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**

"УТВЕРЖДАЮ"
Проректор
Л.Н. Костина
27.04.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.01 **"Информационная безопасность"**

Направление подготовки 40.03.01 Юриспруденция
Профиль "Юриспруденция"

Квалификация ***БАКАЛАВР***

Форма обучения ***очная***

Общая трудоемкость ***2 ЗЕТ***

Год начала подготовки по учебному плану ***2023***

Донецк
2023

Составитель(и):
канд. экон. наук, доцент И.В. Стешенко

Рецензент(ы):
канд. экон. наук, доцент Н.Э. Тарусина

Рабочая программа дисциплины "Информационная безопасность" разработана в соответствии с:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 40.03.01 Юриспруденция (приказ Минобрнауки России от 13.08.2020 г. № 1011)

Рабочая программа дисциплины составлена на основании учебного плана Направление подготовки 40.03.01 Юриспруденция
Профиль "Юриспруденция", утвержденного Ученым советом ФГБОУ ВО "ДОНАУИГС" от 27.04.2023 протокол № 12.

Срок действия программы: 2023-2027

Рабочая программа рассмотрена и одобрена на заседании кафедры Информационных технологий

Протокол от 20.04.2023 № 9

Заведующий кафедрой:

канд. физ.-мат. наук, доцент, Брадул Н.В.

(подпись)

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024 - 2025 учебном году на заседании кафедры Информационных технологий

Протокол от "____"_____2024 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 2025 - 2026 учебном году на заседании кафедры Информационных технологий

Протокол от "____"_____2025 г. №___

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

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

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

Протокол от "____"_____2026 г. №___

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

Визирование РПД для исполнения в очередном учебном году

"УТВЕРЖДАЮ"

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

Протокол от "____"_____2027 г. №___

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

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.04

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

Правоохранительные органы

Психология личности и профессиональное самоопределение юриста

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

Информационные технологии в юридической деятельности

Уголовное право (общая часть)

Уголовное право (особенная часть)

1.4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

ОПК-8.1: Знает существующие базы данных, включая правовые базы данных, и способы получения из них информации

Знать:

Уровень 1	нормативные правовые документы из существующих баз данных в сфере информационной безопасности
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 получения информации из баз данных с учетом требований информационной безопасности

1.4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

ОПК-8.3: Владеет навыками систематизации и обобщения полученной информации с применением информационных технологий и с учетом требований информационной безопасности

Знать:

Уровень 1	уровни управления политикой безопасности на предприятии
Уровень 2	практические методы аутентификации, используемые в настоящее время
Уровень 3	защиту информации на уровне корпоративной сети предприятия

Уметь:

Уровень 1	применять технологии использования электронной цифровой подписи

Уровень 2	проводить классификацию механизмов аутентификации пользователей
Уровень 3	определять нарушения целостности информации
Владеть:	
Уровень 1	системой обнаружения и предотвращения вторжений
Уровень 2	терминами и определениями криптографии
Уровень 3	технологией биометрической аутентификации пользователя

1.4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

ОПК-9.1: Владеет навыками систематизации и обобщения полученной информации с применением информационных технологий и с учетом требований информационной безопасности

Знать:	
Уровень 1	типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду
Уровень 2	методы защиты информации
Уровень 3	типовые средства защиты информации
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 вычислительных 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 Зачет

РАЗДЕЛ 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. ТРУДОЕМКОСТЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Общая трудоёмкость дисциплины "Информационная безопасность" составляет 2 зачётные единицы, 72 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/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.3Л3 .2 Э1 Э2 Э3	0	
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России . /Пр/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.3Л3 .3 Э1 Э2 Э3	0	
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России . /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.3Л3 .2 Л3.4 Э1 Э2 Э3	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.1 Э1 Э2 Э3	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Пр/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.2Л3 .2 Л3.3 Э1 Э2 Э3	0	
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.4Л3 .2 Л3.4 Э1 Э2 Э3	0	
Тема 1.3. Угрозы информационной безопасности . /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.2Л3 .2 Э1 Э2 Э3	0	
Тема 1.3. Угрозы информационной безопасности . /Пр/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.3Л3 .2 Л3.3 Э1 Э2 Э3	0	
Тема 1.3. Угрозы информационной безопасности . /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.3Л3 .4 Э1 Э2 Э3	0	

Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.1Л3.2 Э1 Э2 Э3	0	
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии /Пр/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.4Л3.3 Э1 Э2 Э3	0	
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.1Л3.4 Э1 Э2 Э3	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.2Л3.2 Э1 Э2 Э3	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Пр/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.3Л3.3 Э1 Э2 Э3	0	
Тема 1.5. Технологии защиты от вредоносных программ и спама. /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1 Л1.3Л2.3Л3.4 Э1 Э2 Э3	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.4Л3.2 Э1 Э2 Э3	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Пр/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.2Л3.3 Э1 Э2 Э3	0	
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность. /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.4Л3.4 Э1 Э2 Э3	0	
Раздел 2. Технология защиты информации						
Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.1Л3.1 Л3.5 Э1 Э2 Э3	0	
Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.2Л3.2 Э1 Э2 Э3	0	

Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.3Л3.3 Э1 Э2 Э3	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.4Л3.4 Э1 Э2 Э3	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.1Л3.5 Э1 Э2 Э3	0	
Тема 2.2. Основные принципы и методы в области технической защиты информации /Ср/	3	3	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.2Л3.1 Э1 Э2 Э3	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.3Л3.2 Э1 Э2 Э3	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.4Л3.3 Э1 Э2 Э3	0	
Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.1Л3.4 Э1 Э2 Э3	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.2Л3.5 Э1 Э2 Э3	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.3Л3.1 Э1 Э2 Э3	0	
Тема 2.4. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.4Л3.2 Э1 Э2 Э3	0	
Тема 2.5. Международные стандарты ИБ. COBIT /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.1Л3.3 Э1 Э2 Э3	0	
Тема 2.5. Международные стандарты ИБ. COBIT /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.2Л3.4 Э1 Э2 Э3	0	

Тема 2.5. Международные стандарты ИБ. COBIT /Ср/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.3Л3.5 Э1 Э2 Э3	0	
Тема 2.6. Практические аспекты безопасности ИС /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.4Л3.1 Э1 Э2 Э3	0	
Тема 2.6. Практические аспекты безопасности ИС /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.1Л3.2 Э1 Э2 Э3	0	
Тема 2.6. Практические аспекты безопасности ИС /Ср/	3	3	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.2Л3.3 Э1 Э2 Э3	0	
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.3Л3.4 Э1 Э2 Э3	0	
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.1Л3.5 Э1 Э2 Э3	0	
Тема 2.7. Обеспечение безопасности ОС. Безопасность MS /Ср/	3	3	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.2Л3.1 Э1 Э2 Э3	0	
Раздел 3. Криптографические методы защиты информации						
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.1Л3.2 Э1 Э2 Э3	0	
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Пр/	3	0,5	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.2Л3.3 Э1 Э2 Э3	0	
Тема 3.1. Криптографические методы защиты информации. Классификация криптографических методов защиты. /Ср/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.3Л3.4 Э1 Э2 Э3	0	
Тема 3.2. Симметричные криптографические алгоритмы /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.4Л3.5 Э1 Э2 Э3	0	

Тема 3.2. Симметричные криптографические алгоритмы /Пр/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.1Л3.1 Э1 Э2 Э3	0	
Тема 3.2. Симметричные криптографические алгоритмы /Ср/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.2Л3.2 Э1 Э2 Э3	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.3Л3.3 Э1 Э2 Э3	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Пр/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.4Л3.4 Э1 Э2 Э3	0	
Тема 3.3. Асимметричные криптографические алгоритмы /Ср/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.1Л3.5 Э1 Э2 Э3	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.2Л3.1 Э1 Э2 Э3	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Пр/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.3Л3.2 Э1 Э2 Э3	0	
Тема 3.4. Цифровая электронная подпись (ЭЦП). /Ср/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.4Л3.3 Э1 Э2 Э3	0	
Тема 3.5. Технологии аутентификации. /Лек/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.1Л2.1Л3.4 Э1 Э2 Э3	0	
Тема 3.5. Технологии аутентификации. /Пр/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.2Л2.2Л3.5 Э1 Э2 Э3	0	
Тема 3.5. Технологии аутентификации. /Ср/	3	1	ОПК-8.1 ОПК-8.3 ОПК-9.1	Л1.3Л2.3Л3.1 Э1 Э2 Э3	0	
/Конс/	3	2	ОПК-8.1 ОПК-8.3 ОПК-9.1		0	

РАЗДЕЛ 3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

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

2. При изложении теоретического материала используются такие методы:
- монологический;
- показательный;
- диалогический;
- эвристический;
- исследовательский;
- проблемное изложение.

3. Используются следующие принципы дидактики высшей школы:
- последовательность обучения;
- систематичность обучения;
- доступность обучения;
- принцип научности;
- принципы взаимосвязи теории и практики;
- принцип наглядности и др.

В конце каждой лекции предусмотрено время для ответов на проблемные вопросы.

4. Самостоятельная работа предназначена для внеаудиторной работы студентов, связанной с конспектированием источников, учебного материала, изучением дополнительной литературы по дисциплине, подготовкой к текущему и семестровому контролю, а также выполнением индивидуального задания в форме реферата, эссе, презентации, эмпирического исследования.

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

4.1. Рекомендуемая литература

1. Основная литература

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

2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год
Л2.1	П. Н. Башлы, А. В. Бабаш, Е. К. Баранова.	Информационная безопасность и защита информации: Учебное пособие (311 с.)	Евразийский открытый институт, 2012
Л2.2	Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева.	Информационная безопасность : учебное пособие: Учебное пособие (221 с.)	Государственный Аграрный Университет им. Императора Петра

	Авторы,	Заглавие	Издательство, год
			Первого, 2015
Л2.3	Д. В. Фомин.	Информационная безопасность : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика»: Учебно-методическое пособие (125 с.)	Вузовское образование, 2018
Л2.4	Е. М. Скурыдина.	Информационная безопасность : учебное пособие: Учебное пособие (313 с.)	Алтайский государственный педагогический университет, 2017

3. Методические разработки

	Авторы,	Заглавие	Издательство, год
Л3.1	Семичастный И.Л. Семичастный И.Л.	Рабочая программа по учебной дисциплине «Информационная безопасность» для обучающихся 3 курса образовательной программы бакалавриата направления подготовки 9.03.03 «Прикладная информатика» очной/заочной форм обучения / сост. И.Л. Семичастный. – Протокол заседания кафедры информационных технологий № 1 от 29.08.2022 г: Рабочая программа (27 с.)	Донецк: ГОУ ВПО "ДОНАУИГС", 2022
Л3.2	Семичастный И.Л.	Конспект лекций по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Конспект лекций (147 с.)	Донецк: ГОУ ВПО "ДОНАУИГС", 2022
Л3.3	Семичастный И.Л.	Методические рекомендации для проведения практических занятий по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Методические рекомендации (35 с.)	Донецк: ГОУ ВПО "ДОНАУИГС", 2022
Л3.4	Семичастный И.Л.	Методические рекомендации для самостоятельной работы студентов по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Методические рекомендации (28 с.)	Донецк: ГОУ ВПО "ДОНАУИГС", 2022
Л3.5	Семичастный И.Л.	Индивидуальные задания для самостоятельной работы по учебной дисциплине «Информационная безопасностьх» (для студентов направления подготовки 09.03.03 Прикладная информатика) .- Протокол заседания кафедры информационных технологий №1 от 29.08.2022 г: Индивидуальные задания (87 с.)	Донецк: ГОУ ВПО "ДОНАУИГС", 2022

4.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Научная электронная библиотека «КиберЛенинка»	https://cyberleninka.ru/
Э2	Научная электронная библиотека	http://elibrary.ru
Э3	Библиотека ФГБОУ ВО «ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ГЛАВЕ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ»	https://donampa.ru/biblioteka

4.3. Перечень программного обеспечения

Лицензионное и свободно распространяемое программное обеспечение, в том числе

отечественного производства:
При проведении лекций используется аудитория с мультимедийным оборудованием. Аудиторные занятия проводятся в компьютерных классах с доступом к сети Интернет. Для проведения консультаций в online-режиме используется LMS Moodle и Яндекс.Телемост.
Программное обеспечение:
1. Операционная система Windows XP и выше; пакет Microsoft Office 2010 и выше.

При изучении дисциплины также используются информационные технологии противодействия вредоносному ПО и спаму. Для этого используются следующие демонстрационные версии и свободнораспространяемые пакеты антивирусных программ: Avast, Microsoft Essentials, AVG, Avira, , Dr Web, ESET, Kaspersky Antivirus 2015, Kaspersky Internet Security, Comodo Internet Security, Spybot, Bitdefender, 360Total Security, Symantec Endpoint Protection, McAfee, Panda Security.
Кроме того при изучении технологий криптографии используется компьютерные программы PGP и TrueCrypt, а также библиотека функций, позволяющие выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске.
При изучении технологий VPN (Virtual Private Network) используется программа LogMeIn Hamachi. При изучении дисциплины используется ПО в составе пакета OS MS Windows, MS Office 2010.

4.4. Профессиональные базы данных и информационные справочные системы

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ФГБОУ ВО "ДОНАУИГС") и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобильных устройств.

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

4.5. Материально-техническое обеспечение дисциплины

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

РАЗДЕЛ 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

1. Информационная война как угроза информационной безопасности национального уровня.
2. Объекты и субъекты информационного пространства. Примеры.

3. Субъекты информационных отношений и их интересы.
4. Три уровня управления политикой безопасности на предприятии.
5. Варианты построения виртуальных защищенных каналов.
6. Понятие «модели злоумышленника». Привести примеры.
7. Конфиденциальность информации. Способы обеспечения конфиденциальности информации в организации.
8. Практические методы аутентификации, используемые в настоящее время.
9. Классификация каналов проникновения в систему и утечки информации.
10. Политика информационной безопасности организации.
11. Содержание политики безопасности организации.
12. Определение информационной безопасности и ее составляющие.
13. Причины роста компьютерной преступности. Компьютерные преступления против государственных и общественных интересов.
14. Ключевые категории (понятия) безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008.
15. Классификация вредоносных программ.
16. Сигнатурные методы обнаружения вредоносного ПО.
17. Проактивные методы обнаружения вредоносного ПО.
18. Тенденции развития современных антивирусных программ.
19. Модули и режимы работы современных антивирусных программ.
20. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
21. Защита периметра сети ИС предприятия с помощью межсетевых экранов (МСЭ).
22. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
23. Модель нарушителя антивирусной безопасности. Рекомендуемые методы защиты для классов нарушителей.
24. Тенденции развития современных антивирусных программ.
25. Защита информации на уровне корпоративной сети предприятия.
26. Технические каналы утечки информации. Защита от утечек информации по техническим каналам.
27. Модули и режимы работы современных антивирусных программ.
28. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
29. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
30. Модель нарушителя антивирусной безопасности. Рекомендуемые методы защиты для классов нарушителей.
31. Защита информации на уровне корпоративной сети предприятия.
32. Методика создания демилитаризованных зон в корпоративной сети предприятия.
33. Защита информации от утечки по электромагнитным каналам.
34. Технические каналы утечки информации. Защита от утечек информации по техническим каналам.
35. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
36. Технология обеспечения безопасности ИС при беспроводном соединении.
37. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.
38. Система обнаружения и предотвращения вторжений.
39. Технологии обеспечения безопасности в ОС Windows.
40. Способы защиты информации в организации. Характеристика защитных действий
41. Защита информации от утечки по визуально оптическим каналам.
42. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
43. Технология обеспечения безопасности ИС при беспроводном соединении.
44. Система обнаружения и предотвращения вторжений.
45. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.
46. Защита информации от утечки по электромагнитным каналам.
47. Информационная безопасность на базе стандарта CobiT.
48. Термины и определения криптографии.
49. Классификация криптографических алгоритмов.
50. Критерии безопасности компьютерных систем «Оранжевая книга».
51. Криптографический алгоритм Виженера. Преимущества и недостатки.
52. Технологии биометрической аутентификации пользователя.
53. Преимущества и недостатки симметричных алгоритмов шифрования.

54. Проблемы безопасности IP-сетей.
55. Порядок использования систем с симметричными ключами.
56. Технологии строгой аутентификации пользователя.
57. Симметричные алгоритмы шифрования. Примеры.
58. Структура и функциональность стека протоколов TCP/IP с точки зрения информационной безопасности.
59. Технология использование электронной цифровой подписи.
60. Классификация механизмов аутентификации пользователей.
61. Классификация сетей VPN. Преимущества применения технологий VPN.
62. Структура политики безопасности организации .
63. Преимущества и недостатки асимметричных систем шифрования.
64. Технологии виртуальных защищенных сетей (VPN). Основные понятия и функции сети VPN.
65. Порядок использования систем с асимметричными ключами.
66. Протоколы формирования защищенных каналов сети VPN на сеансовом уровне.
67. Проблема целостности информации. Примеры нарушения целостности информации.
68. Основные варианты архитектуры VPN. Средства обеспечения безопасности VPN.
69. Методы защиты информации на канальном и сеансовом уровнях.
70. Методы защита информации на сетевом уровне. Протокол IPSec.

5.2. Темы письменных работ

Письменные работы не предусмотрены

5.3. Фонд оценочных средств

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

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

5.4. Перечень видов оценочных средств

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

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

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

1) с применением электронного обучения и дистанционных технологий.

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

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

- для лиц с нарушениями зрения: учебно-методические материалы в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные задания и консультации.
- для лиц с нарушениями слуха: учебно-методические материалы в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: учебно-методические материалы в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

РАЗДЕЛ 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО УСВОЕНИЮ ДИСЦИПЛИНЫ

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

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

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

изучаемой дисциплиной.
Подготовку к любой теме курса рекомендуется начинать с изучения презентационных материалов или учебной литературы, в которых дается систематизированное изложение материала, разъясняется смысл разных терминов и сообщается об изменениях в подходах к изучению тех или иных проблем данного курса.
Методические указания по организации самостоятельной работы
Самостоятельная работа по дисциплине организована в следующих видах:
1. изучение теоретического материала по заданной теме;
2. анализ методов решения поставленной задачи;
3. выполнение индивидуальных заданий;
4. оценка достоверности полученных результатов;
5. отчет перед преподавателем по теоретической и практической части индивидуальной работы.

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	40.03.01 Юриспруденция
Профиль	«Юриспруденция»
Квалификация	бакалавр
Форма обучения	очная

Донецк
2023

Фонд оценочных средств по дисциплине «Информационная безопасность» для обучающихся 2 курса образовательной программы бакалавриата направления подготовки 40.03.01 Юриспруденция (профиль: «Юриспруденция») очной формы обучения

Автор,
разработчик: доцент, канд. экон. наук, доцент, Стешенко И.В.

ФОС рассмотрен на
заседании кафедры *информационных технологий*

Протокол заседания кафедры от 20.04.2023 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	40.03.01 Юриспруденция «Юриспруденция»
Количество разделов учебной дисциплины	3
Часть образовательной программы	Б1.О.04.01
Формы текущего контроля	Собеседование, индивидуальные задания, устный опрос
Показатели	Очная форма обучения
Количество зачетных единиц (кредитов)	2
Семестр	3
Общая трудоемкость (академ. часов)	72
Аудиторная контактная работа:	38
Лекционные занятия	18
Практические занятия	18
Консультации	2
Самостоятельная работа	34
Контроль	-
Форма промежуточной аттестации	зачет

1.2. Перечень компетенций с указанием этапов формирования впроцессе освоения образовательной программы

Таблица 2

Перечень компетенций и их элементов

Компетенция	Индикатор компетенции и его формулировка	Элементы индикатора компетенции	Индекс элемента
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Владеет навыками систематизации и обобщения полученной информации с применением информационных технологий и с учетом требований информационной безопасности	***Знать:***	
		1. типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду. 2. методы защиты информации. 3. типовые средства защиты информации.	ОПК-9.1 З-1 ОПК-9.1 З-2 ОПК-9.1 З-3
		Уметь:	
		1. использовать типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду. 2. использовать типовые программно-аппаратные средства и системы зашиты информации от нарушения ее целостности. 3. использовать методы защиты информации в вычислительных системах и сетях.	ОПК-9.1 У-1 ОПК-9.1 У-2 ОПК-9.1 У-3
		Владеть:	

		1. навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях. 2. типовыми программно-аппаратными средствами обеспечения доступности информации. 3. навыками использования типовых программно-аппаратных средств и системзашиты информации от несанкционированного доступа в компьютерную среду.	ПК-9.2 В-1 ПК-9.2 В-2 ПК-9.2 В-3

Код компетенции	Формулировка компетенции	Элементы компетенции	Индекс элемента
ОПК-8. Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности	ОПК-8.1. Знает существующие базы данных , включая правовые базы данных и способы получения из них информации	***Знать:***	
		1. нормативные правовые документы из существующих баз данных всфере информационной безопасности. 2. виды угроз ИС. 3. методы обеспечения информационной безопасности.	ОПК 8.1 З-1 ОПК 8.1 З-2 ОПК 8.1 З-3
		Уметь:	
		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 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 8.1 У-1 ОПК 8.1 У-2 ОПК 8.1 У-3

		Владеть:	
		1. международными и отечественными стандартами в области обеспечения безопасности информационных систем и технологий.	ОПК 8.1 В-1
		2. способностью блокировать угрозы безопасности ИС предприятия с помощью методов обеспечения защиты информации.	ОПК 8.1 В-2
		3. навыками получения информации из баз данных с учетом требований информационной безопасности.	ОПК 8.1 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 .	3	ОПК 9.1 З-1 ОПК 8.1 У-1	Индивидуальная работа №1
2.	Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба	3	ОПК 8.1 З-1 ОПК 8.1 У-2	Индивидуальная работа №1 Устный опрос (вопросы, выносимые на самостоятельное обучение)
3.	Тема 1.3. Угрозы информационной безопасности .	3	ОПК 8.1 З-1 ОПК 8.1 В-1	Индивидуальная работа №2
4.	Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	3	ОПК 8.1 З-3 ОПК 8.1 В-1	Индивидуальная работа №2 Устный опрос (вопросы, выносимые на самостоятельное обучение)
5.	Тема 1.5. Технологии защиты от вредоносных программ и спама.	3	ОПК 8.1 З-2 ОПК-9.1 В-1	Индивидуальная работа №3
6.	Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.	3	ОПК 8.1 З-1 ОПК-9.1 В-1	Индивидуальная работа №3 Устный опрос (вопросы, выносимые на

				самостоятель-ное обучение)
Раздел 2. Технологии защиты информации				
7.	Тема 2.1. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия	3	ОПК 8.1 У-2 ОПК 8.1 В-1 ОПК-9.1 В-2	Индивидуальная работа №4
8.	Тема 2.2. Основные принципы и методы в области технической защиты информации	3	ОПК 8.1 У-1 ОПК 8.1 В-1 ОПК-9.1 В-3	Индивидуальная работа №4 Устный опрос (вопросы, выносимые на самостоятельное обучение)
9.	Тема 2.3. Противодействие несанкционированному доступу к конфиденциальной информации	3	ОПК 8.1 У-3 ОПК 8.1 В-2 ОПК 9.1 В-1	Индивидуальная работа №4
10.	Тема 2.4. Критерии защищенности ком-пьютерных систем. Лицензирование и сертификация ИБ	3	ОПК 8.1 У-1 ОПК 8.1 В-1 ОПК-9.1 В-2	Индивидуальная работа №4 Устный опрос (вопросы, выносимые на самостоятельное обучение)
11.	Тема 2.5. Междуна-родные стандарты ИБ. COBIT	3	ОПК 8.1 У-2 ОПК 8.1 В-3 ОПК-9.1 В-3	Индивидуальная работа №4
12.	Тема 2.6. Практические аспекты безопасности ИС	3	ОПК 8.1 У-3 ОПК 8.1 В-2 ОПК-9.1 В-2	Индивидуальная работа №4 Устный опрос (вопросы, выносимые на самостоятельное обучение)

13.	Тема 2.7. Обеспечение безопасности ОС. Безопасность Windows	3	ОПК 8.1 У-1 ОПК 8.1 У-2 ОПК-9.1 В-1	Индивидуальная работа №5
Раздел 3. Криптографические методы защиты информации				
14.	Тема 3.1. Крипто-графические методы защиты информации. Классификация криптографических методов защиты.	3	ОПК 8.1 У-3 ОПК 8.1 В-2 ОПК 9.1 В-3	Индивидуальная работа №5 Устный опрос (вопросы, выносимые на самостоятельное обучение)
15.	Тема 3.2. Симметричные криптографические алгоритмы	3	ОПК 8.1 У-1 ОПК 8.1 В-2 ОПК 9.1 В-2	Индивидуальная работа №5
16.	Тема 3.3. Асимметричные криптографические алгоритмы	3	ОПК 8.1 У-2 ОПК 8.1 В-1 ОПК 9.1 В-1	Индивидуальная работа №5
17.	Тема 3.4. Цифровая электронная подпись (ЭЦП).	3	ОПК 8.1 У-3 ОПК 8.1 В-3 ПК 9.1 В-2	Индивидуальная работа №5
18.	Тема 3.5. Технологии аутентификации.	3	ОПК 8.1 У-2 ОПК 8.1 В-3 ПК 9.1 В-3	Индивидуальная работа №5 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 учебной 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							
Р.1.Т.1.2							
Р.1.Т.1.3							
Р.1.Т.1.4							
Р.1.Т.1.5							
Р.1.Т.1.6		2	10	12	10	10	3
Р.2.Т.2.1							
Р.2.Т.2.2							
Р.2.Т.2.3							
Р.2.Т.2.4							
Р.2.Т.2.5							
Р.2.Т.2.6							
Р.2.Т.2.7		3	10	13	10	10	3
Р.3.Т.3.1							
Р.1.Т.3.2							
Р.1.Т.3.3							
Р.1.Т.3.4							
Р.1.Т.3.5		5	10	15	10		4
Итого: 100б		**10**	**30**	**40**	**30**	**20**	**10**

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

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.

Индивидуальное задание №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 ли они надежными?

5. Создайте на основе изученных Вами правил надежный пароль уровня Strong. Запишите его и используйте в своей работе.
6. Ознакомьтесь с программным продуктом хранения паролей KeePass? Скачав его с интернет-ресурса https://keepass.info/.
7. Для знакомства с работой программы, скачайте программу, установите программу KeePass и создайте свою базу данных паролей.
8. Создайте свою портативную базу на сменном носителе. Создание новой базы паролей. Добавьте записи о пароле в базу. Добавьте в свою базу все пароли: для почты, соцсетей и другие пароли.
9. Ознакомьтесь с работой генератора паролей. Воспользуйтесь генератором для создания мастер- пароля.
10. Создание резервной копии базы. Создать резервную базу паролей.
11. Все результаты подтвердите скриншотами.
12. Ознакомьтесь с работой сервиса хранения паролей LastPass https://www.lastpass.com/ru
13. Для сервиса **LastPass** повторите пункты с 6 по 10.
14. Все результаты подтвердите скриншотами.

2.2. Рекомендации по оцениванию устных ответов обучающихся

С целью контроля усвоения пройденного материала и определения уровня подготовленности обучающихся к изучению новой темы вначале 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 САМОПОДГОТОВКИ ОБУЧАЮЩИХСЯ

Контролируемые разделы (темы) дисциплины	Вопросы для контроля знаний по разделам 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?
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба	1. 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?
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 программ и спама.	1. Опишите, какие виды антивирусных комплексов используются в настоящее время? 2. Сформулируйте, как реализуется сигнатурный 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	
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.
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.
Тема 2.7. Обеспечение безопасности ОС. Безопасность Windows 7	1. Разъясните, почему необходимо постоянно устанавливались обновления ОС. 2. Разъясните, назначение и принципы реализации 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. Крипто-графические 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). 4. Приведите примеры бесключевых криптографических алгоритмов (КА).

	5. Приведите примеры одноключевых КА.
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.

ВОПРОСЫ К ЗАЧЕТУ ПО РАЗДЕЛАМ (ТЕМАМ) ДИСЦИПЛИНЫ

1. Сформулируйте проблему целостности информации. Приведите примерынарушения целостности информации.
2. Описать модули и режимы работы современных антивирусных программ.
3. Охарактеризовать модель автоматизированной системы (ИС) и типывирусных угроз безопасности ИС для ее различных уровней.
4. Описать содержание политики безопасности организации.
5. Охарактеризовать объекты и субъекты информационного пространства.Примеры.
6. Что такое конфиденциальность информации? Описать способы обеспечения конфиденциальности информации в организации.

7. Охарактеризовать субъекты информационных отношений и их интересы.

8. Описать физические и организационно-технические средства защиты врамках направлений обеспечения ИБ предприятия.

9. Описать организацию защиты информации от утечки по электромагнитным каналам.

10. Описать способы защиты информации в организации. Сформулироватьхарактеристику защитных действий

11. Описать организацию защита информации от утечки по визуально оптическим каналам.

12. Сформулировать способы защита информации на уровне корпоративнойсети предприятия.

13. Описать технические каналы утечки информации. Защита от утечекинформации по техническим каналам.

14. Сформулировать понятие «модели злоумышленника». Привести примеры.

15. Описать структуру политики безопасности организации.

16. Охарактеризовать систему обнаружения и предотвращения вторжений.

17. Описать технологии обеспечения безопасности в ОС Windows.

19. Составить классификацию каналов проникновения в информационнуюсистему и утечки информации.

20. Описать политику информационной безопасности организации. 21.Определение информационной безопасности и ее составляющие.

21. Указать причины роста компьютерной преступности.

22. 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.

31. Охарактеризовать информационная безопасность на базе стандарта CobiT.

32. Описать методику создания демилитаризованных зон в корпоративной сети предприятия.

33. Описать структуру политики безопасности организации.

34. Охарактеризовать критерии безопасности компьютерных систем «Оранжевая книга».

35. Описать организацию защиты периметра сети ИС предприятия с помощью межсетевых экранов (МСЭ).

36. Описать криптоалгоритм Диффи-Хеллмана.

37. Описать сигнатурные методы обнаружения вредоносного ПО. 39.Описать симметричные алгоритмы шифрования. Примеры.

38. Охарактеризовать информационную войну как угрозу информационной безопасности национального уровня.

39. Описать криптографический алгоритм Виженера. Преимущества и недостатки.

40. Описать преимущества и недостатки симметричных алгоритмов шифрования.

41. Описать порядок использования систем с симметричными ключами.

42. Описать классификацию криптографических алгоритмов.

43. Раскрыть понятие «модели злоумышленника». Привести примеры.

44. Охарактеризовать атаку вида «Посредничество в обмене незашифрованными ключами (атака man-in-the-middle)» и способы защиты от нее.

45. Охарактеризовать атаку вида «Отказ в обслуживании (Denial of Service, DoS)» и способы защиты от нее.

46. Охарактеризовать атаку вида «Отказ в обслуживании (Denial of Service, DoS)» и способы защиты от нее.

47. Охарактеризовать парольную атаку вида «полного перебора (brute force attack)» и способы защиты от нее.

48. Охарактеризовать преимущества и недостатки блочных симметричных систем шифрования.

49. Охарактеризовать атаку вида «Троянский конь» и способы защиты от нее.

50. Описать криптографический алгоритм Вернама. Преимущества и недостатки.

51. Охарактеризовать атаку вида «Эксплойт» и способы защиты от нее.

52. Охарактеризовать технологии биометрической аутентификации пользователя.

53. Описать практические методы аутентификации, используемые в настоящее время.

54. Охарактеризовать угрозы ИБ и систему защитных мер для уровней модели OSI для организации.