

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра прикладной механики и компьютерных технологий

УТВЕРЖДАЮ:

Проректор по научно-методической
и учебной работе

Е.И. Скафа

«22» апреля 2020 г.



Рабочая программа учебной дисциплины

«Компьютерная безопасность»

(наименование дисциплины в соответствии с учебным планом)

Направление подготовки:	09.04.04 Программная инженерия
Магистерская программа:	Программная инженерия
Образовательная программа:	академическая магистратура
Квалификация:	магистр
Форма обучения:	очная

Донецк 2020

УТВЕРЖДАЮ:

Декан факультета математики и информационных технологий

И.А. Моисеенко

«16» апреля 2020 г.



Программа составлена на основании Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) направления подготовки 09.04.04 Программная инженерия, утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 932; Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки ДНР № 1171 от «10» ноября 2017 г.; учебного плана и основной образовательной программы Программная инженерия, направления подготовки 09.04.04 Программная инженерия, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

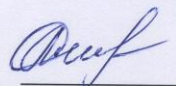
Доцент кафедры ПМиКТ, к.ф.-м.н.

 Н.Н. Щепин

Программа учебной дисциплины утверждена на заседании кафедры прикладной механики и компьютерных технологий
Протокол № 11 от «02» апреля 2020 г.
Заведующий кафедрой

 А.С. Гольцев

Программа учебной дисциплины одобрена учебно-методической комиссией факультета математики и информационных технологий
Протокол № 8 от «15» апреля 2020 г.
Председатель учебно-методической комиссии факультета

 Л.И. Селякова

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Компьютерная безопасность» относится к циклу Дисциплины (модули), Вариативная часть, Обязательные дисциплины. Состоит из двух модулей. Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими и сопутствующими дисциплинами – Информатика, Архитектура компьютеров, Информатика и программирование, Основы программной инженерии, Операционные системы, Компьютерные сети, Защита информации.

Дисциплина «Компьютерная безопасность» является основой для Научно-исследовательской работы (НИР), Производственной (научно-исследовательской) практики и Производственной (преддипломной, подготовки ВКР: магистерской диссертации) практики, связанных с современными сетевыми технологиями. Усвоение основ современных сетевых технологий является обязательным для специалистов в области программной инженерии и информатики.

2. СТРУКТУРА ДИСЦИПЛИНЫ

<i>Характеристика учебной дисциплины</i>		
Направление подготовки	09.04.04 Программная инженерия	
Магистерская программа	Программная инженерия	
Программа подготовки	академическая магистратура	
Квалификация	магистр	
Количество содержательных модулей	2	
Дисциплина базовой / вариативной части образовательной программы	Вариативная часть, обязательные дисциплины	
Формы контроля	1 модульный контроль, экзамен во 2 семестре	
Показатели	очная форма обучения	заочная форма обучения
Количество зачётных единиц (кредитов)	6	
Год подготовки	1	
Семестр	2	
Количество часов	216	
- лекционных	36	
- практических, семинарских	-	
- лабораторных	36	
- самостоятельной работы	144	
в т.ч. индивидуальное задание	–	
Недельное количество часов,	12	
в т.ч. аудиторных	4	

3. ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Цель - подготовка в области применения современных систем информационной безопасности и построения полномасштабной системы безопасности информационной инфраструктуры предприятия.

Задачи – изучение основных организационных и технических систем и средств защиты информации; принципов и методов противодействия несанкционированному доступу к информации; классификации систем и средств обеспечения информационной безопасности; знание базовых принципов функционирования различных систем и средств защиты информации.

Требования к результатам освоения дисциплины: Процесс изучения дисциплины «Компьютерная безопасность» направлен на формирование элементов следующих

компетенций в соответствии с ФГОС ВО РФ направления подготовки 09.04.04 Программная инженерия и основной образовательной программы высшего профессионального образования направления подготовки 09.04.04 Программная инженерия (магистерская программа: Программная инженерия):

а) общепрофессиональных (ОПК):

- *ОПК-2* – способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач;
- *ОПК-3* – способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями;
- *ОПК-5* – способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;
- *ОПК-6* – способен самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности;

б) профессиональных (ПК):

- *ПК-5* – владением существующими методами и алгоритмами решения задач цифровой обработки сигналов;
- *ПК-6* – пониманием существующих подходов к верификации моделей программного обеспечения;
- *ПК-8* – способностью проектировать системы с параллельной обработкой данных и высокопроизводительные системы, и их компоненты;
- *ПК-11* – способностью проектировать основные компоненты операционных систем;
- *ПК-14* – владением навыками программной реализации систем с параллельной обработкой данных и высокопроизводительных систем;
- *ПК-15* – владением навыками создания программного обеспечения для анализа, распознавания и обработки информации, систем цифровой обработки сигналов;
- *ПК-17* – владением навыками создания служб сетевых протоколов;
- *ПК-18* – владением навыками создания компонент операционных систем и систем реального времени;
- *ПК-19* – владением навыками создания систем обработки текстов;
- *ПК-20* – владением навыками организации промышленного тестирования создаваемого программного обеспечения;

В результате изучения учебной дисциплины студент должен

Знать:

- организационные и технические основы систем и средств защиты информации;
- методы и средства противодействия несанкционированному доступу к информации;
- классификацию систем и средств обеспечения информационной безопасности;
- базовые принципы и законы, на которых основано функционирование различных систем и средств защиты информации;

Уметь:

- выявлять возможные способы нарушения информационной безопасности при работе с автоматизированными системами обработки и хранения;
- применять нормативные и правовые базы обеспечения деятельности в области информационной безопасности и защиты информации;
- осуществлять организационные и технические мероприятия по обеспечению информационной безопасности;

Владеть:

- навыками планирования и обеспечения централизованного управления системой безопасности предприятия;
- навыками настройки групповых политик; навыкам настройки служб безопасности систем беспроводной связи;
- навыками построения VPN для обеспечения доступа к сети удаленных пользователей и филиалов;
- навыками обеспечения безопасного доступа к серверам и Internet - ресурсам компании;

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

В рамках изучения дисциплины предусмотрены следующие формы организации учебного процесса: лекции, лабораторные занятия, самостоятельная работа студентов.

Лекционные занятия предполагают овладение теоретическими основами дисциплины, лабораторные – для овладения методами решения задач. Самостоятельная работа студентов предусматривает подготовку к лабораторным занятиям, изучение учебно-методической литературы, составление конспектов, подготовку презентаций и докладов.

Текущий контроль осуществляется путём выполнения индивидуальных заданий по курсу, модульных контрольных работ по проверке теоретических знаний и практических навыков.

В учебном процессе применяются активные и интерактивные формы проведения занятий, внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости, личностно-ориентированное обучение, проблемное обучение.

Материал излагается с использованием объяснительно-иллюстративных, эвристических и исследовательских методов преподавания. При проведении лекции-визуализации для обсуждения материала широко используются мультимедийные презентации, анимации. Также проводятся лекции проблемные, бинарные и с заранее запланированными ошибками.

Порядковый номер и тема	Краткое содержание темы
Содержательный модуль 1	
Тема 1. Основные понятия и принципы информационной безопасности.	Идентификация, аутентификация и авторизация. Модели информационной безопасности. Ущерб и риск. Управление рисками. Типы и примеры атак. Иерархия средств защиты от информационных угроз. Принципы защиты информационной системы. Шифрование — базовая технология безопасности.
Тема 2. Технологии аутентификации, авторизации и управления доступом.	Технологии аутентификации. Технологии управления доступом и авторизации. Системы аутентификации и управления доступом операционных систем. Централизованные системы аутентификации и авторизации.
Тема 3. Технологии безопасности на основе фильтрации мониторинга трафика	Фильтрация. Файерволы. Прокси-серверы. Файерволы с функцией NAT. Программные файерволы хоста. Типовые архитектуры сетей, защищаемых файерволами. Мониторинг трафика. Анализаторы протоколов. Архитектура сети с защитой периметра и разделением внутренних зон. Аудит событий безопасности.

Содержательный модуль 2	
Тема 4. Атаки на транспортную инфраструктуру сети.	TCP-атаки. ICMP-атаки. UDP-атаки. IP-атаки. Сетевая разведка. Атаки на DNS. Безопасность маршрутизации на основе BGP. Технологии защищенного канала.
Тема 5. Безопасность программного кода и сетевых служб	Уязвимости программного кода и вредоносные программы. Безопасность веб-сервиса. Безопасность электронной почты. Облачные сервисы и их безопасность.
Тема 6. Организация виртуальных частных сетей.	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.

Тематический план

Содержательный модуль 1											
Названия содержательных модулей и тем	Количество часов										
	Очная форма обучения						Заочная форма обучения				
	всего	в т.ч.					всего	в т.ч.			
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа
Тема 1. Основные понятия и принципы информационной безопасности.	36	6		6	24						
Тема 2. Технологии аутентификации, авторизации и управления доступом.	36	6		6	24						
Тема 3. Технологии безопасности на основе фильтрации мониторинга трафика	36	6		6	24						
Итого по содержательному модулю 1	108	18		18	72						
Тема 4. Атаки на транспортную инфраструктуру сети.	36	6		6	24						
Тема 5. Безопасность программного кода и сетевых служб	36	6		6	24						
Тема 6. Организация виртуальных частных сетей.	36	6		6	24						

Итого по содержательному модулю 2	108	18		18	72							
Всего часов по модулю	216	36		36	144							

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий

№ п/п	Название темы	Количество часов
1	Основные понятия и принципы информационной безопасности.	6
2	Технологии аутентификации, авторизации и управления доступом.	6
3	Технологии безопасности на основе фильтрации и мониторинга трафика	6
4	Атаки на транспортную инфраструктуру сети	6
5	Безопасность программного кода и сетевых служб	6
6	Организация виртуальных частных сетей	6
	ВСЕГО	36

Темы лабораторных занятий

№ п/п	Название темы	Количество часов
1	Консоль управления ММС	6
2	Администрирование системных элементов Windows 7.	6
3	Администрирование параметров безопасности Windows 7	6
4	Настройка паролей Windows	6
5	Захват сетевого трафика	6
6	Анализ сетевого трафика	6
	ВСЕГО	36

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Организация самостоятельной работы студентов

№ п/п	Название темы	Количество часов
1	Основные понятия и принципы информационной безопасности.	24
2	Технологии аутентификации, авторизации и управления доступом.	24

3	Технологии безопасности на основе фильтрации мониторинга трафика	24
4	Атаки на транспортную инфраструктуру сети	24
5	Безопасность программного кода и сетевых служб	24
6	Организация виртуальных частных сетей	24
	ВСЕГО	144

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Индивидуальная работа № 1

Цель: изучение администрирования системных элементов Windows 7.

Задание: настроить локальные групповые политики Windows по приведенному сценарию.

Индивидуальная работа № 2

Цель: изучение администрирования параметров безопасности Windows 7.

Задание: настроить параметры безопасности Windows по приведенному сценарию.

Индивидуальная работа № 3

Цель: изучение настройки паролей Windows.

Задание: настроить локальные групповые политики Windows по приведенному сценарию.

8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Идентификация, аутентификация и авторизация.
2. Модели информационной безопасности.
3. Ущерб и риск.
4. Управление рисками.
5. Типы и примеры атак.
6. Иерархия средств защиты от информационных угроз.
7. Принципы защиты информационной системы.
8. Шифрование — базовая технология безопасности.
9. Технологии аутентификации.
10. Технологии управления доступом и авторизации.
11. Системы аутентификации и управления доступом операционных систем.
12. Централизованные системы аутентификации и авторизации.
13. Фильтрация.
14. Файерволы.
15. Прокси-серверы.
16. Файерволы с функцией NAT.
17. Программные файерволы хоста.
18. Типовые архитектуры сетей, защищаемых файерволами.
19. Мониторинг трафика.
20. Анализаторы протоколов.
21. Архитектура сети с защитой периметра и разделением внутренних зон.
22. Аудит событий безопасности.

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

<i>Направление подготовки:</i>	09.04.04 Программная инженерия
<i>Магистерская программа:</i>	Программная инженерия
<i>Программа подготовки:</i>	академическая магистратура
<i>Семестр</i>	2
<i>Учебная дисциплина</i>	Компьютерная безопасность

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА

ВАРИАНТ №1

1. Идентификация, аутентификация и авторизация.
2. Мониторинг трафика.
3. Управление рисками.

Утверждено на заседании кафедры прикладной механики и компьютерных технологий
 Протокол № ___ от «___» _____ 20__ г.

Заведующий кафедрой _____ Гольцев А. С.

Преподаватель _____ Щепин Н. Н.

Критерии оценивания модульного контроля

<i>Номер задания</i>	<i>Количество баллов</i>
1	10
2	10
3	10
Всего	30

10. Образец экзаменационного билета

Теоретические вопросы к экзамену

1. Идентификация, аутентификация и авторизация.
2. Модели информационной безопасности.
3. Ущерб и риск.
4. Управление рисками.
5. Типы и примеры атак.
6. Иерархия средств защиты от информационных угроз.
7. Принципы защиты информационной системы.
8. Шифрование — базовая технология безопасности.
9. Технологии аутентификации.
10. Технологии управления доступом и авторизации.
11. Системы аутентификации и управления доступом операционных систем.
12. Централизованные системы аутентификации и авторизации.
13. Фильтрация.
14. Файерволы.

15. Прокси-серверы.
16. Файерволы с функцией NAT.
17. Программные файерволы хоста.
18. Типовые архитектуры сетей, защищаемых файерволами.
19. Мониторинг трафика.
20. Анализаторы протоколов.
21. Архитектура сети с защитой периметра и разделением внутренних зон.
22. Аудит событий безопасности.
23. TCP-атаки.
24. ICMP-атаки.
25. UDP-атаки.
26. IP-атаки.
27. Сетевая разведка.
28. Атаки на DNS.
29. Безопасность маршрутизации на основе BGP.
30. Технологии защищенного канала.
31. Уязвимости программного кода и вредоносные программы.
32. Безопасность веб-сервиса.
33. Безопасность электронной почты.
34. Облачные сервисы и их безопасность.
35. Задачи, решаемые VPN.
36. Туннелирование в VPN.
37. Уровни защищенных каналов.
38. Защита данных на канальном уровне.

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

<i>Направление подготовки:</i>	09.04.04 Программная инженерия
<i>Магистерская программа:</i>	Программная инженерия
<i>Программа подготовки:</i>	академическая магистратура
<i>Семестр</i>	2
<i>Учебная дисциплина</i>	Компьютерная безопасность

БИЛЕТ №1

1. Атаки на DNS..
2. Мониторинг трафика.
3. Задачи, решаемые VPN.

Утверждено на заседании кафедры прикладной механики и компьютерных технологий
 Протокол № ___ от «___» _____ 20__ г.

Заведующий кафедрой _____ Гольцев А. С.

Экзаменатор _____ Щепин Н. Н.

Критерии оценивания экзамена

<i>Номер задания</i>	<i>Количество баллов</i>
1	15
2	15
3	20
Всего	50

11. Критерии оценивания

По курсу предполагается проведение промежуточной аттестации в виде модульного контроля, выполнение индивидуальных заданий и экзамена. Экзамен сдают студенты с целью повышения рейтинга

Распределение баллов, которые могут получить студенты в процессе изучения дисциплины

Организационно учебная работа студента	СРС			Всего
	Индивидуальная работа	Модульный контроль	Индивидуальная творческая работа	
Мах 20 баллов	мах 30 баллов	мах 30 баллов	мах 20 баллов	100 баллов
Активность на лабораторных занятиях	Выполнение индивидуальных заданий	Выполнение модульной контрольной работы	Разработка доклада на студенческую научную конференцию	

Шкала соответствия баллов национальной шкале

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале (экзамен, дифференцированный зачет)	Оценка по государственной шкале (зачет)
A	90-100	5 (отлично)	зачтено
B	80-89	4 (хорошо)	зачтено
C	75-79	4 (хорошо)	зачтено
D	70-74	3 (удовлетворительно)	зачтено
E	60-69	3 (удовлетворительно)	зачтено
FX	35-59	2 (неудовлетворительно) с возможностью повторной сдачи	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

12. Материально-техническое обеспечение учебного процесса

Лабораторные занятия проводятся в компьютерном классе, оборудованном компьютерами с сетевым программным обеспечением, столами, доской.

13. Рекомендованная литература

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
<i>Основная литература</i>			
1.	Современные сетевые технологии и компьютерная безопасность: учебное пособие / Сост.: Н.Н. Щепин, С.А. Приيمنко, Р.Н. Нескороев. – Донецк: ДонНУ, 2019. – 158 с.	-	+

2.	Компьютерная безопасность: учебно-методическое пособие / Сост.: Н.Н. Щепин. – Донецк: ДонНУ, 2019. – 84 с.	-	+
3.	Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Москва [и др.] : Питер, 2010. - 943 с.	27	-
Дополнительная литература			
4.	Таненбаум, Э. С. Компьютерные сети / Э. С. Таненбаум, Д. Уэзеролл ; [пер. с англ. А. Гребеньков]. - 5-е изд. - Санкт-Петербург [и др.] : Питер, 2012. - 955 с.	4	-
5.	Олифер, В. Г. Сетевые операционные системы : [Учеб. пособие для студентов вузов по направлению подгот. дипломир. специалистов "Информатика и вычислительная техника] / В. Г. Олифер, Н. А. Олифер. - СПб. и др. : Питер, 2003. - 538 с.	70	-
6.	Спортак, М. Компьютерные сети и сетевые технологии : Platinum Editions / М. Спортак, Ф. Ч. Паппас, Р. Пит и др. - М. : DiaSoft, 2005. - 720 с.	3	-

14. Информационные ресурсы

1. Компьютерные сети и технологии
<http://www.xnets.ru/>
2. Компьютерные сети и безопасность
<https://habr.com>

15. Программное обеспечение

Стандартное программное обеспечение Microsoft Office, системы анализа сетевого трафика, сетевое программное обеспечение.

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной механики и компьютерных технологий с изменениями (без изменений) на 20____ год.

Протокол заседания кафедры № ____ от ____.

Зав. кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной механики и компьютерных технологий с изменениями (без изменений) на 20____ год.

Протокол заседания кафедры № ____ от ____.

Зав. кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной механики и компьютерных технологий с изменениями (без изменений) на 20____ год.

Протокол заседания кафедры № ____ от ____.

Зав. кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры прикладной механики и компьютерных технологий с изменениями (без изменений) на 20____ год.

Протокол заседания кафедры № ____ от ____.

Зав. кафедрой _____