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
24.04.2025 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 ***2025***

Донецк
2025

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:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (Приказ Министерства образования и науки Российской Федерации от 19.09.2017 г. № 922).

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 24.04.2025 протокол № 12.
Срок действия программы: 2025-2029

Рабочая программа рассмотрена и одобрена на заседании кафедры Информационных технологий

Протокол от 02.04.2025 № 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 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)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2029 - 2030 учебном году на заседании кафедры Информационных технологий

Протокол от "____" _____ 2029 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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1	0	

				Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4		
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России . /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России . /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.3. Угрозы информационной безопасности . /Лек/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.3. Угрозы информационной безопасности . /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3	0	

				Э4		
Тема 1.3. Угрозы информационной безопасности . /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Ср/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая	5	1	ОПК-3.1 ОПК ОС-	Л1.1 Л1.2 Л1.3Л2.1	0	

безопасность. /Лек/			10.1	Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4		
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Пр/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	

Тема 2.2. Основные принципы и методы в области технической защиты информации /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Лек/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2	0	

				Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4		
Тема 2.5. Международные стандарты ИБ. COBIT /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.5. Международные стандарты ИБ. COBIT /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.5. Международные стандарты ИБ. COBIT /Ср/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.6. Практические аспекты безопасности ИС /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.6. Практические аспекты безопасности ИС /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.6. Практические аспекты безопасности ИС /Ср/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5	0	

				Э1 Э2 Э3 Э4		
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Пр/	5	0,5	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.2. Симметричные криптографические алгоритмы /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.2. Симметричные криптографические алгоритмы /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1	0	

				Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4		
Тема 3.2. Симметричные криптографические алгоритмы /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3	0	

				Э4		
Тема 3.5. Технологии аутентификации. /Лек/	5	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.5. Технологии аутентификации. /Пр/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 3.5. Технологии аутентификации. /Ср/	5	1	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
/Конс/	5	2	ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.1. Проблемы информационной безопасности сетей /Пр/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.1. Проблемы информационной безопасности сетей /Ср/	6	11	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3	0	

				Э4		
Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей /Пр/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры. /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры. /Пр/	6	4	ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры. /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.4. Технологии VPN. /Лек/	6	4	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.4. Технологии VPN. /Пр/	6	6	ОПК-3.1 ОПК ОС-	Л1.1 Л1.2 Л1.3Л2.1	0	

			10.1	Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4		
Тема 4.4. Технологии VPN. /Ср/	6	11	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP /Лек/	6	2	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP /Пр/	6	6	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP /Ср/	6	9	ОПК-3.1 ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	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	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5 Э1 Э2 Э3 Э4	0	
/Конс/	6	2	ОПК ОС-10.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Л3.4 Л3.5	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	Баланов А.Н.	Комплексная информационная безопасность (400 с.)	Издательство "Лань", 2025
Л1.2	Бондаренко И.С.	Информационная безопасность (254)	Лань, 2023
Л1.3	Тесленко И.Б.	Информационная безопасность: Учебное пособие (212 с.)	Лань, 2023

2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год
Л2.1	Партыка Т.Л..	Информационная безопасность: Учебное пособие (432 с.)	Москва : ФОРУМ : ИНФРА-М, 2021
Л2.2	Попов И.В.	Информационная безопасность: Практикум (90 с.)	Самара : Самарский юридический институт ФСИН России, 2022
Л2.3	Раченко Т. А.	Информационная безопасность: Учебно-методическое пособие (135 с.)	, 2024

3. Методические разработки

	Авторы,	Заглавие	Издательство, год
Л3.1	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 № 9 от 02.04.2025 г: Рабочая программа (27 с.)	Донецк :ДОНАУИГС, 2023
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 №9 от 02.04.2025 г: Конспект лекций (147 с.)	Донецк: ДОНАУИГС, 2023
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 №9 от 02.04.2025 г: Методические рекомендации (35 с.)	Донецк: ДОНАУИГС, 2023
Л3.4		Методические рекомендации для самостоятельной	Донецк ДОНАУИГС,

	Авторы,	Заглавие	Издательство, год
	И.Л. Семичастный	работы студентов по учебной дисциплине «Информационная безопасность» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №9 от 02.04.2025 г: Методические рекомендации (28 с.)	2023
Л3.5	И.Л. Семичастный	Индивидуальные задания для самостоятельной работы по учебной дисциплине «Информационная безопасность» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №9 от 02.04.2025 г: Индивидуальные задания (87 с.)	Донецк: ДОНАУИГС, 2023

4.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	ЭБС «ЗНАНИУМ»	https://znanium.ru/
Э2	Научная электронная библиотека «КиберЛенинка»	https://cyberleninka.ru/
Э3	ЭБС «ЛАНЬ»	https://e.lanbook.com/
Э4	ЭБС «SOCHUM»	https://sochum.ru/

4.3. Перечень программного обеспечения

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

- Libre Office (лицензия Mozilla Public License v2.0.)
- 7-Zip (лицензия GNU Lesser General Public License)
- AIMP (лицензия LGPL v.2.1)
- STDU Viewer (freeware for private non-commercial or educational use)
- GIMP (лицензия GNU General Public License)
- Inkscape (лицензия GNU General Public License).

4.4. Профессиональные базы данных и информационные справочные системы

Не используется

4.5. Материально-техническое обеспечение дисциплины

Для проведения учебных занятий, предусмотренных образовательной программой, закреплены аудитории согласно расписанию учебных занятий:
рабочее место преподавателя, посадочные места по количеству обучающихся, доска меловая, персональный компьютер с лицензированным программным обеспечением общего назначения, мультимедийный проектор, экран, интерактивная панель.

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.

ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗАДАНИЯ ЗАКРЫТОГО ТИПА
Раздел 1. Технологии и методы обеспечения ИБ
Задание 1

Что такое компьютерные преступления? Выберите правильный вариант ответа и обоснуйте его.

А. Компьютерные преступления - это исключительно взлом компьютеров правительственных организаций.
Б. К разряду компьютерных преступлений следует отнести те из них, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер.
В. Компьютерные преступления — это установка нелицензионного программного обеспечения на рабочий компьютер.
Г. Компьютерные преступления — это любые действия, совершаемые с помощью компьютера, включая игру в видеоигры и общение в социальных сетях.
Д. Компьютерные преступления — это покупка нового оборудования для своего компьютера.

Задание 2

Что такое информационный объект? Выберите правильный вариант ответа и обоснуйте его.

А. Информационный объект - это исключительно запоминающее устройство для хранения информации, например, жёсткий диск или флешка.
Б. Информационный объект - это только текстовый объект, созданный пользователем.
В. Информационный объект – среда, в которой информация создается, передается, обрабатывается или хранится.
Г. Информационный объект - это программа, управляющая компьютером, не содержащая данных.
Д. Информационный объект - это любой объект, который можно найти в глобальной сети.

Задание 3

Угрозы информационной безопасности разбиваются на две большие группы. Какие это группы?

А. Визуальные угрозы.
Б. Естественные (случайные) угрозы.
В. Искусственные угрозы.
Г. Электромагнитные угрозы.
Д. Звуковые угрозы.

Задание 4

Объясните ваше понимание двух групп факторов, влияющих на ведение информационной войны.

1) Объясните, что такое технологические факторы, влияющих на развитие информационной войны.
2) Разъясните, что такое социально-политические факторы, влияющих на развитие информационной войны.

Задание 5

1) Объясните, что такое информационная безопасность в широком смысле.
2) Разъясните, что такое безопасность информации, то есть ИБ в более узком смысле.

Задание 6

1) Объясните, что такое конфиденциальность информации как составная часть ИБ.
2) Разъясните, что такое целостность информации, как составная часть ИБ.
3) Разъясните, что такое доступность информации, как составная часть ИБ

Задание 7
1) Объясните, что такое идентификация субъекта.
2) Разъясните, что такое аутентификация субъекта.
3) Разъясните, что такое авторизация субъекта

Задание 8
1) Объясните, что означает гриф документа «особой важности».
2) Разъясните, что означает гриф документа «совершенно секретно».
3) Разъясните, что означает гриф документа «секретно».

Задание 9
1) Объясните, что такое коммерческая тайна.
2) Разъясните, что такое профессиональная тайна.
3) Разъясните, что такое личная тайна (персональные данные).

Задание 10
Процесс проверки подлинности обеих сторон это?

А. Двухфакторная аутентификация
Б. Многофакторная аутентификация
В. Двухстороняя аутентификация
Г. Биометрическая аутентификация
Д. Парольная аутентификация

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 "Информационные системы и технологии" 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.

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.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Факультет государственной службы и управления
Кафедра информационных технологий

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
«Информационная безопасность»

Направление подготовки	09.03.03 Прикладная информатика
Профиль	«Прикладная информатика в управлении корпоративными информационными системами»
Квалификация	бакалавр
Форма обучения	очная

Донецк
2025

Фонд оценочных средств по дисциплине «Информационная безопасность» для обучающихся 3 курса образовательной программы бакалавриата направления подготовки 09.03.03 Прикладная информатика (профиль: «Прикладная информатика в управлении корпоративными информационными системами») очной формы обучения

Автор,
разработчик: доцент, канд. техн. наук, доцент, Семичастный И.Л

ФОС рассмотрен на заседании
кафедры *информационных технологий*

Протокол заседания кафедры от 02.04.2025 г. № № 9

Заведующий кафедрой _____ Н.В. Брадул

РАЗДЕЛ 1.
ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Информационная безопасность»

1.1. Основные сведения о дисциплине

Таблица 1

Характеристика дисциплины (сведения соответствуют разделуРПУД)

Образовательная программа	бакалавриат
Направление подготовки Профиль	09.03.03 Прикладная информатика «Прикладнаяинформатикавуправлении корпоративными информационными системами»
Количество разделов дисциплины	5
Часть образовательной программы	Б1.О.19
Формы текущего контроля	Индивидуальные задания, устный опрос, письменный опрос, тестовые задания, реферат, доклад
Показатели	Очная форма обучения
Количество зачетных единиц (кредитов)	6
Семестр	5,6
Общая трудоемкость (академ. часов)	216
Аудиторная контактная работа:	106
Лекционные занятия	54
Практические занятия	48
Консультации	4
Самостоятельная работа	83
Контроль	27
Форма промежуточной аттестации	д/зачет, экзамен

1.2. Перечень компетенций с указанием этапов формирования в процессе освоения образовательной программы.

Таблица 2

Перечень компетенций и их элементов

Компетенция	Индикатор компетенции и его формулировка	Элементы индикатора компетенции	Индекс элемента
ПК-9.2	Участвует в организации ИТ инфраструктуры и управлении информационной безопасностью	***Знать:***	
		1. типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду.	ПК-9.2 З-1
		2. методы защиты информации в вычислительных системах и сетях.	ПК-9.2 З-2
		3. типовые средства защиты информации в вычислительных системах и сетях.	ПК-9.2 З-3
		Уметь:	
		1. использовать типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду.	ПК-9.2 У-1
		2. использовать типовые программно-аппаратные средства и системы зашиты информации от нарушения ее целостности.	ПК-9.2 У-2
		3. использовать методы защиты информации в вычислительных системах и сетях.	ПК-9.2 У-3
		Владеть:	

Компетенция	Индикатор компетенции и его формулировка	Элементы индикатора компетенции	Индекс элемента
		1. навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях. 2. типовыми	ПК-9.2 В-1
		программно-аппаратными средствами обеспечения доступности информации. 3. навыками использования типовых программно-аппаратных средств и систем зашиты информации от несанкционированного доступа в компьютерную среду.	ПК-9.2 В-2 ПК-9.2 В-3
	Решает стандартные задачи профессиональной деятельности на	***Знать:***	
		1. нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий. 2. виды угроз ИС. 3. методы обеспечения информационной безопасности.	ОПК 3.1 З-1 ОПК 3.1 З-2 ОПК 3.1 З-3
		Уметь:	

Компетенция	Индикатор компетенции и его формулировка	Элементы индикатора компетенции	Индекс элемента
ОПК-3.1	основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	1. использовать нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий для организации защиты информации. 2. применять методы анализа прикладной области на концептуальном, логическом, и алгоритмическом уровнях с целью выявления угроз	ОПК 3.1 У-1 ОПК 3.1 У-2
Код компетенции	Формулировка компетенции	Элементы компетенции	Индекс элемента
		безопасности. 3. решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК 3.1 У-3
		Владеть:	

Компетенция	Индикатор компетенции и его формулировка	Элементы индикатора компетенции	Индекс элемента
		1. международными и отечественными стандартами в области обеспечения безопасности информационных систем и технологий. 2. способностью блокироватьугрозы безопасности ИС предприятия с помощью методов обеспечения защиты информации. 3. навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	ОПК 3.1 В-1 ОПК 3.1 В-2 ОПК 3.1 В-3

Таблица 3

Этапы формирования компетенций в процессе освоения основной образовательной программы

№ п/п	Контролируемые разделы (темы) дисциплины	Номер семестра	Код индикатора компетенции	Наименование оценочного средства
Раздел 1. Технологии и методы обеспечения ИБ				
1.	Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России .	5	ПК 9.2 З-1 ОПК 3.1 У-1	Индивидуальная работа №1

№ п/п	Контролируемые разделы (темы) дисциплины	Номер семестра	Код индикатора компетенции	Наименование оценочного средства
2.	Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба	5	ОПК 3.1 З-1 ОПК 3 У-2	Индивидуальная работа №1 Устный опрос (вопросы, выносимые на самостоятельное обучение)
3.	Тема 1.3. Угрозы информационной безопасности .	5	ОПК 3.1 З-1 ОПК 3.1 В-1	Индивидуальная работа №2 Индивидуальная работа №2
4.	Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	5	ОПК 3.1 З-3 ОПК 3.1 В-1	Устный опрос (вопросы, выносимые на самостоятельное обучение) Индивидуальная работа №3
5.	Тема 1.5. Технологии защиты от вредоносных программ и спама.	5	ОПК 3.1 З-2 ПК-9.2 В-1	Индивидуальная работа №3 Устный опрос
6.	Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.	5	ОПК 3.1 З-1 ПК-9.2 В-1	(вопросы, выносимые на самостоятельное обучение)
	Раздел 2. Технологии защиты информации			
7.	Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия	5	ОПК 3.1 У-2 ОПК 3.1 В-1 ПК-9.2 В-2	Индивидуальная работа №4

№ п/п	Контролируемые разделы (темы) дисциплины	Номер семестра	Код индикатора компетенции	Наименование оценочного средства
8.	Тема 2.2. Основные принципы и методы в области технической защиты информации	5	ОПК 3.1 У-1 ОПК 3.1 В-1 ПК-9.2 В-3	Индивидуальная работа №4 Устный опрос (вопросы, выносимыена самостоятельное обучение)
9.	Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации	5	ОПК 3.1 У-3 ОПК 3.1 В-2 ПК 9.2 В-1	Индивидуальная работа №4 Индивидуальная работа
10.	Тема 2.4. Критерии защищенности ком-пьютерных систем. Лицензирование и сертификация ИБ.	5	ОПК 3.1 У-1 ОПК 3.1 В-1 ПК-9.2 В-2	№4 Устный опрос (вопросы, выносимыена самостоятельное обучение) Индивидуальная работа №4
11.	Тема 2.5. Междуна-родные стандарты ИБ. COBIT	5	ОПК 3.1 У-2 ОПК 3.1 В-3 ПК-9.2 В-3	
12.	Тема 2.6. Практические аспекты безопасности ИС	5	ОПК 3.1 У-3 ОПК 3.1 В-2 ПК-9.2 В-2	Индивидуальная работа №4 Устный опрос (вопросы, выносимые на самостоятельное обучение)
13.	Тема 2.7. Обеспечение безопасности ОС. Безопасность Windows 7	5	ОПК 3.1 У-1 ОПК 3.1 У-2 ПК-9.2 В-1	Индивидуальная работа №5
Раздел 3. Криптографические методы защиты информации				

№ п/п	Контролируемые разделы (темы) дисциплины	Номер семестра	Код индикатора компетенции	Наименование оценочного средства
14.	Тема 3.1. Крипто-графические методы защиты информации. Классификация криптографических методов защиты.	5	ОПК 3.1 У-3 ОПК 3.1 В-2 ПК 9.2 В-3	Индивидуальная работа №5 Устный опрос (вопросы, выносимые на самостоятельное обучение) Индивидуальная работа
15.	Тема 3.2. Симметричные криптографические алгоритмы	5	ОПК 3.1 У-1 ОПК 3.1 В-2 ПК 9.2 В-2	№5 Индивидуальная работа
16.	Тема 3.3. Асимметричные криптографические алгоритмы	5	ОПК 3.1 У-2 ОПК 3.1 В-1 ПК 9.2 В-1	№5 Индивидуальная работа
17.	Тема 3.4. Цифровая электронная подпись (ЭЦП).	5	ОПК 3.1 У-3 ОПК 3.1 В-3 ПК 9.2 В-2	№5
18.	Тема 3.5. Технологии аутентификации.	5	ОПК 3.1 У-2 ОПК 3.1 В-3 ПК 9.2 В-3	Индивидуальная работа №5 Устный опрос (вопросы, выносимые на самостоятельное обучение)
Раздел 4 Информационная безопасность ИС и сетей				
19.	Тема 4.1. Проблемы информационной безопасности сетей	6	ОПК 3.1 В-1 ОПК 3.1 В-2 ПК 9.2 В-1	Индивидуальная работа №6 Устный опрос
20.	Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей	6	ОПК 3.1 У-2 ОПК 3.1 В-2 ПК 9.2 В-2	Индивидуальная работа №6 Индивидуальная работа №7 Устный опрос (вопросы, выносимыена самостоятельное обучение)

№ п/п	Контролируемые разделы (темы) дисциплины	Номер семестра	Код индикатора компетенции	Наименование оценочного
21.	Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры.	6	ОПК 3.1 У-3 ОПК 3.1 В-3 ПК 9.2 В-3	Индивидуальная работа №7 Устный опрос (вопросы, выносимые на самостоятельное обучение)
22.	Тема 4.4. Технологии VPN.	6	ОПК 3.1 З-1 ОПК 3.1 В-1 ПК 9.2 В-1	Индивидуальная работа №8 Устный опрос (вопросы, выносимые на самостоятельное обучение)
23.	Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP	6	ОПК 3.1 У-2 ОПК 3.1 В-3 ПК 9.2 В-2	Индивидуальная работа №8 Устный опрос (вопросы, выносимые на самостоятельное обучение)
Раздел 5. Особенности защиты информации на уровнях модели OSI				
24.	Тема 5.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.	6	ОПК 3.1 В-1 ОПК 3.1 В-2 ПК 9.2 В-3	Индивидуальная работа №9 Устныйопрос (вопросы, выносимые на самостоятельное обучение)
25.	Тема 5.2. Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне	6	ОПК 3.1 В-3 ОПК 3.1 В-2 ПК 9.2 В-1	Индивидуальная работа №9 Контрольная рбота Устный опрос (вопросы, выносимые на самостоятельное обучение)

РАЗДЕЛ 2
ТЕКУЩИЙ КОНТРОЛЬ ПО ДИСЦИПЛИНЕ
«Информационная безопасность»

Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной работой) обучающихся.

В условиях балльно-рейтинговой системы контроля результаты текущего оценивания обучающегося используются как показатель его текущего рейтинга. Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы по индивидуальной инициативе преподавателя. Данный вид контроля стимулирует у обучающегося стремление к систематической самостоятельной работе по изучению дисциплины.

Таблица 2.1.

Распределение баллов по видам учебной деятельности
(балльно-рейтинговая система)

Наименование Раздела/Темы	Вид задания						
		ПЗ		Всего за тему	КЗР	Р (СР)	ИЗ
	ЛЗ	УО	ТЗ				
Р.1.Т.1.1		1		1	15	1	4
Р.1.Т.1.2		1		1			
Р.1.Т.1.3		1		1		1	4
Р.1.Т.1.4		1		1			
Р.1.Т.1.5		1		10		1	4
Р.1.Т.1.6		1	3				
Р.2.Т.2.1		1		1	15	1	4
Р.2.Т.2.2		1		1			
Р.2.Т.2.3		1		1		1	4
Р.2.Т.2.4		1		1			
Р.2.Т.2.5		1		10		1	4
Р.2.Т.2.6		1 Р.2	.2.7				
		1	3				
Р.3.Т.3.1		1		1	10	1	4
Р.1.Т.3.2		1		11			
Р.1.Т.3.3		1				1	4
Р.1.Т.3.4		1					
Р.1.Т.3.5		1	3				
Р.1.Т.4.1		1 Р.1	.4.2		15	1	4
		1					
Р.1.Т.4.3		1				1	4
Р.1.Т.4.4		1					
Р.1.Т.4.5		1	3			1	4
Р.1.Т.5.1		1 Р.1	.5.2		5	1	4
		1	3				
Итого: 100б		**25**	**15**	**40**	**60**	**12**	**48**

ЛЗ – лекционное занятие;
УО – устный опрос;
ТЗ – тестовое задание;
ПЗ – практическое занятие;
КЗР – контроль знаний по Разделу;

Р – реферат.
СР – самостоятельная работа обучающегося
ИЗ – индивидуальное задание

РАЗДЕЛ 2.1 Рекомендации по оцениванию индивидуальных заданий обучающихся

2.1. Рекомендации по оцениванию индивидуальных заданий обучающихся

Максимальное количество баллов*	Критерии
Отлично	Выставляется обучающемуся: если выполнены все пункты работы самостоятельно, без ошибок, если предложен более рациональный алгоритм решения задачи.
Хорошо	Выставляется обучающемуся: если самостоятельно выполнены все пункты работы, допущены незначительные ошибки, если предложен более рациональный алгоритм решения задачи.
Удовлетворительно	Выставляется обучающемуся: если самостоятельно (или с помощью преподавателя) выполнены все пункты работы, допущены грубые ошибки.
Неудовлетворительно	Выставляется обучающемуся: если с помощью преподавателя выполнены не все пункты работы, допущены грубые ошибки.

* Представлено в таблице 2.1.

ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИИ

Раздел 1. Технологии и методы обеспечения ИБ

Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России

Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба

Индивидуальноезадание№1

1. Изучите требования по созданию надежных паролей.
2. Скачайте программу генерации паролей Advanced Password Generator по ссылке https://drive.google.com/open?id=1Q7qLTrCefuZNJ3XDzq0FFZ2lWIsINW-S
3. Сгенерируйте при помощи скачанной программы группы паролей по следующей схеме: 8-10-12-20 символов (буквы / буквы+цифры / буквы+цифры+спецсимволы).
4. При помощи интернет ресурса http://www.passwordmeter.com/ проверьте сгенерированные пароли. Опишите изменения стойкости паролей в

зависимости от их структуры (описания подтвердите скриншотами). Являются лиони надежными?

5. Создайтена основе изученных Вами правил надежный пароль уровня Strong. Запишитеегои используйте всвоейработе.
6. Ознакомьтесь с программнымпродуктом хранения паролей KeePass? Скачав егос интернет-ресурсаhttps://keepass.info/.
7. Для знакомства с работой программы, скачайте программу, установите программуKeePassисоздайтесвоюбазуданныхпаролей.
8. Создайте свою портативную базуна сменном носителе. Создание новой базы паролей. Добавьте записи о пароле в базу. Добавьте в свою базу все пароли: дляпочты, соцсетей идругиепароли.
9. Ознакомьтесь с работой генератора паролей. Воспользуйтесь генератором для создания мастер- пароля
10. Созданиерезервной копиибазы.Создатьрезервнуюбазупаролей.
11. Всерезультатыподтвердитескриншотами.
12. Ознакомьтесь с работой сервиса хранения паролей LastPass https://www.lastpass.com/ru
13. Длясервиса**LastPass**повторитепунктыс6по10.
14. Всерезультатыподтвердитескриншотами.

Тема 1.3. Угрозы информационной безопасности .
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

Тема 1.3. Угрозы информационной безопасности .
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии

Индивидуальное задание №2:

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомьтесь с **Приложениями C, D** и **E** ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант индивидуального задания).

По каждому активу дать наименование, описание, условную стоимость в рублях.

4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь **Приложением C** ГОСТа сформулируйте три угрозы, реализация которых возможна, пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь двумя методами (см. вариант) предложенных в **Приложении E** ГОСТа, произведите оценку рисков информационной безопасности. Оценка рисков обязательно должна включать их ранжирование по примеру на основании Таблицы 2 ГОСТа, что является качественной оценкой рисков.
7. Оценку ценности информационного актива производить на основании

возможных потерь для организации в случае реализации угрозы.
8. Рассчитать экономические потери от реализации угроз (количественный оценки рисков):

- ♦ По каждой угрозе;
- ♦ В сумме для организации.

9. Разработать систему защитных мер по обеспечению безопасности, которые должны блокировать угрозы. При этом расставить приоритеты, в соответствии с выполненным ранжированием угроз.
Защитные меры: название, какой угрозе противостоит, начальная стоимость, стоимость в год.
10. Посчитать оценку защитных мер в рублях. Дать расчет стоимости или оценку каждой меры в отдельности и сумме общих затрат на защитные меры по обеспечению информационной безопасности предприятия.
Мера 1 – 10000 р +
мера 2 - 40000 р.
+ мера 3 - ....Итого: 100000 р.
11. Разработать политику безопасности, которая является системой управления информационной безопасностью Вашего предприятия. В ее основе перечень вопросов для предприятия (на примере Приложения А ГОСта), а также требования по СУИБ, изложенные в Лекции 5 и презентации к этой лекции.

Тема 1.5. Технологии защиты от вредоносных программ и спама
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.
ПРАКТИЧЕСКАЯ РАБОТА № 3 .
Индивидуальное задание № 3

1. Изучите возможности программы TrueCrypt.
2. Скачайте программу TrueCrypt версии 7.01a. Создайте на домашнем ПК небольшой зашифрованный диск. Используйте для доступа к этому диску созданный пароль.
3. Изучите возможности программы VeraCrypt.
4. Скачайте программу VeraCrypt. Создайте на ПК небольшой зашифрованный диск. Используйте для доступа к этому диску созданный пароль.
5. Изучите возможности программы Windows Bitlocker.
6. Используя программу Windows Bitlocker, создайте на ПК небольшой зашифрованный диск. Используйте для доступа к этому диску созданный пароль.
7. Сравните все опробованные программы, укажите их слабые и сильные стороны, а также функциональные особенности. Сделайте выводы о целесообразности применения той или иной рассмотренной программы в определенных условиях (офис, домашнее использование, сменный носитель

Тема 1.7. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия

Тема 1.8. Основные принципы и методы в области технической защиты информации

Тема 1.9. Противодействие несанкционированному доступу к конфиденциальной информации

Тема 1.10. Критерии защищенности ком-пьютерных систем. Лицензирование и сертификация ИБ.

Индивидуальное задание №4

1. На основании данных варианта задания из Таблицы 1, скачать инсталляционную версию антивирусного пакета.
2. Установить ее на свой ПК, предварительно отключив антивирусный пакет, установленный на нем.
3. Протестировать установленный антивирусный пакет в течение нескольких дней. Изучить режимы его работы, на основании полученных данных заполнить Таблицу №2 для своего антивирусного пакета по своему варианту.
4. Сохранить в файле отчета скриншоты основных режимов использования программы-антивируса в формате презентации.
5. Изучить отчет по анализу рынка антивирусных программ https://ichip.ru/rejjting-antivirusov-full
6. Подготовиться к ответам на теоретические вопросы из столбца №6 при защите отчета по работе.

Таблица №1

Номер варианта	**Вендор**	**Web-сайт**	**Free-antivirus-download**	**Доля рынка по данным компании OPSWAT (январь 2018)**	**Вопросы для самостоятельной работы**
1.	Avast	http://www.avast.com/free-antivirus-download	+	21.4%	1,3,4
2.	Microsoft	http://windows.microsoft.com/ru-RU/windows/products/security-essentials	+	19.4%	2,5,7
3.	AVG	http://free.avg.com/	+	8.6%	8,10, 12
4.	Avira	http://www.avira.com/en/avira-free-antivirus	+	7.4%	9,11, 13

5.	Symantec	http://norton.symantec.com/norton/ps/bb/3up_ns1_ns_nsbu_ru_ru_largo_tw_brfr.html?om_sem_cid=hho_sem_sy:ru:ggl:ru:e|kw0000517242|71830912762|c	Бесплатная пробная версия	7.1%	6, 15, 17

Таблица №2

Наличие режимов программного антивирусного комплекса

№	Режим использования	Название пакета	Достоинства	достатки
1.	Защита от руткитов и шпионских программ			
2.	Технология DeepScreen			
3.	Режимы Hardened («белый» список приложений)			
4.	Веб-защита			
5.	Очистка браузеров «Browser Cleanup»			

Тема 1.14. Криптографические методы защиты информации. Классификация криптографических методов защиты.

Тема 1.15. Симметричные криптографические алгоритмы

Тема 1.16. Асимметричные криптографические алгоритмы

Тема 1.17. Цифровая электронная подпись (ЭЦП).

Тема 1.18. Технологии аутентификации.

Варианты индивидуального задания №5.

Зашифруйте и расшифруйте сообщение методом Цезаря и Вижинера, для этой цели составьте алгоритм и программу на Excel, Visual Basic или C++.

N вар.	Метод Цезаря	Метод Виженера		Вопросы
		Вариант сообщения	Вариант ключа	
1.	Чу, я слышу пушек гром! ROT1	Достаточно надежное закрытие информации	Алгоритм	2, 6, 23
2.	Чу, я слышу пушек гром!	Такая замена равносильна	Случайно	30, 7, 22
	ROT2	введению ключа		
3.	Чу, я слышу пушек гром! ROT3	Процедура наложения гаммы на открытый текст	Значение	29, 8, 21

4.	Чу, я слышу пушек гром! ROT4	Разделяют две разновидности гаммирования	Качество	28, 9, 20
5.	Чу, я слышу пушек гром! ROT5	Эффективное средство повышения стойкости	Процедура	27, 10, 19

Раздел 2. Информационная безопасность ИС и сетей Тема 2.1. Проблемы информационной безопасности сетей
Тема 2.2 Угрозы и уязвимости проводных корпоративных сетей

Индивидуальное задание №6.

Часть 1. Загрузить и установить программу Wireshark (необязательно при использовании ПО на удаленном сервере).

Часть 2. Ознакомиться с методическими рекомендациями при использовании программы Wireshark.

Часть 3. Собрать и провести анализ данных протокола ICMP по локальным узлам в программе Wireshark

- Начать и остановить сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам.
- Найти данные об IP- и MAC-адресах в полученных PDU.

Часть 4. Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.
- Поясните, почему MAC-адреса удалённых узлов отличаются от MAC-адресов локальных узлов.
- При этом описать все протоколы, используемые утилитой. Описать все поля протоколов. Составить диаграмму взаимодействия машин при работе утилиты ping.

Часть 5. Захватить 100 произвольных пакетов. Определить статистические данные:

- процентное соотношение трафика разных протоколов в сети;
- среднюю скорость кадров/сек;
- среднюю скорость байт/сек;
- минимальный, максимальный и средний размеры пакета;
- степень использования полосы пропускания канала (загрузку сети)
- на примере любого IP-пакета указать структуры протоколов Ethernet и IP, отметить поля заголовков и описать их.

Тема 2.3. Технология защиты межсетевого обмена данными. Брандмауэры.
Тема 2.4. Технологии VPN.

Индивидуальное задание №7.

1. Загрузить программу «LogMeIn Hamachi» с сайта

http://hamachi.ru.softonic.com/ на оба компьютера будущей сети.
2. Создать сеть, пользуясь подсказками на сайте http://hamachiinfo.ru/nastrojka.html
3. Объединить в сеть принтер, камеру или другое устройство либо развернуть в сети какое-либо программное обеспечение (например, игру).
4. Подготовить отчет. При защите отчета ответить на вопросы для самостоятельной работы по варианту (Лекция №19-21).

Тема 2.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP
Тема 2.6. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.

Индивидуальное задание №8

1. Изучите разделы методических указаний и ответьте на вопросы для самопроверки, приведенные в конце темы.
2. Создайте личный ключ шифрования.
3. Запишите свои ключи pubring.pkr и sekring.skr на дискету для дальнейшего использования.
4. Запишите (export) свой публичный (открытый) ключ на дискету (или перешлите по сети) и передайте его участникам электронного обмена информацией.
5. Получите открытые ключи от участников обмена информацией и импортируйте их на свой компьютер.
6. Подпишите ключи партнёров и установите к ним доверие.
7. Создайте файл(ы) в MS Word, зашифруйте его, подпишите электронной подписью и передайте участнику обмена информацией, ключом которого шифровался файл.
8. Получите от участников обмена информацией зашифрованные и подписанные файлы и расшифруйте их.

Тема 2.7. Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне

Индивидуальное задание №9

1. Пользуясь Таблицей 1, изучить работу с утилитами своего варианта.
2. Выполнить операции с этими утилитами с основными параметрами. Результаты сохранить в файле отчета в виде презентации.
3. Пользуясь Консолью администрирования установить оснастку по варианту. Выполнить с ней несколько операций. Результаты сохранить в файле отчета.
4. Пользуясь Консолью администрирования установить Запрет использования внешних носителей (флешек) всем пользователям кроме администратора с помощью групповых политик. Результат сохранить в файле отчета.
5. Ответить на теоретические вопросы по варианту.

Таблица №1

Номер варианта	Утилита	Консоль администри-рования в MS Windows	Вопросы для самосто-ятельной работы
1.	**ping** **netstat /a** **systeminfo**	Политики учетных записей Аудит	1,3,4
2.	**systeminfo** **Ping** **tasklist**	входа в систему	2,5,7
3.	**Ttracert** **Systeminfo** **Ping** **netstat /a**	Локальные политики	8,10, 12
4.	**Netsat /a** **Systeminfo** **tracert**	Шаблоны безопасности	9,11, 13
5.	**Netsat /a** **systeminfo** **Ping** **tracert**	Локальная политика безопасности Создание журналов безопасности	6, 15, 17

2.2. Рекомендации по оцениванию устных ответов обучающихся

С целью контроля усвоения пройденного материала и определения уровня подготовленности обучающихся к изучению новой темы в начале практического занятия преподавателем проводится индивидуальный устный опрос по выполненным заданиям предыдущей темы.

Критерии оценки.

Оценка «отлично» ставится, если обучающийся:

1) полно и аргументировано отвечает по содержанию вопроса;

2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры;

3) излагает материал последовательно и правильно, с соблюдением исторической и хронологической последовательности;

Оценка «хорошо» – ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает одна-две ошибки, которые сам же исправляет.

Оценка «удовлетворительно» – ставится, если обучающийся обнаруживает знание и понимание основных положений данного задания, но:

1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил;

2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;

3) излагает материал непоследовательно и допускает ошибки.

ВОПРОСЫ ДЛЯ САМОПОДГОТОВКИОБУЧАЮЩИХСЯ

Контролируемые разделы (темы) учебной дисциплины	***Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины***)
Раздел 1. Технологии и методы обеспечения ИБ	
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России .	1. Разъясните, в чем заключаются причины роста компьютерной преступности ? 2. Опишите, что такое информация и дайте определение этой категории 3. Разъясните, чем информация отличается от данных? 4. Опишите, что такое знания? 5. Разъясните, что такое информационный объект? 1.
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба	Опишите, какими особенностями отличается информация как объект? 2. Что такое информационное общество? 3. Разъясните, в чем принципиальное отличие пятого экономического и технологического уклада от четвертого (индустриального). 4. Опишите, что такое информационное пространство? 5. Назовите компоненты информационного пространства.
Тема 1.3. Угрозы информационной безопасности .	1. Сформулируйте, что такое угроза информационной безопасности ИС? 2. Что такое источник угрозы безопасности информации? 3. Опишите, на какие группы разделяются угрозы информационной безопасности? 4. Сформулируйте, из каких структурно-функциональных элементов состоят ИС и каким угрозам они могут быть подвержены? 5. Разъясните, что такое естественные угрозы (случайные) ИС?

Контролируемые разделы (темы) учебной дисциплины	***Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины***)
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	1. Сформулируйте, что такое искусственные угрозы ИС? 2. Перечислите непреднамеренные искусственные угрозы ИС? 3. Перечислите преднамеренные искусственные угрозы. 4. Перечислите виды нарушений работоспособности систем и несанкционированного доступа к информации. 5. Разъясните, какие факторы способствуют росту угроз информационных сетевых ресурсов?
Тема 1.5. Технологии защиты от вредоносных програм спама.	1. Опишите, какие виды антивирусных комплексов используются в настоящее время? 2. Сформулируйте, как реализуется сигнатурный и анализ? Опишите его основные достоинства и недостатки? 3. Разъясните, что представляют собой проактивные методы обнаружения? Дайте характеристики двух наиболее известных подходов. 4. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов. 5. Назовите и опишите функции дополнительных модулей антивирусных средств.
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.	1. Сформулируйте модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней. 2. Охарактеризуйте предприятия защиту на уровне его\ корпоративной сети 3. Опишите организацию защиты ИС предприятия на уровне рабочих станций пользователей и серверов 4. Опишите способы защиты информации в организации. Дайте характеристику защитным действий 5. Опишите направления обеспечения ИБ предприятия. Правовая и организационная защита.
Раздел 2. Технология защиты информации	

Контролируемые разделы (темы) учебной дисциплины	***Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины***)
Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия	1. Опишите основные тенденции развития современных вредоносных программ. 2. Опишите основные этапы развития современных вредоносных программ. 3. Сформулируйте основные тенденции развития антивирусного программного обеспечения 4. Разъясните, какие особенности развития информационных технологий способствуют распространению вредоносных программ и угроз с их стороны на уровне обеспечения информационной безопасности отдельного пользователя 5. Разъясните, какие особенности развития информационных технологий способствуют распространению вредоносных программ и угроз с их стороны на уровне обеспечения информационной безопасности организации
Тема 2.2. Основные принципы и методы в области технической защиты информации	1. Сформулируйте, какие объективные и субъекивные факторы создают возможности для утечки конфиденциальной информации. 2. Опишите структуру канала утечки конфиденциальной информации 3. Опишите методы блокирования утечки конфиденциальной информации по визуально-оптическому каналу 4. Опишите методы блокирования утечки конфиденциальной информации по электромагнитным каналам 5. Опишите методы блокирования утечки конфиденциальной информации по акустическому каналу
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации	1. Опишите способы несанкционированного доступа к информации. Приведите примеры реализации каждого из них 2. Опишите методы защиты от наблюдения и подслушивания 3. Опишите методы защиты от подслушивания 4. Опишите методы защиты от перехвата электромагнитных сигналов 5. Опишите методы защиты от перехвата сигналов по сети переменного тока

Контролируемые разделы (темы) учебной дисциплины	***Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины*)**
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ.	1. Сформулируйте, как осуществляется лицензирование и сертификация в сфере информационной безопасности 2. Опишите отечественные стандарты безопасности информационных технологий 3. Сформулируйте значение «Оранжевой книги» в разработке международных стандартов информационной безопасности 4. Опишите требования Стандарта ISO/IEC 27001 к информационной безопасности 5. Опишите стандарты информационной безопасности в Интернет
Тема 2.5. Международные стандарты ИБ. COBIT	1. Сформулируйте, назначение и функции международных стандартов информационной безопасности 2. Сформулируйте, назначение и функции международного стандарта информационной безопасности COBIT 3. Разъясните основные принципы, лежащие в основе стандарта COBIT, в плане взаимодействия ИТ-подразделений организации и ее руководства 4. Разъясните основные принципы, лежащие в основе стандарта COBIT, с точки зрения управления ИТ и менеджментом организации 5. Опишите процесс эволюции стандарта COBIT и отличие его версии COBIT 2019 от предыдущих версий
Тема 2.6. Практические аспекты безопасности ИС	1. На какие этапы разбивается процесс построения КСЗИ организации? 2. Дайте краткое обоснование необходимости каждого этапа построения КСЗИ организации. 3. Опишите первые три этапа создания КСЗИ организации. 4. Опишите задачи, которые решаются на третьем и четвертом этапах создания КСЗИ организации. 5. Перечислите организационные меры, которые разрабатываются в организации в рамках КСЗИ

Контролируемые разделы (темы) учебной дисциплины	***Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины***)
Тема 2.7. Обеспечение безопасности ОС. Безопасность Windows	1. Разъясните, почему необходимо постоянно устанавливались обновления ОС 2. Разъясните, назначение и принципы реализации 7 процедуры резервирования с точки зрения обеспечения безопасности ОС 3. Сформулируйте, какую роль играет аудит безопасности для организации в целом и для фунционирования ОС в частности 4. Опишите процедуру управления политика безопасности в ОС MS Windows 5. Опишите функции Active Directoty и его значения для безопасности ОС MS Windows
Раздел 3. Криптографические методы защиты информации	
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты.	1. Сформулируйте, что такое криптография? В чем заключается главная задача криптографии? 2. Сформулируйте, кто является «противником» в криптографии? Составьте модель противника в криптографии. 3. Опишите, что такое шифр и ключ в криптографии? 4. Сформулируйте, что такое криптографическиий алгоритм (КА). 5. Опишите, в чем заключается Принцип Керкхоффса? Как он применяется на практике?
Тема 3.2. Симметричные криптографические алгоритмы	1. Опишите основные периоды криптографии алгоритмы, которые применялось в эпоху античности и средневековья? 2. Сформулируйте, что такое шифр согласно стандарта ГОСТ 28147— 9? 3. Сформулируйте классификацию криптографических алгоритмов (КА). Приведите примеры бесключевых криптографических алгоритмов (КА). 5. Приведите примеры одноключевых КА.

Контролируемые разделы (темы) учебной дисциплины	***Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины***)
Тема 3.3. Асимметричные криптографические алгоритмы	1. Сформулируйте отличительные особенности асимметричных криптосистем. 2. Опишите преимущества и недостатки асимметричных криптосистем 3. Разъясните, какую роль в инфраструктуре открытых ключей (Public Key Infrastructure, PKI) играет удостоверяющий Центр (УЦ) 4. Опишите функции сертификатов УЦ, а также их содержание 5. Опишите алгоритм RCA. Разъясните, какую роль в его реализации выполняет функция Эйлера
Тема 3.4. Цифровая электронная подпись (ЭЦП).	1. Сформулируйте, в чем заключается предназначение электронной цифровой подписи (ЭЦП). 2. Опишите преимущества применения электронной цифровой подписи 3. Опишите реализацию алгоритма создания ЭЦП и его составных элементов 4. Опишите виды ЭЦП и разъясните их назначение 5. Сформулируйте, какую роль в реализации ЭЦП играет хэш-функция
Тема 3.5. Технологии аутентификации.	1. Разъясните, что такое идентификация. Приведите примеры ее реализации 2. Объясните, что такое аутентификация. Приведите примеры ее реализации 3. Объясните, что такое авторизация. Приведите примеры ее реализации 4. Приведите практические примеры двухфакторной аутентификации 5. Опишите классификацию методов аутентификации.
Раздел 4. Информационная безопасность ИС и сетей	
Тема 4.1. Проблемы информационной безопасности сетей	1. Перечислите уровни модели TCP/IP. 2. Сформулируйте, какие три системы адресации используются в сетевых технологиях? 3. Разъясните, на каком уровне модели OSI задаются IP-адреса? 4. Опишите структуру и функциональность стека протоколов TCP/IP с точки зрения информационной безопасности 5. Сформулируйте проблемы безопасности IP-сетей

Контролируемые разделы (темы) учебной дисциплины	***Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины*)**
Тема 4.2 Угрозы и уязвимости проводных корпоративных сетей	1. Разъясните, какую роль играет модель OSI в реализации взаимодействия открытых систем 2. Опишите четырехуровневую технологическую модель подсистемы информационной безопасности 3. Опишите структуру и функциональность стека протоколов TCP/IP 4. Разъясните, как реализуются логические и физические соединения между уровнями стека протоколов TCP/IP 5. Опишите угрозы и уязвимости проводных корпоративных сетей
Тема 4.3. Технология защиты межсетевого обмена данными. Брандмауэры.	1. Сформулируйте, что такое виртуальная защищенная сеть и туннель VPN. 2. Опишите, на каких технологиях основана защита информации в процессе ее передачи по туннелю VPN 3. Приведите описание таким категориям, как VPN-клиент, VPN-сервер и шлюз безопасности VPN 4. Разъясните, как реализуется технология туннелирования 5. Сформулируйте, как технология туннелирования решает проблему защиты конфиденциальности, целостности и аутентичности передаваемой информации
Тема 4.4. Технологии VPN.	1. Разъясните, какие протоколы играют роль протокола-«пассажира», несущего протокола и протокола туннелирования в технологии VPN 2. Разъясните, каковы варианты построения виртуальных защищенных каналов при использовании VPN 3. Объясните, почему вариант, при котором конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений, С точки зрения обеспечения информационной безопасности является лучшим? 4. Разъясните, с помощью каких компонент в узлах защищенного соединения сети VPN создается туннель 5. Опишите, как обеспечивается конфиденциальность, а также целостность и подлинность инкапсулируемых пакетов при туннелировании в сети VPN

Контролируемые разделы (темы) учебной дисциплины	*Вопросы для подготовки к индивидуальному устному опросу по темам дисциплины*)
Тема 4.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP	1. Опишите процесс инкапсуляция данных и роль, которую он выполняет в стеке TCP/IP 2. Сформулируйте, каковы основные функции Уровня 1 модели OSI 3. Сформулируйте, каковы основные функции
	Уровня 2 модели OSI 4. Опишите структуру стека протоколов TCP/IP и ее отличия от модели OSI. 5. Разъясните, что такое фаза проекта? Привести характеристики фаз и результатов из своего проекта.
Раздел 5. Особенности защиты информации на уровнях модели OSI	
Тема 5.1. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.	1. Разъясните, в чем заключается назначение средств VPN, которые используются на канальном и сеансовом уровне 2. Опишите, какие протоколы используются на канальном и сеансовом уровне, для формирования защищенных каналов в сети VPN 3. Сформулируйте, какие функции необходимо реализовывать протоколам на канальном и сеансовом уровне в сети VPN, для создания защищенного соединения 4. Опишите протоколы формирования защищенных каналов на сеансовом уровне в сети VPN 5. Сформулируйте, какие функции необходимо реализовывать протоколам на сеансовом уровне в сети VPN
Тема 5.2. Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне	1. Опишите как создавался протокол IPSec и для каких целей это делалось. 2. Опишите, для реализации каких функций используется стек протоколов IPSec. Можно ли считать его стеком протоколов и почему 3. Опишите структуру IP-пакета и объясните какие задачи обеспечения безопасности IP-пакетов он решает. 4. Сформулируйте преимущества средств безопасности IPSec 5. Опишите основные схемы применения IPSec

2.3. Рекомендации по оцениванию результатов тестовых заданий обучающихся

В завершении изучения каждого раздела дисциплины проводиться тестирование (контроль знаний по разделу).

Критерии оценивания. Уровень выполнения текущих тестовых заданий оценивается в баллах. Максимальное количество баллов по тестовым заданиям представлено в таблице 2.1.

Тестовые задания представлены в виде оценочных средств и в полном объеме представлены в банке тестовых заданий в электронном виде. В фонде оценочных средств представлены типовые тестовые задания, разработанные для изучения дисциплины «Защита информации в корпоративных информационных системах».

ТИПОВЫЕ ТЕСТОВЫЕ ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗАДАНИЯ ЗАКРЫТОГО ТИПА

Раздел 1. Технологии и методы обеспечения ИБ

ВЫБЕРИТЕ ОДИН ВЕРНЫЙ ОТВЕТ / ВЫБЕРИТЕ НЕСКОЛЬКО ВЕРНЫХ ОТВЕТОВ*

1. *Задание 1.* Информационное общество — это общество, в котором:

   A. большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей её формы — знаний;

   B. постоянно растет количество интернет-пользователей;

   C. реализованы технологии электронного управления и электронного правительства;

   D. электронная коммерция является преобладающей экономической моделью.

Задание 2. Информационный объект – это _____

A. аппаратная часть информационной инфраструктуры, хранящая данные;

B. файлы (документы), ресурсы локальных и глобальных сетей;

C. среда, в которой информация создается, передается, обрабатывается или хранится;

D. файлы (документы), сайты, порталы, средства их создания .

Задание 3. Является ли информационное общество реализацией экономического и технологического уклада?

A. да;

B. нет;

Задание 4. Основными компонентами информационного пространства являются:

A. пользователи, информационные ресурсы, провайдеры;

B. владельцы, провайдеры, информационная инфраструктура;

C. информационные ресурсы, средства информационного взаимодействия, иформационная инфраструктура;

D. государство, владельцы, посредники .

Задание 5. Субъектами информационного пространства являются:

A. государство, юридические лица, физические лица;

B. пользователи, провайдеры, владельцы информации;

C.) государство, пользователи, владельцы информации;

D. физические лица, юридические лица, посредники.

Задание 6. Компьютерные преступления – это те преступления, в которых:

A. с помощью несанкционированного доступа нарушается конфиденциальность информации;

B. результатом является нарушение системы безопасности предприятия;

C. объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер;

D. нарушается целостность и достоверность информации.

Задание 7. Аутентификация субъекта – это:

A. получение субъектом идентификатора, предоставляющего право доступа к определенной части информации,;

B. это проверка подлинности субъекта с данным идентификатором;

C. ввод логина пользователем при входе в локальную сеть;

D. определение прав доступа субъекта с определенным логином и паролем..

Задание 8. Авторизация субъекта – это:

A. проверка подлинности его идентификатора;

B. это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети);

C. проверка соответствия субъекту своему идентификатору;

D. проверка его цифровой подписи.

Задание 9. Злоумышленник – это:

a) лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно;

b) лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.);

c) лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства;

d) нарушитель информационной безопасности, намеренно идущий на нарушение из корыстных побуждений.

Задание Собственник информации – это:

А. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

В. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

С. участник правоотношений в информационных процессах;

D. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

(ответ – все ответы верны – быть не может)

ЗАДАНИЯ ОТКРЫТОГО ТИПА
Раздел 1. Технологии и методы обеспечения ИБ

Задание 1.

Информационная объект – это_____

Задание 2.

Принципы расширения субъектности в информационном пространстве – это_____

Задание 3.

Принцип достижения информационного господства в информационном пространстве – это_____

Задание 4.

Угроза безопасности информации – это_____

Задание 5.

Конфиденциальность информации – это_____

Задание 6.

Целостность информации – это_____

Задание 7.

Достоверность информации – это_____

Задание 8.

Доступность информации – это_____

Задание 9.

Под информационной безопасностью РФ понимается_____

Задание 10.

Неформальная модель нарушителя - это_____

2.4. Рекомендации по оцениванию рефератов, докладов.

Максимальное количество баллов*	Критерии
Отлично	Выставляется обучающемуся, если он выразил своё мнение по сформулированной проблеме, аргументировал его,

	точно определив проблему содержание и составляющие. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно правового характера. Обучающийся знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.
Хорошо	Выставляется обучающемуся, если работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы.Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены отдельные ошибки в оформлении работы.
Удовлетворительно	Выставляется обучающемуся, если в работе студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в содержании проблемы, оформлении работы.
Неудовлетворительно	Выставляется обучающемуся, если работа представляет собой пересказанный или полностью заимствованный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в содержании раскрываемой проблемы, в оформлении работы.

* Представлено в таблице 2.1.

ТЕМЫ РЕФЕРАТОВ, ДОКЛАДОВ ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИИ

1. Глобальные вызовы информационной безопасности в текущем году
2. Требования нормативных и правовых документов РФ по обеспечению защищённости информации в локальных вычислительных сетях
3. Требования нормативных и правовых документов РФ по обеспечению защищённости информации в цифровых телефонных линиях связи
4. Структура и порядок организации работы службы безопасности предприятия в обычных и чрезвычайных условиях.
5. Технологии защиты конфиденциальной информации от вирусных атак.
6. Комплексное обеспечение информационной безопасности в коммерческих структурах.
7. Исследование проблем информационной безопасности объектов критической информационной инфраструктуры.
8. Выявление технических каналов утечки информации.

9. Организация и проведение поисковых мероприятий на объекте с целью обнаружения каналов утечки информации, выявления средств съема информации.
10. Методы и средства защиты информации от утечки по техническим каналам
11. Как обеспечить безопасность при работе в Интернет
12. Национальные интересы России и информационное противостояние в современном мире

ВОПРОСЫ К ДИФФЕРЕНЦИРОВАННОМУ ЗАЧЕТУ ПО РАЗДЕЛАМ (ТЕМАМ) ДИСЦИПЛИНЫ

1. Опишите проактивные методы обнаружения вредоносного ПО.
2. Сформулируйте проблему целостности информации. Приведите примеры нарушения целостности информации.
3. Описать модули и режимы работы современных антивирусных программ.
4. Охарактеризовать модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
5. Описать содержание политики безопасности организации.
6. Охарактеризовать объекты и субъекты информационного пространства. Примеры.
7. Что такое конфиденциальность информации? Описать способы обеспечения конфиденциальности информации в организации.
8. Охарактеризовать субъекты информационных отношений и их интересы.
9. Описать физические и организационно-технические средства защиты в рамках направлений обеспечения ИБ предприятия.
10. Описать организацию защиты информации от утечки по электромагнитным каналам
11. Описать способы защиты информации в организации. Сформулировать характеристику защитных действий
12. Описать организацию защита информации от утечки по визуально оптическим каналам.
13. Сформулировать способы защита информации на уровне корпоративной сети предприятия.
14. Описать технические каналы утечки информации. Защита от утечек информации по техническим каналам
15. Сформулировать понятие «модели злоумышленника». Привести примеры.
16. Описать структуру политики безопасности организации.
17. Охарактеризовать Систему обнаружения и предотвращения вторжений.
18. Описать технологии обеспечения безопасности в ОС Windows 7.
19. Составить классификацию каналов проникновения в информационную систему и утечки информации
20. Описать политику информационной безопасности организации.
21. Определение информационной безопасности и ее составляющие.
22. Указать причины роста компьютерной преступности. Компьютерные преступления против государственных и общественных интересов.
23. Описать ключевые категории (понятия) безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008.

24. Приведите классификацию вредоносных программ.
25. Описать модель нарушителя антивирусной безопасности и рекомендуемые методы защиты для классов нарушителей.
26. Сформулировать тенденции развития современных антивирусных программ
27. Опишите организацию защиты ИС предприятия на уровне рабочих станций пользователей и серверов.
28. Охарактеризовать направления обеспечения ИБ предприятия. Правовая и организационная защита.
29. Описать технологию обеспечения безопасности ИС при беспроводном соединении
30. Опишите сигнатурные методы обнаружения вредоносного ПО.
31. Охарактеризуйте три уровня управления политикой безопасности на предприятии.
32. Охарактеризовать информационная безопасность на базе стандарта CobiT
33. Описать методику создания демилитаризованных зон в корпоративной сети предприятия
34. Описать структуру политики безопасности организации
35. Охарактеризовать критерии безопасности компьютерных систем «Оранжевая книга».
36. Описать организацию защиты периметра сети ИС предприятия с помощью межсетевых экранов (МСЭ)
37. Описать криптоалгоритм Диффи-Хеллмана.
38. Описать сигнатурные методы обнаружения вредоносного ПО.
39. Описать симметричные алгоритмы шифрования. Примеры
40. Охарактеризовать информационную войну как угрозу информационной безопасности национального уровня.
41. Описать криптографический алгоритм Виженера. Преимущества и недостатки.
42. Описать преимущества и недостатки симметричных алгоритмов шифрования
43. Описать порядок использования систем с симметричными ключами.
44. Описать классификацию криптографических алгоритмов
45. Раскрыть понятие «модели злоумышленника». Привести примеры.
46. Охарактеризовать атаку вида «Посредничество в обмене незашифрованными ключами (атака man-in-the-middle)» и способы защиты от нее.
47. Охарактеризовать атаку вида «Отказ в обслуживании (Denial of Service, DoS)» и способы защиты от нее.
48. Охарактеризовать атаку вида «Отказ в обслуживании (Denial of Service, DoS)» и способы защиты от нее
49. Охарактеризовать парольную атаку вида «полного перебора (brute force attack)» и способы защиты от нее.
50. Охарактеризовать преимущества и недостатки блочных симметричных систем шифрования.
51. Охарактеризовать атаку вида «Троянский конь» и способы защиты от нее.

52. Описать криптографический алгоритм Вернама. Преимущества и недостатки.
53. Охарактеризовать атаку вида «Эксплойт» и способы защиты от нее.
54. Охарактеризовать технологии биометрической аутентификации пользователя.
55. Описать практические методы аутентификации, используемые в настоящее время.
56. Охарактеризовать угрозы ИБ и систему защитных мер для уровней модели OSI для организации

ВОПРОСЫ К ЭКЗАМЕНУ ПО РАЗДЕЛАМ (ТЕМАМ) ДИСЦИПЛИНЫ

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 MS Windows. 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

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ»

Направление подготовки 09.03.03 Прикладная информатика
Профиль «Прикладная информатика в управлении корпоративными информационными системами»
Кафедра информационных технологий
Дисциплина «Информационная безопасность информационных системах»
Курс 3 Семестр 5,6 Форма обучения очная

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1

Теоретические вопросы.

1. Составить классификацию каналов проникновения в информационную систему иутечки информации
2. Описать методы защита информации на сетевом уровне. Протокол IPSec.

Практическое задание.

3. Зашифруйте и расшифруйте сообщение «Перекрытие каналов утечки» с ключем
«Процедура» методом Виженера. Для этой цели составьте алгоритм и программу наExcel, Visual Basic или C++.

Экзаменатор: _____ _____

Утверждено на заседании кафедры «____» _____20___г. (протокол №_____от «___» _____20___г.)

*Зав.кафедрой:*_____Н.В. Брадул