архитектура Web приложений J2EE Вы знаете?

24) Какие задачи выполняют органы радиотехнической разведки?

25) Из чего состоит типовой комплекс перехвата радиосигналов?

26) Что такое технические средства приема, обработки, хранения и передачи информации (ТСПИ)?

27) Перечислите технические каналы утечки информации, как они классифицируются в зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата?

28) В чем заключается тестирование на проникновение?

29) В чем заключается разница между тестирование сетевого уровня и уровня приложений?

30) Каковы методы аудита при проведении пентеста?

31) Каким образом проводится сбор информации о веб-приложении?

32) Как проводится определение точек входа?

33) Что такое ВТСС?

34) Что такое случайная антенна?

35) Что такое электромагнитные каналы утечки информации?
36) Что такое параметрические каналы утечки информации?
37) Утечка какого вида информации возможна в материально-вещественном канале?
38) Какой основной объект анализа объекта защиты?
39) Что необходимо для создания полной модели объекта защиты?
40) Какие бывают уровни конфиденциальности информации?
41) Какие объекты обычно указывают на планах этажей зданий?
42) Что определяет уровень конфиденциальности информации?

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Скулябина О.В. Системный анализ в информационной безопасности / О.В. Скулябина, С.Ю.Страхов - Санкт-Петербург: БГТУ "Военмех" им. Д.Ф. Устинова, 2021. - 50 с. [Электронный ресурс]:. – Режим доступа: https://e.lanbook.com/book/220316 (Дата обращения 26.08.2024).

2. «Методика оценки угроз безопасности информации», утв. ФСТЭК России 5 февраля 2021 г.: офи- циальный сайт ФСТЭК России [Электронный ресурс] // Режим доступа: https://fstec.ru/tekhni cheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-etodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021) (Дата обращения 26.08.2024).

3. Лозовецкий В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей/ В.В. Лозовецкий, Е.Г. Комаров, В.В. Лебедев: учебное пособие для вузов. - Санкт-Петербург: Лань, 2023. - 488 с. [Электронный ресурс] – Режим доступа: https://e.lanbook.com/book/352292 (дата обращения: 26.08.2024).

4. 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). – 15 экз.

Дополнительная литература

1. Лабутин Н.Г. Моделирование процессов выявления инцидентов информационной безопасности и реагирования на них / Н.Г. Лабутин, П.В. Костин, Н.Ю. Шадрунова // Труды НГТУ им. Р.Е. Алексеева. 2020. № 4 (131). С. 16-25. [Электронный ресурс]: https://www.elibrary.ru/item.asp?id=44451301 Режим доступа: для авторизованных пользователей (дата обращения: 26.08.2024).

Учебно-методические материалы и пособия

1. Погорелов Р.Н. Моделирование угроз информационной безопасности: методические указания к лабораторным работам [Электронный ресурс] – URL: https://moodle.dstu.education/course Режим доступа: для авториз. пользователей. — Текст: электронный. (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 СКС 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 6.

Таблица 6 – 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.)

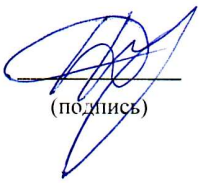
И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)


(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

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	