МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ"

Факультет **Факультет государственной службы и управления**

Кафедра **Информационных технологий**

"УТВЕРЖДАЮ"
Проректор
_____Л.Н. Костина
27.04.2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.18 **"Информационная безопасность"**

Направление подготовки 09.03.03 Прикладная информатика
Профиль "Прикладная информатика в управлении корпоративными информационными системами"

Квалификация ***Бакалавр***

Форма обучения ***очная***

Общая трудоемкость ***6 ЗЕТ***

Год начала подготовки по учебному плану ***2024***

Донецк
2024

Составитель(и):
канд. техн. наук, доцент _____И.Л.Семичастный И.Л.

Рецензент(ы):
канд. экон. наук, доцент _____Е.Г.Литвак

Рабочая программа дисциплины (модуля) "Информационная безопасность" разработана в соответствии с:

Федеральным государственным образовательным стандартом высшего образования – бакалавриата по направлению подготовки 09.03.03 Прикладная информатика (Приказ Министерства образования и науки Российской Федерации от 19.09.2017 г. № 922 с изменениями).

Самостоятельно установленным образовательным стандартом по направлению подготовки высшего образования 09.03.03 Прикладная информатика (приказ ФГБОУ ВО «РАНХиГС» от 07.09.2023 г № 01-24607)

Рабочая программа дисциплины (модуля) составлена на основании учебного плана Направление подготовки 09.03.03 Прикладная информатика

Профиль "Прикладная информатика в управлении корпоративными информационными системами", утвержденного Ученым советом ФГБОУ ВО "ДОНАУИГС" от 27.04.2024 протокол № 12.

Срок действия программы: 2024-2028

Рабочая программа рассмотрена и одобрена на заседании кафедры Информационных технологий

Протокол от 16.04.2024 № 9

Заведующий кафедрой:
Брадул Н.В. _____
(подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025 - 2026 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2025 г. №__

Зав. кафедрой Брадул Н.В. _____ (подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026 - 2027 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2026 г. №__

Зав. кафедрой Брадул Н.В. _____ (подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027 - 2028 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2027 г. №__

Зав. кафедрой Брадул Н.В. _____ (подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028 - 2029 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2028 г. №__

Зав. кафедрой Брадул Н.В. _____ (подпись)

РАЗДЕЛ 1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ

1.1. ЦЕЛИ ДИСЦИПЛИНЫ

Сформировать знания о принципах и способах противодействия опасностям и угрозам, возникающим в процессе развития современного информационного общества в сфере информационной безопасности.

1.2. УЧЕБНЫЕ ЗАДАЧИ ДИСЦИПЛИНЫ

- ознакомить студентов с современными технологиями, применяемыми в решении задач информационной безопасности, моделями возможных угроз, нормативными документами, терминологией и основными понятиями теории защиты информации;
- приобрести практические навыки анализа и выбора методов и средств защиты компьютерной информации.

1.3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОПОП ВО:	Б1.О

1.3.1. Дисциплина "Информационная безопасность" опирается на следующие элементы ОПОП ВО:

Вычислительные системы, сети и телекоммуникации

Базы данных

Информационные системы и технологии

1.3.2. Дисциплина "Информационная безопасность" выступает опорой для следующих элементов:

ИТ инфраструктура предприятия

Корпоративные информационные системы

1.4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

ОПК-3.1: Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать:

Уровень 1	нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий
Уровень 2	виды угроз ИС
Уровень 3	методы обеспечения информационной безопасности

Уметь:

Уровень 1	использовать нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий для организации защиты информации
Уровень 2	применять методы анализа прикладной области на концептуальном, логическом, и алгоритмическом уровнях с целью выявления угроз безопасности
Уровень 3	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

Владеть:

Уровень 1	международными и отечественными стандартами в области обеспечения безопасности информационных систем и технологий
Уровень 2	способностью блокировать угрозы безопасности ИС предприятия с помощью методов обеспечения защиты информации
Уровень 3	навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности

1.4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

ОПК ОС-10.1: Разрабатывает и реализует алгоритмы решения комплекса задач, связанных с обеспечением безопасности в процессе создания, эксплуатации и развития прикладных информационных систем

Знать:

Уровень 1	типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду
Уровень 2	методы защиты информации в вычислительных системах и сетях

Уровень 3	типовые средства защиты информации в вычислительных системах и сетях
Уметь:	
Уровень 1	использовать типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду
Уровень 2	использовать типовые программно-аппаратные средства и системы зашиты информации от нарушения ее целостности
Уровень 3	использовать методы защиты информации в вычислительных системах и сетях
Владеть:	
Уровень 1	навыками работы с методами и типовыми средствами защиты информации в системах и сетях
Уровень 2	типовыми программно-аппаратными средствами обеспечения доступности информации
Уровень 3	навыками использования типовых программно-аппаратных средств и систем зашиты информации от несанкционированного доступа в компьютерную среду

В результате освоения дисциплины "Информационная безопасность" обучающийся должен:

3.1	**Знать:**
	нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий.
3.2	**Уметь:**
	использовать нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий для организации защиты информации.
3.3	**Владеть:**
	международными и отечественными стандартами в области обеспечения безопасности информационных систем и технологий.

1.5. ФОРМЫ КОНТРОЛЯ

Текущий контроль успеваемости позволяет оценить уровень сформированности элементов компетенций (знаний, умений и приобретенных навыков), компетенций с последующим объединением оценок и проводится в форме: устного опроса на лекционных и семинарских/практических занятиях (фронтальный, индивидуальный, комплексный), письменной проверки (тестовые задания, контроль знаний по разделу, ситуационных заданий и т.п.), оценки активности работы обучающегося на занятии, включая задания для самостоятельной работы.

Промежуточная аттестация

Результаты текущего контроля и промежуточной аттестации формируют рейтинговую оценку работы студента. Распределение баллов при формировании рейтинговой оценки работы студента осуществляется в соответствии с действующим локальным нормативным актом. По дисциплине "Информационная безопасность" видом промежуточной аттестации является Экзамен

РАЗДЕЛ 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. ТРУДОЕМКОСТЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Общая трудоёмкость дисциплины "Информационная безопасность" составляет 6 зачётные единицы, 216 часов.

Количество часов, выделяемых на контактную работу с преподавателем и самостоятельную работу обучающегося, определяется учебным планом.

2.2. СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
Раздел 1. Технологии и методы обеспечения ИБ						
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России . /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.2 Э1 Э2 Э3	0	

Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России . /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.3 Э1 Э2 Э3	0	
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России . /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.2 Л3.4 Э1 Э2 Э3	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.1 Э1 Э2 Э3	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.2Л3.2 Л3.3 Э1 Э2 Э3	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.4Л3.2 Л3.4 Э1 Э2 Э3	0	
Тема 1.3. Угрозы информационной безопасности . /Лек/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.2Л3.2 Э1 Э2 Э3	0	
Тема 1.3. Угрозы информационной безопасности . /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.3Л3.2 Л3.3 Э1 Э2 Э3	0	
Тема 1.3. Угрозы информационной безопасности . /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.3Л3.4 Э1 Э2 Э3	0	
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии /Лек/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.1Л3.2 Э1 Э2 Э3	0	
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии /Пр/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.4Л3.3 Э1 Э2 Э3	0	
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии /Ср/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.1Л3.4 Э1 Э2 Э3	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.2Л3.2 Э1 Э2 Э3	0	

Тема 1.5. Технологии защиты от вредоносных программ и спама. /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.3Л3.3 Э1 Э2 Э3	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Ср/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.3Л2.3Л3.4 Э1 Э2 Э3	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Лек/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.4Л3.2 Э1 Э2 Э3	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Пр/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.2Л3.3 Э1 Э2 Э3	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.4Л3.4 Э1 Э2 Э3	0	
Раздел 2. Технология защиты информации						
Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.1Л3.1 Л3.5 Э1 Э2 Э3	0	
Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.2Л3.2 Э1 Э2 Э3	0	
Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия /Ср/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.3Л3.3 Э1 Э2 Э3	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.4Л3.4 Э1 Э2 Э3	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.1Л3.5 Э1 Э2 Э3	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.2Л3.1 Э1 Э2 Э3	0	

Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Лек/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.2 Э1 Э2 Э3	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.4Л3.3 Э1 Э2 Э3	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.1Л3.4 Э1 Э2 Э3	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.2Л3.5 Э1 Э2 Э3	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.3Л3.1 Э1 Э2 Э3	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.4Л3.2 Э1 Э2 Э3	0	
Тема 2.5. Международные стандарты ИБ. COBIT /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.1Л3.3 Э1 Э2 Э3	0	
Тема 2.5. Международные стандарты ИБ. COBIT /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.2Л3.4 Э1 Э2 Э3	0	
Тема 2.5. Международные стандарты ИБ. COBIT /Ср/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.3Л3.5 Э1 Э2 Э3	0	
Тема 2.6. Практические аспекты безопасности ИС /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.4Л3.1 Э1 Э2 Э3	0	
Тема 2.6. Практические аспекты безопасности ИС /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.1Л3.2 Э1 Э2 Э3	0	
Тема 2.6. Практические аспекты безопасности ИС /Ср/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.2Л3.3 Э1 Э2 Э3	0	

Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.4 Э1 Э2 Э3	0	
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.1Л3.5 Э1 Э2 Э3	0	
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.2Л3.1 Э1 Э2 Э3	0	
Раздел 3. Криптографические методы защиты информации						
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.1Л3.2 Э1 Э2 Э3	0	
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.2Л3.3 Э1 Э2 Э3	0	
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.3Л3.4 Э1 Э2 Э3	0	
Тема 3.2. Симметричные криптографические алгоритмы /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.4Л3.5 Э1 Э2 Э3	0	
Тема 3.2. Симметричные криптографические алгоритмы /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.1Л3.1 Э1 Э2 Э3	0	
Тема 3.2. Симметричные криптографические алгоритмы /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.2Л3.2 Э1 Э2 Э3	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.3 Э1 Э2 Э3	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.4Л3.4 Э1 Э2 Э3	0	

Тема 3.3. Асимметричные криптографические алгоритмы /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.1Л3.5 Э1 Э2 Э3	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.2Л3.1 Э1 Э2 Э3	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.3Л3.2 Э1 Э2 Э3	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.4Л3.3 Э1 Э2 Э3	0	
Тема 3.5. Технологии аутентификации. /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.1Л3.4 Э1 Э2 Э3	0	
Тема 3.5. Технологии аутентификации. /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.2Л3.5 Э1 Э2 Э3	0	
Тема 3.5. Технологии аутентификации. /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.3Л3.1 Э1 Э2 Э3	0	
/Конс/	5	2	ОПК ОС-10.1		0	
Раздел 4. Информационная безопасность ИС и сетей						
Тема 4.1. Проблемы информационной безопасности сетей /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
Тема 4.1. Проблемы информационной безопасности сетей /Пр/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.1Л3.3 Э1 Э2 Э3	0	
Тема 4.1. Проблемы информационной безопасности сетей /Ср/	6	11	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.2Л3.1 Л3.5 Э1 Э2 Э3	0	

Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.2 Э1 Э2 Э3	0	
Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей /Пр/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.4Л3.3 Э1 Э2 Э3	0	
Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.1Л3.1 Л3.5 Э1 Э2 Э3	0	
Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры. /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.2Л3.2 Э1 Э2 Э3	0	
Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры. /Пр/	6	4	ОПК ОС-10.1	Л1.2Л2.3	0	
Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры. /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.4Л3.1 Л3.5 Э1 Э2 Э3	0	
Тема 4.4. Технологии VPN. /Лек/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.1Л3.1 Э1 Э2 Э3	0	
Тема 4.4. Технологии VPN. /Пр/	6	6	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.2Л3.3 Э1 Э2 Э3	0	
Тема 4.4. Технологии VPN. /Ср/	6	11	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.3Л3.1 Л3.5 Э1 Э2 Э3	0	
Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.4Л3.2 Э1 Э2 Э3	0	
Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP /Пр/	6	6	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.1Л3.3 Э1 Э2 Э3	0	
Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.2Л3.4 Э1 Э2 Э3	0	

Раздел 5. Особенности защиты информации на уровнях модели OSI						
Тема 5.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне. /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.3Л3.1 Л3.2 Э1 Э2 Э3	0	
Тема 5.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне. /Пр/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.4Л3.2 Э1 Э2 Э3	0	
Тема 5.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне. /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.1Л3.3 Э1 Э2 Э3	0	
Тема 5.2. Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1Л2.2Л3.4 Э1 Э2 Э3	0	
Тема 5.2. Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне /Пр/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.2Л2.3Л3.5 Э1 Э2 Э3	0	
Тема 5.2. Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.3Л2.4Л3.1 Э1 Э2 Э3	0	
/Конс/	6	2	ОПК ОС-10.1		0	

РАЗДЕЛ 3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе освоения дисциплины используются следующие образовательные технологии: лекции (Л), практические занятия (ПР), самостоятельная работа студентов (СР) по выполнению различных видов заданий.

1. В процессе освоения дисциплины используются следующие интерактивные образовательные технологии: проблемная лекция (ПЛ). Лекционный материал представлен в виде слайд-презентации в формате «Power Point». Для наглядности используются материалы различных научных и технических экспериментов, справочных материалов, научных статей т.д. В ходе лекции предусмотрена обратная связь со студентами, активизирующие вопросы, просмотр и обсуждение видеофильмов. При проведении лекций используется проблемно-ориентированный междисциплинарный подход, предполагающий творческие вопросы и создание дискуссионных ситуаций.

2. При изложении теоретического материала используются такие методы:

− монологический;
− показательный;
− диалогический;
− эвристический;

− исследовательский;
− проблемное изложение.
3. Используются следующие принципы дидактики высшей школы:
− последовательность обучения;
− систематичность обучения;
− доступность обучения;
− принцип научности;
− принципы взаимосвязи теории и практики;
− принцип наглядности и др.
В конце каждой лекции предусмотрено время для ответов на проблемные вопросы.
4. Самостоятельная работа предназначена для внеаудиторной работы студентов, связанной с конспектированием источников, учебного материала, изучением дополнительной литературы по дисциплине, подготовкой к текущему и семестровому контролю, а также выполнением индивидуального задания в форме реферата, эссе, презентации, эмпирического исследования.

РАЗДЕЛ 4. УЧЕБНО-МЕТОДИЧЕСКОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Рекомендуемая литература

1. Основная литература

	Авторы,	Заглавие	Издательство, год
Л1.1	А. В. Артемов.	Информационная безопасность : курс лекций: Курс лекций (256 с.)	Межрегиональная Академия безопасности и выживания (МАБИВ, 2014
Л1.2	В. Ф. Шаньгин.	Информационная безопасность и защита информации: Курс лекций (702 с.)	Профобразование, 2019
Л1.3	О. В. Прохорова.	Информационная безопасность и защита информации: Учебник (113 с.)	Самарский государственный архитектурно-строительный университет, 2014

2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год
Л2.1	П. Н. Башлы, А. В. Бабаш, Е. К. Баранова.	Информационная безопасность и защита информации: Учебное пособие (311 с.)	Евразийский открытый институт, 2012
Л2.2	Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева.	Информационная безопасность : учебное пособие: Учебное пособие (221 с.)	Государственный Аграрный Университет им. Императора Петра Первого, 2015
Л2.3	Д. В. Фомин.	Информационная безопасность : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика»: Учебно-методическое пособие (125 с.)	Вузовское образование, 2018
Л2.4	Е. М. Скурыдина.	Информационная безопасность : учебное пособие: Учебное пособие (313 с.)	Алтайский государственный педагогический университет, 2017

3. Методические разработки

	Авторы,	Заглавие	Издательство, год
Л3.1	Семичастный И.Л. Семичастный И.Л.	Рабочая программа по учебной дисциплине «Информационная безопасность» для обучающихся 3 курса образовательной программы бакалавриата направления подготовки 9.03.03 «Прикладная информатика» очной/заочной форм обучения / сост. И.Л. Семичастный. – Протокол заседания кафедры информационных технологий № 1 от 29.08.2022 г:	Донецк :ДОНАУИГС, 2022

	Авторы,	Заглавие	Издательство, год
		Рабочая программа (27 с.)	
Л3.2	И.Л. Семичастный	Конспект лекций по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Конспект лекций (147 с.)	Донецк: ДОНАУИГС, 2022
Л3.3	И.Л. Семичастный	Методические рекомендации для проведения практических занятий по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Методические рекомендации (35 с.)	Донецк: ДОНАУИГС, 2022
Л3.4	И.Л. Семичастный	Методические рекомендации для самостоятельной работы студентов по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Методические рекомендации (28 с.)	Донецк ДОНАУИГС, 2022
Л3.5	И.Л. Семичастный	Индивидуальные задания для самостоятельной работы по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Индивидуальные задания (87 с.)	Донецк: ДОНАУИГС, 2022

4.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Научная электронная библиотека «КиберЛенинка»	https://cyberleninka.ru/
Э2	Научная электронная библиотека	http://elibrary.ru
Э3	Библиотека ФГБОУВО «ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ»	https://donampa.ru/biblioteka

4.3. Перечень программного обеспечения

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:

При проведении лекций используется аудитория с мультимедийным оборудованием. Аудиторные занятия проводятся в компьютерных классах с доступом к сети Интернет. Для проведения консультаций в online-режиме используется LMS Moodle и Яндекс.Телемост.

Программное обеспечение:

1. Операционная система Windows XP и выше; пакет Microsoft Office 2010 и выше.

При изучении дисциплины также используются информационные технологии противодействия вредоносному ПО и спаму. Для этого используются следующие демонстрационные версии и свободнораспространяемые пакеты антивирусных программ: Avast, Microsoft Essentials, AVG, Avira, , Dr Web, ESET, Kaspersky Antivirus 2015, Kaspersky Internet Security, Comodo Internet Security, Spybot, Bitdefender, 360Total Security, Symantec Endpoint Protection, McAfee, Panda Security.

Кроме того при изучении технологий криптографии используется компьютерные программы PGP и TrueCrypt, а также библиотека функций, позволяющие выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске.

При изучении технологий VPN (Virtual Private Network) используется программа LogMeIn Hamachi. При изучении дисциплины используется ПО в составе пакета OS MS Windows, MS Office 2010.

4.4. Профессиональные базы данных и информационные справочные системы

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в

электронную информационно-образовательную среду (ЭИОС ГОУ ВПО ДОНАУИГС) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств.

В процессе изучения дисциплины используются возможности информационно-справочной системы портала http://window.edu.ru/.

4.5. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного, семинарского типа, групповых занятий и консультаций, текущего контроля и промежуточной аттестации: аудитория № 704 учебный корпус № 1.
- компьютеры (16); программное обеспечение - Microsoft Office 2010 (лицензия № 47556582 от 19.10.2010 г., лицензия № 49048130 от 19.09.2011);
- комплект мультимедийного оборудования: ноутбук, мультимедийный проектор, экран; программное обеспечение - Windows 8.1 Professional x86/64 (академическая подписка DreamSpark Premium), LibreOffice 4.3.2.2 (лицензия GNU LGPL v3+ и MPL2.0);
- специализированная мебель: рабочее место преподавателя, рабочие места обучающихся (32), стационарная доска.
2. Помещения для самостоятельной работы с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно образовательную среду организации:
читальные залы, учебные корпуса 1, 6. Адрес: г. Донецк, ул. Челюскинцев 163а, г. Донецк, ул. Артема 94.
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ГОУ ВПО ДОНАУИГС) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств.
Сервер: AMD FX 8320/32Gb(4x8Gb)/4Tb(2x2Tb). На сервере установлена свободно распространяемая операционная система DEBIAN 10. MS Windows 8.1 (Лицензионная версия операционной системы подтверждена сертификатами подлинности системы Windows на корпусе ПК), MS Windows XP (Лицензионная версия операционной системы подтверждена сертификатами подлинности системы Windows на корпусе ПК), MS Windows 7 (Лицензионная версия операционной системы подтверждена сертификатами подлинности системы Windows на корпусе ПК), MS Office 2007 Russian OLP NL AE (лицензии Microsoft № 42638778, № 44250460), MS Office 2010 Russian (лицензии Microsoft № 47556582, № 49048130), MS Office 2013 Russian (лицензии Microsoft № 61536955, № 62509303, № 61787009, № 63397364), Grub loader for ALT Linux (лицензия GNU LGPL v3), Mozilla Firefox (лицензия MPL2.0), Moodle (Modular Object-Oriented Dynamic Learning Environment, лицензия GNU GPL), IncScape (лицензия GPL 3.0+), PhotoScape (лицензия GNU GPL), 1С ERP УП, 1С ЗУП (бесплатные облачные решения для образовательных учреждений от 1Cfresh.com), OnlyOffice 10.0.1 (SaaS, GNU Affero General Public License3)

РАЗДЕЛ 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

1. Информационная война как угроза информационной безопасности национального уровня
2. Объекты и субъекты информационного пространства. Примеры.
3. Субъекты информационных отношений и их интересы.
4. Три уровня управления политикой безопасности на предприятии.
5. Варианты построения виртуальных защищенных каналов.
6. Понятие «модели злоумышленника». Привести примеры.
7. Конфиденциальность информации. Способы обеспечения конфиденциальности информации в организации.
8. Практические методы аутентификации, используемые в настоящее время
9. Классификация каналов проникновения в систему и утечки информации
10. Политика информационной безопасности организации.
11. Содержание политики безопасности организации.
12. Определение информационной безопасности и ее составляющие.
13. Причины роста компьютерной преступности. Компьютерные преступления против государственных и общественных интересов.
14. Ключевые категории (понятия) безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008.
15. Классификация вредоносных программ.
16. Сигнатурные методы обнаружения вредоносного ПО.
17. Проактивные методы обнаружения вредоносного ПО.
18. Тенденции развития современных антивирусных программ
19. Модули и режимы работы современных антивирусных программ.

20. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
21. Защита периметра сети ИС предприятия с помощью межсетевых экранов (МСЭ)
22. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
23. Модель нарушителя антивирусной безопасности. Рекомендуемые методы защиты для классов нарушителей.
24. Тенденции развития современных антивирусных программ
25. Защита информации на уровне корпоративной сети предприятия.
26. Технические каналы утечки информации. Защита от утечек информации по техническим каналам
27. Модули и режимы работы современных антивирусных программ.
28. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
29. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
30. Модель нарушителя антивирусной безопасности. Рекомендуемые методы защиты для классов нарушителей.
31. Защита информации на уровне корпоративной сети предприятия.
32. Методика создания демилитаризованных зон в корпоративной сети предприятия
33. Защита информации от утечки по электромагнитным каналам
34. Технические каналы утечки информации. Защита от утечек информации по техническим каналам
35. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
36. Технология обеспечения безопасности ИС при беспроводном соединении
37. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.
38. Система обнаружения и предотвращения вторжений.
39. Технологии обеспечения безопасности в ОС Windows 7.
40. Способы защиты информации в организации. Характеристика защитных действий
41. Защита информации от утечки по визуально оптическим каналам.
42. Способы защиты информации в организации. Характеристика защитных действий
43. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
44. Технология обеспечения безопасности ИС при беспроводном соединении
45. Система обнаружения и предотвращения вторжений.
46. Технологии обеспечения безопасности в ОС Windows 7.
47. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.
48. Защита информации от утечки по электромагнитным каналам
49. Информационная безопасность на базе стандарта CobiT
50. Термины и определения криптографии.
51. Классификация криптографических алгоритмов
52. Критерии безопасности компьютерных систем «Оранжевая книга».
53. Криптографический алгоритм Виженера. Преимущества и недостатки.
54. Технологии биометрической аутентификации пользователя.
55. Преимущества и недостатки симметричных алгоритмов шифрования
56. Проблемы безопасности IP-сетей
57. Порядок использования систем с симметричными ключами.
58. Технологии строгой аутентификации пользователя.
59. Симметричные алгоритмы шифрования. Примеры
60. Структура и функциональность стека протоколов TCP/IP с точки зрения информационной безопасности.
61. Технология использование электронной цифровой подписи.
62. Классификация механизмов аутентификации пользователей
63. Классификация сетей VPN. Преимущества применения технологий VPN.
64. Структура политики безопасности организации
65. Преимущества и недостатки асимметричных систем шифрования.
66. Технологии виртуальных защищенных сетей (VPN). Основные понятия и функции сети VPN
67. Порядок использования систем с асимметричными ключами
68. Протоколы формирования защищенных каналов сети VPN на сеансовом уровне
69. Проблема целостности информации. Примеры нарушения целостности информации
70. Основные варианты архитектуры VPN. Средства обеспечения безопасности VPN.
71. Методы защиты информации на канальном и сеансовом уровнях.
72. Методы защита информации на сетевом уровне. Протокол IPSec

5.2. Темы письменных работ

Письменные работы не предусмотрены

5.3. Фонд оценочных средств

Фонд оценочных средств дисциплины "Информационная безопасность" разработан в соответствии с локальным нормативным актом ФГБОУ ВО "ДОНАУИГС".

Фонд оценочных средств дисциплины "Информационная безопасность" в полном объеме представлен в виде приложения к данному РПД.

5.4. Перечень видов оценочных средств

Устный опрос (контроль знаний раздела учебной дисциплины)
Собеседование (самостоятельная работа)
Индивидуальные задания

РАЗДЕЛ 6. СРЕДСТВА АДАПТАЦИИ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ К ПОТРЕБНОСТЯМ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

1) с применением электронного обучения и дистанционных технологий.

2) с применением специального оборудования (техники) и программного обеспечения, имеющихся в ФГБОУ ВО "ДОНАУИГС".

В процессе обучения при необходимости для лиц с нарушениями зрения, слуха и опорно-двигательного аппарата предоставляются следующие условия:

- для лиц с нарушениями зрения: учебно-методические материалы в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные задания и консультации.

- для лиц с нарушениями слуха: учебно-методические материалы в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

- для лиц с нарушениями опорно-двигательного аппарата: учебно-методические материалы в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

РАЗДЕЛ 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО УСВОЕНИЮ ДИСЦИПЛИНЫ

Аудиторные занятия по дисциплине "Информационная безопасность" проводятся в форме лекционных и практических занятий.

На лекционных занятиях, согласно учебному плану дисциплины, обучающимся предлагается рассмотреть основные темы курса. Студенту предлагается участвовать в диалоге с преподавателем, в ходе которого могут обсуждаться моменты, актуальные для его будущей практической деятельности; он может высказать свое мнение после сопоставления разных фактов и разнообразных точек зрения на них.

К числу важнейших умений, являющихся неотъемлемой частью успешного учебного процесса, относится умение работать с различными литературными источниками, содержание которых так или иначе связано с изучаемой дисциплиной.

Подготовку к любой теме курса рекомендуется начинать с изучения презентационных материалов или учебной литературы, в которых дается систематизированное изложение материала, разъясняется смысл разных терминов и сообщается об изменениях в подходах к изучению тех или иных проблем данного курса.

Методические указания по организации самостоятельной работы

Самостоятельная работа по дисциплине организована в следующих видах:

1. изучение теоретического материала по заданной теме;
2. анализ методов решения поставленной задачи;
3. выполнение индивидуальных заданий;
4. оценка достоверности полученных результатов;
5. отчет перед преподавателем по теоретической и практической части индивидуальной работы;
6. работа над индивидуальными заданиями представлена в виде элементов электронного курса в системе elearn:

https://elearn.donampa.ru/course/view.php?id=14