

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
«Защита информации»

Направление подготовки:	09.03.04 Программная инженерия
Профиль подготовки:	Программная инженерия
Образовательная программа:	бакалавриат
Квалификация:	Академический бакалавр
Форма обучения:	<u>очная, очно-заочная, заочная, в том</u> <u>числе с ускоренным сроком обучения</u> нужное подчеркнуть

Донецк 2020

УТВЕРЖДАЮ:

Декан факультета математики
и информационных технологий

И. А. Моисеенко

«06» апреля 2020

МП

Программа учебной дисциплины «Защита информации» составлена на основании Государственного образовательного стандарта высшего профессионального образования (ГОС ВПО) Донецкой Народной Республики (ДНР) по направлению подготовки 09.03.04 Программная инженерия, утверждённого приказом Министерства образования и науки ДНР от 21 января 2016 г. № 33;

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 высшего профессионального образования направления подготовки 09.03.04 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

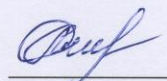
Протокол № 11 от «02» апреля 2020 г.

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 «Защита информации» относится к циклу вариативной части профессионального блока и 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.

2. Структура дисциплины

<i>Характеристика учебной дисциплины</i>				
Направление подготовки	09.03.04 Программная инженерия			
Профиль	Программная инженерия			
Образовательная программа	Бакалавриат			
Квалификация	Академический бакалавр			
Количество содержательных модулей	2			
Дисциплина базовой / вариативной части образовательной программы	Дисциплина вариативной части			
Формы контроля (МК, экзамен, зачет)	модульный контроль, экзамен			
Показатели	очная форма обучения		заочная форма обучения	
	нормат. срок	ускор. срок	нормат. срок	ускор. срок
Количество зачётных единиц (кредитов)	5	5	5	–
Год подготовки	4	4	4	–
Семестр	7	7	7	–
Количество часов	180	180	180	–
- лекционных	32	32	10	–
- практических, семинарских	–	–	–	–
- лабораторных	48	48	10	–
- самостоятельной работы	100	100	160	–
в т.ч. индивидуальное задание	–	–	–	–
Недельное количество часов,	11,25	11,25	–	–
в т.ч. аудиторных	5	5	–	–

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 направлен на формирование элементов следующих компетенций по данному направлению подготовки (профилю):

а) общекультурных (ОК):

способностью к самоорганизации и самообразованию (ОК-7);

б) общепрофессиональных (ОПК):

владением основными концепциями, принципами, теориями и фактами, связанными с информатикой (ОПК-1);

способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять её в требуемом формате с использованием информационных, компьютерных и сетевых технологий (ОПК-4).

в) профессиональных (ПК):

организационно-управленческая деятельность:

владением методами управления процессами разработки требований, оценки рисков, приобретения, проектирования, конструирования, тестирования, эволюции и сопровождения (ПК-7);

сервисно-эксплуатационная деятельность:

владением основными концепциями и моделями эволюции и сопровождения программного обеспечения (ПК-10);

научно-исследовательская деятельность:

готовностью обосновать принимаемые проектные решения, осуществлять постановку и выполнение экспериментов по проверке их корректности и эффективности (ПК-14);

аналитическая деятельность:

способностью формализовать предметную область программного проекта и разработать спецификации для компонентов программного продукта (ПК-16).

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

Курс дисциплины "Защита информации" предусматривает следующие формы организации учебного процесса: лекции, лабораторные занятия, самостоятельная работа студента.

Материал излагается с использованием объяснительно-иллюстративных, эвристических и исследовательских методов преподавания. При проведении лекций для обсуждения материала широко используются мультимедийные презентации и раздаточные материалы. В учебном процессе широко применяются активные и интерактивные формы проведения занятий (разбор конкретных ситуаций, дискуссия, полемика), внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости, личностно-ориентированное обучение, проблемное обучение, блочно-модульное обучение. В учебном процессе используются интернет-ресурсы по данному курсу; рассматриваются задачи, максимально приближенные к конкретным практическим ситуациям.

Самостоятельная работа студентов предусматривает выполнение индивидуальных заданий, подготовку к лабораторным занятиям, изучение учебной и методической литературы, составление конспектов.

Порядковый номер и тема	Краткое содержание темы
Содержательный модуль 1.	
Тема 1. Компьютерная система и защита информации.	Основные понятия информационной безопасности. Основные требования по информационной безопасности к автоматизированным системам. Нормативная база информационной безопасности.
Тема 2. Методы защиты информации.	Основные методы защиты информации. Идентификация и аутентификация пользователя. Ограничение и разграничение доступа. Регистрация событий (аудит). Криптографическая защита. Контроль целостности. Комплексный подход к защите информации.
Тема 3. Классификация и общая характеристика программно-аппаратных средств защиты информации.	Классификация средств защиты информации. Средства криптографической защиты. Средства защиты от несанкционированного доступа. Средства защиты информации сетевого действия.
Содержательный модуль 2.	
Тема 4. Защита компьютерной сети с помощью межсетевых экранов.	Понятие брандмауэра. Компоненты брандмауэра. Политика межсетевого экранирования.
Тема 5. Организация виртуальных частных сетей.	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.
Тема 6. Аудит информационной безопасности компьютерных сетей.	Понятие аудита информационной безопасности. Методика проведения инструментальных проверок. Анализ защищенности web – серверов.

Тематический план

	Содержательный модуль 1																					
Названия содержательных модулей и тем	Количество часов																					
	Очная форма обучения												Заочная форма обучения									
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения			
	всего	в т.ч.					всего	в т.ч.					всего	в т.ч.					всего	в т.ч.		
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная		лекции	практические	лабораторные	самостоятельная работа	индивидуальная		лекции	практические	лабораторные	самостоятельная работа	индивидуальная		лекции	практические	самостоятельная работа
Тема 1. Компьютерная система и защита информации.	16	4			12		16	4			12	–	24	4			20	–	–	–	–	–
Тема 2. Методы защиты информации.	32	6		12	14		32	6		12	14	–	34	2		2	30	–	–	–	–	–
Тема 3. Классификация и общая характеристика программно-аппаратных средств защиты информации.	32	6		12	14		32	6		12	14	–	32			2	30	–	–	–	–	–
Итого по содержательному модулю 1	80	16		24	40		80	16		24	40	–	90	6		4	80	–	–	–	–	–

Содержательный модуль 2																						
Тема 4. Защита компьютерной сети с помощью межсетевых экранов.	24	4			20		24	4			20	–	22	2			20	–	–	–	–	–
Тема 5. Организация виртуальных частных сетей.	38	6		12	20		38	6		12	20	–	36	2		4	30	–	–	–	–	–
Тема 6. Аудит информационной безопасности компьютерных сетей.	38	6		12	20		38	6		12	20	–	32			2	30	–	–	–	–	–
Итого <i>по содержательному</i> <i>модулю 2</i>	100	16		24	60		100	16		24	60	–	90	4		6	80	–	–	–	–	–
Всего по дисциплине	180	32		48	100		180	32		48	100		180	10		10	160					

5. Методические рекомендации для проведения лабораторных, практических и семинарских занятий

Темы лекционных занятий

<i>№ п/п</i>	<i>Название темы</i>	<i>Количество часов</i>
1	Компьютерная система и защита информации.	4
2	Методы защиты информации.	6
3	Классификация и общая характеристика программно-аппаратных средств защиты информации.	6
4	Защита компьютерной сети с помощью межсетевых экранов.	4
5	Организация виртуальных частных сетей.	6
6	Аудит информационной безопасности компьютерных сетей.	6
	ВСЕГО	32

Темы лабораторных занятий

<i>№ п/п</i>	<i>Название темы</i>	<i>Количество часов</i>
1	Консоль управления MMC	12
2	Администрирование параметров безопасности Windows	12
3	Настройка паролей Windows	12
4	Захват сетевого трафика	12
	ВСЕГО	48

6. Методические рекомендации по организации самостоятельной работы студентов

Организация самостоятельной работы студентов

<i>№ п/п</i>	<i>Название темы</i>	<i>Количество часов</i>
1	Компьютерная система и защита информации.	12
2	Методы защиты информации.	14
3	Классификация и общая характеристика программно-аппаратных средств защиты информации.	14
4	Защита компьютерной сети с помощью межсетевых экранов.	20
5	Организация виртуальных частных сетей.	20
6	Аудит информационной безопасности компьютерных сетей.	20
	ВСЕГО	100

7. Контрольные вопросы к промежуточной аттестации

1. Компьютерная система и защита информации.
2. Типичные требования к защите компьютерной системы.

3. Идентификация и аутентификация пользователей.
4. Ограничение доступа на вход в систему.
5. Разграничение доступа к информации.
6. Дискреционная модель разграничения доступа.
7. Мандатная модель разграничения доступа.
8. Регистрация событий аудит.
9. Криптографическая защита данных.
10. Классификация криптографических алгоритмов.
11. Контроль целостности данных.
12. Управление политикой безопасности.
13. Уничтожение остаточной информации.
14. Классификация программно-аппаратных средств защиты информации. Состав комплексных систем защиты.
15. Системы криптозащиты и системы защиты от несанкционированного доступа.

8. Образец модульного контроля

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки:	09.03.04 Программная инженерия
Магистерская программа:	Программная инженерия
Программа подготовки:	бакалавриат
Семестр	7
Учебная дисциплина	Защита информации

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА

ВАРИАНТ №1

1. Мандатная модель разграничения доступа.
2. Регистрация событий аудит.
3. Компьютерная система и защита информации.

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

Заведующий кафедрой _____ **Гольцев А. С.**
(подпись) (фамилия и инициалы)

Преподаватель _____ **Щепин Н. Н.**
(подпись) (фамилия и инициалы)

Критерии оценивания модульного контроля

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

9. Образец экзаменационного билета

Теоретические вопросы к экзамену

1. Компьютерная система и защита информации.
2. Типичные требования к защите компьютерной системы.
3. Идентификация и аутентификация пользователей.
4. Ограничение доступа на вход в систему.
5. Разграничение доступа к информации.
6. Дискреционная модель разграничения доступа.
7. Мандатная модель разграничения доступа.
8. Регистрация событий аудит.
9. Криптографическая защита данных.
10. Классификация криптографических алгоритмов.
11. Контроль целостности данных.
12. Управление политикой безопасности.
13. Уничтожение остаточной информации.
14. Классификация программно-аппаратных средств защиты информации. Состав комплексных систем защиты.
15. Системы криптозащиты и системы защиты от несанкционированного доступа.
16. Понятие межсетевого экрана. Политика межсетевого экранирования.
17. Компоненты межсетевого экрана.
18. Архитектура межсетевых экранов.
19. Основные функции VPN.
20. Туннелирование в VPN. Уровни защищенных каналов.
21. Защита данных на канальном уровне в VPN.
22. Применение МЭ на основе двудомного узла.
23. Применение МЭ на основе фильтрующего маршрутизатора.
24. Применение МЭ на основе экранирующего узла.
25. Применение технологии трансляции сетевых адресов.
26. Использование сканеров безопасности.
27. Анализ защищенности web-серверов.
28. Применение технологии терминального доступа.
29. Проектирование защиты IIS.
30. Создание концептуального плана защиты сетевой инфраструктуры
31. Проектирование логической защитной инфраструктуры
32. Проектирование физической защиты для инфраструктуры сети
33. Администрирование системы безопасности с помощью сетевых политик

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Направление подготовки:

09.03.04 Программная инженерия

Магистерская программа:

Программная инженерия

Программа подготовки:

бакалавриат

Семестр

7

Учебная дисциплина

Защита информации

БИЛЕТ №1

1. Применение технологии трансляции сетевых адресов.
2. Использование сканеров безопасности.
3. Анализ защищенности web-серверов.

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

Заведующий кафедрой _____ **Гольцев А. С.**
 (подпись) (фамилия и инициалы)

Экзаменатор _____ **Щепин Н. Н.**
 (подпись) (фамилия и инициалы)

Критерии оценивания экзамена

Номер задания	Количество баллов
1	15
2	15
3	20
Всего	50

10. 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
----------	------	---	------------

11. Материально-техническое обеспечение учебного процесса

Лекционные, практические и лабораторные занятия проводятся в компьютерном классе, оборудованном компьютерами с лицензионным программным обеспечением, доступом к сети Интернет, столами, доской.

12. Рекомендованная литература

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
Основная литература			
1.	Современные сетевые технологии и компьютерная безопасность: учебное пособие / Сост.: Н.Н. Щепин, С.А. Прийменко, 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

1. Windows 7 PRO (корпоративная лицензия ДОННУ № 46484614);
2. Microsoft Office (корпоративная лицензия ДОННУ лицензия № 46472919);
3. Системы анализа сетевого трафика, сетевое программное обеспечение.

Рабочая программа рассмотрена и переутверждена на заседании кафедры с изменениями (без изменений) на 20____ год. Протокол заседания кафедры № ____ от ____ .
Зав. кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры с изменениями (без изменений) на 20____ год. Протокол заседания кафедры № ____ от ____ .
Зав. кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры с изменениями (без изменений) на 20____ год. Протокол заседания кафедры № ____ от ____ .
Зав. кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры с изменениями (без изменений) на 20____ год. Протокол заседания кафедры № ____ от ____ .
Зав. кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры с изменениями (без изменений) на 20____ год. Протокол заседания кафедры № ____ от ____ .
Зав. кафедрой _____