МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ:
Первый проректор ДОННТУ

_____ А.А. Каракозов
(подпись)

«31» марта 2023 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.07 Защита информации в компьютерных системах
(код и наименование дисциплины согласно учебному плану)

Направление подготовки 09.03.01 «Информатика и вычислительная техника»
(код и наименование направления подготовки / специальности)

Профили: Компьютерная инженерия, Системное программирование, Компьютерные системы цифровой экономики
(наименование профиля / магистерской программы /специализации)

Программа: Бакалавриат
(бакалавриат, магистратура, специалитет)

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

Форма обучения	Очная	Заочная
Семестр(ы)	7	10
Общая трудоёмкость в ЗЕТ/часах	3,0/108	3,0/108
Контактная работа (час.), в том числе:	55	20
лекции (час.)	34	8
лабораторные работы (час.)	17	6
практические (семинарские) занятия (час.)	-	-
Самостоятельная работа (час.), в том числе:	17	52
курсовой проект (работа) (семестр/час.)	-	-
Контроль (экзамен, час./зачёт)	экзамен, 36	экзамен, 36

Донецк, 2023 г.

Рабочая программа дисциплины *Защита информации в компьютерных системах (КС)* составлена в соответствии с учебным планом по направлению подготовки 09.03.01 «Информатика и вычислительная техника» профили «Компьютерная инженерия», «Системное программирование», «Компьютерные системы цифровой экономики» для 2023 года приёма по очной и заочной формам обучения.

Составитель:
старший преподаватель
кафедры «Компьютерная инженерия» _____ Достлев Ю.С.
(подпись) (Ф.И.О.)

Рабочая программа **рассмотрена и принята** на заседании кафедры «Компьютерная инженерия».
Протокол от «21» марта 2023 года № 8

Заведующий кафедрой _____ Аноприенко А.Я.
(подпись)

Рабочая программа **одобрена учебно-методической комиссией** ГОУВПО «ДОННТУ» по направлению 09.03.01 «Информатика и вычислительная техника».
Протокол от «21» марта 2023 года № 4

Председатель _____ Аноприенко А.Я.
(подпись)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Компьютерная инженерия».
Протокол от «_____» _____20___ года № _____

Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Компьютерная инженерия».
Протокол от «_____» _____20___ года № _____

Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Компьютерная инженерия».
Протокол от «_____» _____20___ года № _____

Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20___ года приёма на заседании кафедры «Компьютерная инженерия».

Протокол от «_____» _____20___ года № _____

Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)

1. ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина **рассматривает** вопросы формирования у студентов, обучающихся по направлению подготовки 09.03.01 «Информатика и вычислительная техника», теоретических и практических навыков построения и оценки параметров систем защиты информации. Особое внимание уделено организационным вопросам и вопросам обеспечения безопасности информационных каналов.

Целью дисциплины является: изучение основных принципов, методов, систем и средств, составляющих защиту информации: теоретические основы и формальные модели защиты информации; способы оценки защищенных систем; правовое регулирование в области защиты информации; средства проектирования и реализации программно-аппаратных средств защиты программ и данных; методы применения программно-аппаратных средств защиты информации в операционных системах и вычислительных сетях; криптографические методы защиты информации.

Задачи освоения дисциплины: дать теоретические знания в области построения систем защиты информации компьютерных систем; обучить навыкам работы с нормативными документами, отражающими требования к структурам и уровням защиты информации; познакомить с методами анализа функционирования систем защиты информации и практикой принятия обоснованных решений модернизации существующих систем защиты информации с целью повышения уровня защиты.

В результате освоения дисциплины студент должен:

знать: действующую законодательную базу в области информационной безопасности, теоретический аппарат и формальные модели защиты информации; стандартные криптографические решения для защиты информации, оценку их качества; программно-аппаратные средства и методы защиты информации;

уметь: использовать средства и возможности современных ЭВМ и сетей, микропроцессоров, операционных систем, для проектирования и реализации средств обеспечения информационной безопасности; применять системный подход к обеспечению защиты информации; практически решать задачи защиты программ и данных программно-аппаратными средствами;

владеть: основными принципами определяющими уровень информационной защищенности компьютерных систем; навыками выбора методов решения практических и исследовательских задач на основе фундаментальных знаний в области защиты информации; навыками выбора метода анализа особых ситуаций и нарушений в области защиты информации; навыками оценки результатов работы информационной защиты и составления обоснованного прогноза совершенствования уровня защиты.

Перечисленные результаты обучения являются основой для формирования следующих **компетенций:**

- способен использовать современные информационные технологии программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности **(ОПК-2);**

- способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий (**ОПК-3);**

- способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (**ОПК-4);**

- способен разрабатывать алгоритмы и программы, пригодные для практического применения **(ОПК-8).**

2. МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к циклу профессиональной подготовки базовой части обязательного блока дисциплин учебного плана.

Базируется на знаниях и умениях, которые студент приобрел при освоении предшествующих дисциплин: “Математика” - все разделы; “Дискретная математика” - все разделы; “Системное программирование” - все разделы; “Системное программное обеспечение” - все разделы; “Программирование” - все разделы.

Знания и умения, приобретенные при освоении данной дисциплины необходимы специалистам в области программной и компьютерной инженерии для практической работы в условиях рыночной экономики.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Распределение учебных часов по темам дисциплины и видам занятий

№ темы	Наименование темы (содержательных модулей)	Количество часов (очная / заочная форма)				
		Всего	В том числе			
			Лекции	Лабор.	Практ.	СР
1	Тема 1. Правовое и организационное обеспечение информационной безопасности	6/3	4/1	2/0	0/0	2/9
2	Тема 2. Теоретические основы компьютерной безопасности. Основные методы нарушения целостности информации.	11/6	6/1	3/1	0/0	3/11
3	Тема 3. Защита программ от разрушающих программных влияний.	15/18	4/1	3/1	0/0	3/9

№ темы	Наименование темы (содержательных модулей)	Количество часов (очная / заочная форма)				
		Всего	В том числе			
			Лекции	Лабор.	Практ.	СР
	Вирусы.					
4	Тема 4. Программно-аппаратные методы и способы защиты программ и данных	18/18	7/1	3/1	0/0	3/9
5	Тема 5. Разработка и применение базовых алгоритмов сжатия информации системы	12/14	8/3	3/3	0/0	3/5
6	Тема 6. Криптографические методы и способы защиты информации	12/13	5/1	3/0	0/0	3/9
Контактная работа (дополнительная)		4/6				
Курсовой проект		0/0				0/0
Итого по видам занятий		72/72	34/8	17/6	0/0	17/52
Контроль		36/36				
ИТОГО		**108/108**				

Формирование компетенций в результате освоения тем дисциплины

Компетенции	Темы дисциплины, нацеленные на выработку компетенции
ОПК-1	Тема 2, 4, 5
ОПК-2	Тема 1, 2
ОПК-3	Тема 1, 2, 3
ОПК-8	Тема 3, 5. 6

3.2. Лекции

Тема 1. *Правовое и организационное обеспечение информационной безопасности.*

Содержание темы 1:

Информация как объект защиты. Нормативные документы - источники требований и норм защиты информации. Основные организационные мероприятия повышения информационной безопасности.

Литература к теме 1: [1, 6]

Тема 2. *Теоретические основы компьютерной безопасности. Основные методы нарушения целостности информации.*

Содержание темы 2:

Критерии оценки информационной безопасности. Политика безопасности. Гарантированность.

Литература к теме 2: [1, 5, 9]

Тема 3. *Защита программ от разрушающих программных влияний. Вирусы*

Содержание темы 3:

Форматы исполнимых файлов в разных операционных системах. Загрузочные и встроенные компьютерные вирусы. Известные структуры и способы заражения программ.

Литература к теме 3: [1, 5, 7, 9]

Тема 4. *Программно-аппаратные методы и способы защиты программ и данных*

Содержание темы 4:

Технические способы и методы защиты информации - электронные ключи. Программно-аппаратные методы: ограничения доступа к файлам, компонентам ЭВМ, привязка программного обеспечения к системному окружению, хранение ключевой информации.

Литература к теме 4: [1, 5, 9]

Тема 5. *Разработка и применение базовых алгоритмов сжатия информации*

Содержание темы 5:

Обратимое – необратимое сжатие. Спастические и алфавитные методы сжатия. Деревья Хаффмана и методы арифметического кодирования. Статические и адаптивные модели.

Литература к теме 5: [1, 5, 6, 9]

Тема 6. *Криптографические методы и способы защиты информации*

Содержание темы 6:

Основные понятия криптографии. Симметричные и ассиметричные криптосистемы. Блочные и потоковые методы шифрования. Методы формирования ключей шифрования. Синхронные и самосинхронизирующиеся ключи. Методы шифрования с открытыми и закрытыми ключами.

Литература к теме 6: [2, 3, 6, 7, 9]

3.3 Практические (семинарские) занятия

В учебном плане не запланировано.

3.4. Лабораторные работы

№ п/п	Тема работы	Объем, час. очн/ заочн	Литература
1	Исследование целостности исполнимых файлов в разных операционных системах.	4/1	[1, 2, 5]
2	Исследование алгоритма заражения файлов простым вирусом.	4/1	[7,9]
3	Разработка и исследование алгоритмов сжатия данных.	4/1	[1,5,9]
4	Разработка и исследование криптографических	5/1	[7,9]

	алгоритмов с открытыми ключами.		
Итого:		**17/4**	

3.5. Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час очная/заочная
1	Изучение лекционного материала	8/18
2	Подготовка к практическим занятиям	0/0
3	Подготовка к лабораторным занятиям	9/18
4	Выполнение курсового проекта	0/0
5	Выполнение индивидуального задания	0/16
ИТОГО:		17/52

3.6 Курсовой проект (работа), индивидуальное задание

Учебным планом курсовое проектирование не запланировано.

Индивидуальная расчетно - программная работа посвящена разработке, верификации и исследованию программы, которая реализует индивидуально заданный алгоритм симметричного блочного шифрования - расшифрования –9 часов.

Тематика индивидуального задания связана с самостоятельным изучением теоретических вопросов по тематике дисциплины.

Рекомендуемый объем отчета по расчетно – программной работе – не более 10 страниц формата А4 (210×297 мм).

4 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

4.1 Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Составляющая компетенции – полнота знаний

– нулевой уровень: неверные, не аргументированные, с множеством грубых ошибок ответы на вопросы. Уровень знаний ниже минимальных требований;

– минимальный уровень: даны неполные, неточные и неаргументированные ответы на вопросы. Допущено много грубых ошибок. Уровень знаний ниже минимальных требований;

– пороговый уровень: даны недостаточно полные, точные и аргументированные ответы на вопросы. Плохо знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено много негрубых ошибок;

– средний уровень: даны достаточно полные, точные и аргументированные ответы на вопросы. В целом знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;

– продвинутый уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;

– высокий уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько неточностей.

Составляющая компетенции – умения

– нулевой уровень: полное отсутствие понимания сути методики решения задачи, допущено множество грубейших ошибок / задания не выполнены вообще;

– минимальный уровень: слабое понимание сути методики решения задачи, допущены грубые ошибки. Решения не обоснованы. Не умеет использовать нормативно-техническую литературу. Не ориентируется в специальной научной литературе;

– пороговый уровень: достаточное понимание сути методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую литературу. Слабо ориентируется в специальной научной литературе;

– средний уровень: в целом понимает суть методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую и специальную научную литературу;

– продвинутый уровень: в целом понимает суть методики решения задачи, допущены неточности. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу;

– высокий уровень: Понимает суть методики решения задачи. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу, передовой опыт.

Составляющая компетенции – владение навыками

– нулевой уровень: не демонстрирует владение навыками выполнения профессиональных задач. Не может выполнить задания;

– минимальный уровень: не демонстрирует владение навыками выполнения профессиональных задач. Испытывает существенные трудности при выполнении отдельных заданий;

– пороговый уровень: владеет навыками выполнения профессиональных задач на пороговом уровне. Задания выполняет медленно и некачественно;

– средний уровень: владеет навыками выполнения профессиональных задач. Задания выполняет на среднем уровне по быстроте и качеству;

– продвинутый уровень: владеет уверенными навыками выполнения профессиональных задач. Быстро и качественно выполняет задания, иногда допуская незначительные погрешности;

– высокий уровень: владеет уверенными навыками выполнения профессиональных задач. Быстро и качественно выполняет задания, при необходимости демонстрируя творческий подход.

Обобщенная оценка сформированности компетенций

– нулевой уровень: на нулевом уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– минимальный уровень: на минимальном уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– пороговый уровень: на пороговом уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– средний уровень: на среднем уровне сформированы: все составляющие; одна или две из трёх, остальные – на более высоком уровне;

– продвинутый уровень: на продвинутом уровне сформированы: все составляющие; одна или две из трёх, остальные – на высоком уровне;

– высокий уровень: на высоком уровне сформированы все составляющие компетенций.

4.2 Вопросы к экзамену и пример экзаменационного билета

Вопросы к экзамену:

1. Основные уровни защиты компьютерных и информационных ресурсов.
2. Определить структуру и содержание метки безопасности при принудительном управлении доступом
3. Детализировать основные элементы политики безопасности в соответствии с «Желтой книгой».
4. Понятие информационной безопасности и ее цель.
5. Основные технологии, которые использовались при компьютерных преступлениях.
6. Признаки, свидетельствующие о наличии поражаемых мест в информационной защите.
7. Меры защиты информационной безопасности.
8. Правила и администрирование защиты паролей.
9. Критерии оценки информационной надежности.
10. Политика безопасности надежных информационных систем.
11. Гарантированность надежных информационных систем.
12. Основные требования к мониторам обращений.
13. Основные элементы политики безопасности.
14. Произвольное управление доступом в системах защиты информации.

15. Принудительное управление доступом в системах защиты информации.
16. Архивация как форма защиты, кодирование по алгоритму RLE.
17. Архивация как форма защиты, метод Хаффмана.
18. Архивация как форма защиты, метод арифметического кодирования.
19. Основные понятия и классификация современных криптосистем.
20. Симметричные криптосистемы.
21. Блочные шифры.
22. Асимметрические криптосистемы.
23. Особенности и примеры алгоритмов ассиметричного шифрования

Пример экзаменационного билета:

ГОУВПО «Донецкий национальный технический университет»

Уровень высшего профессионального образования:	бакалавриат
Направление подготовки (специальность):	09.03.01 «Информатика и вычислительная техника»
Профиль (магистерская программа, специализация):	«Вычислительные машины, комплексы, системы и сети» «Программное обеспечение средств вычислительной техники»
Семестр:	8
Учебная дисциплина:	Защита информации в КС

БИЛЕТ № ___61____

1. Основные требования к мониторам обращений в системах защиты информации

2. Основные технологии, которые использовались при компьютерных преступлениях.

3. Закодировать сообщение «северс» алгоритмом арифметического кодирования.
Привести все этапы сжатия и восстановления.

Утверждено на заседании кафедры компьютерной инженерии

Протокол № X от XX.XX.20XX г.

Зав. кафедрой

Экзаменатор

4.3 Критерии оценивания

Оценивание уровня освоения студентом учебного материала дисциплины «Защита информации в компьютерных системах» производится в ходе текущего контроля и промежуточной аттестации (экзамена).

Текущий контроль знаний студента очной формы обучения осуществляется по результатам посещения лекций, выполнения заданий на лабораторных занятиях, выполнения индивидуального задания. Выполнение заданий на лабораторных занятиях и индивидуального задания являются необходимым условием допуска к экзамену студентом очной формы обучения. Итогом текущего контроля знаний студентов является выполнение экзаменационного задания, выполнение которого является обязательным для получения оценки по экзамену.

Текущий контроль студента заочной формы обучения осуществляется по результатам выполнения и защиты индивидуального задания. Выполнение студентом индивидуального задания является обязательным условием для получения допуска к экзамену. Итогом текущего контроля знаний студентов заочной формы обучения, является выполнение экзаменационного задания, выполнение которого является обязательным для получения оценки по экзамену.

Распределение баллов текущего контроля работы студента на протяжении семестра:

Форма контроля	Возможное количество баллов	Примечание
Для студентов очной формы обучения		
Отчёт о выполнении лабораторной работы	**5**	Работа выполнена правильно, соотношения полученных количественных значений параметров обоснован, приведен анализ полученного результата. Отчет защищен своевременно – по плану выполнения лабораторных работ.
	2	Задание выполнено в целом правильно, рекомендации не всегда обоснованы, возникли трудности в объяснении полученных результатов или отчет предоставлен и защищен с задержкой – с отставанием от плана выполнения лабораторных работ.
Итого по лабораторным занятиям (максимально возможное)	**20**	Из расчёта 4 лабораторных занятий. Оценивается каждое занятие.
Выполнение	**10**	При выполнении задания получены

Форма контроля	Возможное количество баллов	Примечание
индивидуального задания		правильные значения, изложение материала аргументированное, последовательное, работа оформлена грамотно, работа защищена уверенно
	5	Задание выполнено в целом правильно, результаты не всегда обоснованы, имеются замечания по оформлению работы и защите работы
Итого по домашним заданиям	**10**	Максимально возможное. Из расчёта одного индивидуального задания.
Посещение лекционного и лабораторного занятия	**1**	Студент конспектирует материал лекции, активно участвует в обсуждении вопросов на лабораторном занятии
	0,5	Студент опоздал на лекцию (пришел после переклички) или пассивно присутствует на лекции – не все конспектирует или не участвует в обсуждении вопросов на лабораторном занятии
Итого по посещению лекционных и лабораторных занятий (максимально возможное)	**20**	Из расчета 20 лекционных и лабораторных занятий. Оценивается каждое занятие
Выполнение экзаменационного задания	Оценка ответа на теоретические вопросы экзаменационного билета	
	20	Вопросы освещены полностью, выводы аргументированы (максимальная оценка)
	10	Вопросы освещены не в полной мере или с допущением ошибок
	Оценка выполнения практического задания экзаменационного билета	
	30	Задание выполнено правильно, выполнен анализ полученных результатов (максимальная оценка)
	10	Задание выполнено с ошибками, но с использованием правильных

Форма контроля	Возможное количество баллов	Примечание
		алгоритмов, допущены ошибки в количественных значениях получаемых значений
Итого по выполнению экзаменационного задания (максимально возможное)	**50**	Максимально возможное
ИТОГО	**100**	Максимально возможное
Для студентов заочной формы обучения		
Индивидуальное задание	**40**	При выполнении задания получены правильные результаты и обоснованы их значения, изложение материала аргументированное, последовательное, работа оформлена грамотно, работа защищена уверенно
	20	Задание выполнено в целом правильно, полученные результаты не всегда обоснованы, имеются замечания по оформлению работы и защите работы
Итого по индивидуальному заданию	**40**	Максимально возможное
Выполнение экзаменационного задания	Оценка ответа на теоретические вопросы экзаменационного билета	
	20	Вопросы освещены полностью, выводы аргументированы (максимальная оценка)
	10	Вопросы освещены не в полной мере или с допущением ошибок
	Оценка выполнения практического задания экзаменационного билета	
	40	Задание выполнено правильно, выполнен анализ полученных результатов (максимальная оценка)
	20	Задание выполнено с ошибками, но с использованием правильных алгоритмов, допущены ошибки в количественных значениях получаемых значений
Итого по	**60**	Максимально возможное

Форма контроля	Возможное количество баллов	Примечание
выполнению экзаменационного задания (максимально возможное)		
ИТОГО	**100**	Максимально возможное

Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме экзамена. По результатам работы в семестре суммируются баллы за посещение лекций и лабораторных занятий, за выполнение и защиту отчетов по лабораторным занятиям, за выполнение индивидуального задания и экзаменационного задания.

Таким образом, **итоговая оценка** для студентов очной и заочной форм обучения определяется путем суммирования количества баллов по результатам текущего контроля.

Максимально возможное количество баллов – 100.

Полученная оценка по 100-балльной шкале определяет оценку по государственной шкале и шкале ESTS:

Сумма баллов по 100-бальной шкале	Оценка по шкале ECTS	Оценка по государственной шкале
90-100	A	Зачтено
80-89	B	
75-79	C	
70-74	D	
60-69	E	
35-59	FX	Не зачтено
0-34	F*	

* – с обязательным повторным изучением дисциплины.

4.4 Пример текущего опроса на лабораторных занятиях

На примере темы «Исследование алгоритма заражения файлов простым вирусом»:

1. Возможное размещение вирусного программного кода в объеме программы?
2. Способы получения управления вирусного кода.
3. Способы «заражения» файлов простейшими вирусами.
4. Возможные механизмы распространения – «размножения» вирусов.
5. Алгоритмические основы идентификации заражения файлов простейшими вирусами.

4.5 Курсовое проектирование

Учебным планом курсовое проектирование не запланировано.

5 РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

I Основная литература

1. Фомин Д.В. Информационная безопасность : учебник / Фомин Д.В.. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118876.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/118876

2. Фомин Д.В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства : практикум / Фомин Д.В.. — Саратов : Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/110329.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/110329

3. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н.А. Руденков [и др.].. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102207.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей

4. Ревнивых А.В. Информационная безопасность в организациях : учебное пособие / Ревнивых А.В.. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108227.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/108227

5. Мэйволд Э. Безопасность сетей : учебное пособие для СПО / Мэйволд Э.. — Саратов : Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102183.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей

II Дополнительная литература

6. Основы теории информации : учебное пособие для СПО / Д.Н. Резеньков [и др.].. — Саратов : Профобразование, 2022. — 100 с. — ISBN 978-5-4488-1537-9. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/122433.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/122433

7. Куликов С.С. Информационная безопасность глобальных компьютерных сетей : практикум / Куликов С.С.. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2021. — 66 с. — ISBN 978-5-7731-0970-9. — Текст : электронный // IPR SMART : [сайт]. — URL:

https://www.iprbookshop.ru/118613.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей

8. Куликов С.С. Информационная безопасность локальных компьютерных сетей : практикум / Куликов С.С.. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2021. — 57 с. — ISBN 978-5-7731-0969-3. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118614.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей

9. Теория информации : учебное пособие / Д.Н. Резеньков [и др.].. — Москва : Ай Пи Ар Медиа, 2022. — 132 с. — ISBN 978-5-4497-1698-9. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/122434.html (дата обращения: 03.06.2022). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/122434

6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебно-методические издания, разработанные в ДонНТУ:

10. Конспект лекций по дисциплине «Защита информации в компьютерных системах» [Электронный ресурс]: для обучающихся по образовательной программе «бакалавриат» направления подготовки 09.03.01 «Информатика и вычислительная техника» всех форм обучения / ГОУВПО «ДОННТУ», Фак. интеллект. систем и программир., каф. комп. инженерии ; [сост. Ю. С. Достлев]. – Донецк : ГОУВПО «ДОННТУ», 2023 (доступ через личный кабинет студента)

11. Методические указания к лабораторным занятиям по дисциплине «Защита информации в компьютерных системах» [Электронный ресурс]: для обучающихся по образовательной программе «бакалавриат» направления подготовки 09.03.01 «Информатика и вычислительная техника» всех форм обучения / ГОУВПО «ДОННТУ», Фак. интеллект. систем и программир., каф. комп. инженерии ; [сост. Ю. С. Достлев]. – Донецк : ГОУВПО «ДОННТУ», 2023 (доступ через личный кабинет студента)

Электронно-информационные ресурсы

ЭБС ДОННТУ – http://donntu.org/library
ЭБС IPR book – http://www.iprbookshop.ru

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1Лекционные занятия:

Учебная аудитория № 4.37 учебный корпус 4 для проведения занятий лекционного и практического типа, групповых и индивидуальных консультаций, текущего контроля. Мультимедийное оборудование: ноутбук, ОС – Windows 7 максимальная (академическая подписка DreamSparkPremium), LibreOffice 4.3.2.2

(лицензия GNULGPLv3+ и MPL2.0), мультимедийный проектор, экран; специализированная мебель: доска аудиторная, парты, демонстрационные стенды и плакаты.

7.2 Лабораторные занятия:

Учебная аудитория №4.40 учебный корпус 4, для проведения лабораторных работ, индивидуальных консультаций, текущего контроля и промежуточной аттестации. Используется специализированная мебель: доска аудиторная, столы аудиторные, столы компьютерные, стулья ученические и компьютерная техника с возможностью подключения к сети «Интернет» - 6ПК Celeron 2,0GZ,RAM 256,HDD 40Gb; программное обеспечение: ОС Windows 7, UBUNTU (бесплатная версия 18.04);

7.3 Самостоятельная работа:

Помещения для самостоятельной работы с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации: читальные залы, учебные корпуса 2,3 (Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ДОННТУ) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств. ОС – Microsoft Windows 7, OpenOffice 2.0.3 – общественная лицензия MPL 2.0/ Grub loader for ALT Linux - лицензия GNU LGPL v3/ Mozilla Firefox - лицензия MPL2.0, Moodle (Modular Object-Oriented Dynamic Learning Environment) - лицензия GNU GPLect-OrientedDynamicLearning Environment, лицензия GNUGPL).