

Документ подписан простой электронной подписью  
Информация о владельце:

ФИО: Мещеряков Николай Николаевич

Должность: Ректор

Дата подписания: 17.10.2023 10:38:10

Уникальный программный ключ:

c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ

Начальник отдела лицензирования и аккредитации

Чаленко К.Н.

« 07 » 06 2020 г.

**Рабочая программа дисциплины  
Информационная безопасность**

Специальность 38.05.01 "Экономическая безопасность" специализация 38.05.01.01  
"Экономико-правовое обеспечение экономической безопасности"

Для набора 2016 года

Квалификация  
Экономист

**КАФЕДРА Информационные технологии и защита информации****Распределение часов дисциплины по курсам**

Курс Вид занятий	3		Итого	
	уп	рп		
Лекции	4	4	4	4
Практические	6	6	6	6
Итого ауд.	10	10	10	10
Контактная работа	10	10	10	10
Сам. работа	58	58	58	58
Часы на контроль	4	4	4	4
Итого	72	72	72	72

**ОСНОВАНИЕ**

Учебный план утвержден учёным советом вуза от 25.02.2020 протокол № 8.

Программу составил(и): к.э.н., доцент, Рутта Н.А. 

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. 

Методическим советом направления: дэн, профессор, Суржиков М.А. 

### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	изучение принципов обеспечения информационной безопасности, видов защищаемой информации в системе экономической безопасности государства и получение практических навыков применения различных информационных ресурсов и технологий, применяемых при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности
-----	---

### 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**ОК-12:** способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

**ПК-28:** способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач

**ПК-41:** способностью принимать участие в разработке стратегии обеспечения экономической безопасности организаций, подготовке программ по ее реализации

**ПСК-2:** способностью использовать при решении профессиональных задач возможности лиц, оказывающих содействие органам внутренних дел

#### В результате освоения дисциплины обучающийся должен:

**Знать:**

- информационные возможности лиц, оказывающих содействие органам внутренних дел при решении профессиональных задач
- информационные средства, необходимые в разработке стратегии обеспечения экономической безопасности организаций и программы по их реализации;
- методы сбора, анализа, систематизации, оценки и интерпретации данных для решения профессиональных задач;

- различные информационные ресурсы и технологии, применяемые при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности;

**Уметь:**

- применять информационные возможности лиц, оказывающих содействие органам внутренних дел при решении профессиональных задач
- осуществлять выбор информационных средств, необходимых в разработке стратегии обеспечения экономической безопасности организаций и программы по их реализации;
- применять различные методы сбора, анализа, систематизации, оценки и интерпретации данных для решения профессиональных задач;

- осуществлять выбор и применять различные информационные ресурсы и технологии, применяемые при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности;

**Владеть:**

- информационными возможностями лицам, оказывающих содействие органам внутренних дел при решении профессиональных задач
- основными методами применения информационных средств, необходимых в разработке стратегии обеспечения экономической безопасности организаций и программы по их реализации;
- различными методами сбора, анализа, систематизации, оценки и интерпретации данных для решения профессиональных задач;

- различными информационными ресурсами и технологиями, применяемыми при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности;

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
	<b>Раздел 1. Общие вопросы информационной безопасности. Правовые основы защиты коммерческой тайны и конфиденциальной информации</b>				
1.1	Тема 1. «Введение в информационную безопасность». Понятие информации, защиты информации, информационной системы, информационной безопасности. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность. /Лек/	3	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.3

1.2	Практическое занятие 1. «Введение в информационную безопасность. Работа с документами с системе Консультант Плюс". Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Работа в программе MS Word. /Пр/	3	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Практическое занятие 2. «Парольные системы идентификации и аутентификации пользователей». Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС Windows по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи. /Пр/	3	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Вопросы для самостоятельного изучения. Правовые основы лицензирования в области защиты информации. Сущность и содержание сертификации в области защиты информации. Правовые основы защиты коммерческой тайны. Правовые основы защиты конфиденциальной информации. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Неформальная модель нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации. Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Виды утечки информации. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации. Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей. Защита электронной почты. /Ср/	3	30	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.3
<b>Раздел 2. Методы и средства криптографической защиты</b>					
2.1	Тема 1. «Принципы криптографической защиты информации». Понятие криптографии, шифрования и дешифрования, ключа шифрования, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем. /Лек/	3	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.3
2.2	Практическое занятие 3. «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. Система шифрования Цезаря. Шифры перестановки. /Пр/	3	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Вопросы для самостоятельного изучения: Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для криптографической защиты информации. Особенности использования вычислительной техники в криптографии. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана. Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA /Ср/	3	28	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.3
2.4	/Зачёт/	3	4	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

#### 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	<a href="https://biblioclub.ru/index.php?page=book&amp;id=438331">https://biblioclub.ru/index.php?page=book&amp;id=438331</a> неограниченный доступ для зарегистрированных пользователей
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	<a href="https://biblioclub.ru/index.php?page=book&amp;id=493175">https://biblioclub.ru/index.php?page=book&amp;id=493175</a> неограниченный доступ для зарегистрированных пользователей
Л1.3	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	<a href="http://www.iprbookshop.ru/86938.html">http://www.iprbookshop.ru/86938.html</a> неограниченный доступ для зарегистрированных пользователей

### 5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2014	<a href="https://biblioclub.ru/index.php?page=book&amp;id=230502">https://biblioclub.ru/index.php?page=book&amp;id=230502</a> неограниченный доступ для зарегистрированных пользователей
Л2.2	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	<a href="http://www.iprbookshop.ru/86357.html">http://www.iprbookshop.ru/86357.html</a> неограниченный доступ для зарегистрированных пользователей
Л2.3	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	<a href="http://www.iprbookshop.ru/87995.html">http://www.iprbookshop.ru/87995.html</a> неограниченный доступ для зарегистрированных пользователей

### 5.3 Профессиональные базы данных и информационные справочные системы

Справочная правовая система "Консультант Плюс"

ФСТЭК России/fstec.ru

Web of Science apps.webofknowledge.com

ScienceDirect <https://www.sciencedirect.com/>

### 5.4. Перечень программного обеспечения

MS Windows

MS Word

### 5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

**6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование.

**7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
<b>ОК-12: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации</b>			
З: различные информационные ресурсы и технологии, применяемые при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности;	изучает основную и дополнительную литературу, лекционный материал; знает основные источники и правила доступа, а также использования информации, в том числе в профессиональных целях; знает основные методы хранения и обработки информации, а также ее трансляции при подготовке к зачету	соответствие ответов материалам лекций и учебной литературы, сведениям из информационных ресурсов Интернет; сформировавшееся систематическое знание основных источников и правил доступа, а также использования информации, в том числе в профессиональных целях; основных методов хранения и обработки информации, а также ее трансляции при ответе на вопросы зачета	З (1-20) УО (Раздел 1 вопросы 1-24, Раздел 2 вопросы 1-8)
У: осуществлять выбор и применять различные информационные ресурсы и технологии, применяемые при получении, хранении, систематизации,	умеет находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять уровень	сформировавшееся систематическое умение находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных	ПЗ (1, 2) ПОЗ (2, 3, 4,6)

обработки и передачи информации в профессиональной деятельности;	достоверности источников информации и давать ей критическую оценку для решения практико-ориентированных и практических заданий	задач; определять уровень достоверности источников информации и давать ей критическую оценку при выполнении практико-ориентированных и практических заданий	
В: различными информационными ресурсами и технологиями, применяемыми при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности;	обладает навыками использования современных информационно-коммуникационных технологий и различных ресурсов для решения практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками использования современных информационно-коммуникационных технологий и различных информационных ресурсов при выполнении практико-ориентированных и практических заданий	ПЗ (1, 2) ПОЗ (2, 3, 4,6)
<b>ПК-28: способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач</b>			
З: методы сбора, анализа, систематизации, оценки и интерпретации данных для решения профессиональных задач;	знает принципы и критерии сбора, анализа, систематизации, оценки и интерпретации данных при подготовке к зачету	сформировавшееся систематическое знание принципов и критериев сбора, анализа, систематизации, оценки и интерпретации данных при ответе на вопросы зачета	З (1-31) УО (Раздел 1 вопросы 1-24, Раздел 2 вопросы 1-16)
У: применять различные методы сбора, анализа, систематизации, оценки и интерпретации данных для решения профессиональных задач;	обобщает информацию и формирует базы данных, обрабатывает эмпирические и экспериментальные данные при решении практико-ориентированных и практических заданий	сформированные умения обобщать информацию и формировать базы данных, обрабатывать эмпирические и экспериментальные данные при выполнении практико-ориентированных и практических	ПЗ (1, 2, 3) ПОЗ (1, 2, 3, 4, 5, 6, 7, 8)

		заданий	
В: различными методами сбора, анализа, систематизации, оценки и интерпретации данных для решения профессиональных задач	владеет навыками работы с информационными данными при выполнении практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками работы с информационными данными при выполнении практико-ориентированных и практических заданий	ПЗ (1, 2, 3) ПОЗ (1, 2, 3, 4, 5, 6, 7, 8)
<b>ПК-41: способностью принимать участие в разработке стратегии обеспечения экономической безопасности организаций, подготовке программ по ее реализации</b>			
З: информационные средства, необходимые в разработке стратегии обеспечения экономической безопасности организаций и программы по их реализации;	знает методы разработки стратегии обеспечения экономической безопасности организаций при подготовке зачету	корректность использования методов разработки стратегии обеспечения экономической безопасности организаций при ответе на вопросы зачета	З (5,16-31) УО (Раздел 1 вопросы 6, 21-24, Раздел 2 вопросы 11-16)
У: осуществлять выбор информационных средств, необходимых в разработке стратегии обеспечения экономической безопасности организаций и программы по их реализации;	анализирует угрозы экономической безопасности при планировании и осуществлении стратегии обеспечения экономической безопасности при выполнении практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками анализа угроз экономической безопасности при планировании и осуществлении стратегии обеспечения экономической безопасности при выполнении практико-ориентированных и практических заданий	ПЗ (1, 2, 3) ПОЗ (1, 2, 3, 4, 5, 6)

В: основными методами применения информационных средств, необходимых в разработке стратегии обеспечения экономической безопасности организаций и программы по их реализации;	владеет навыками подготовки программ по реализации стратегии экономической безопасности предприятия при выполнении практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками подготовки программ по реализации стратегии экономической безопасности предприятия при выполнении практико-ориентированных и практических заданий	ПЗ (1, 2, 3) ПОЗ (1, 2, 3, 4, 5, 6)
<b>ПСК-2: способностью использовать при решении профессиональных задач возможности лиц, оказывающих содействие органам внутренних дел</b>			
З: информационные возможности лиц, оказывающих содействие органам внутренних дел при решении профессиональных задач	знает виды потенциальных и реальных угроз экономической безопасности организации при подготовке к зачету	сформировавшееся систематическое знание видов потенциальных и реальных угроз экономической безопасности организации при ответе на вопросы зачета	З (2-31) УО (Раздел 1 вопросы 2-24, Раздел 2 вопросы 11-16)
У: применять информационные возможности лиц, оказывающих содействие органам внутренних дел при решении профессиональных задач	применяет возможности лиц, оказывающих содействие органам внутренних дел, в целях определения потенциальных и реальных угроз экономической безопасности организации при выполнении практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками применения возможности лиц, оказывающих содействие органам внутренних дел, в целях определения потенциальных и реальных угроз экономической безопасности организации при выполнении практико-ориентированных и практических заданий	ПЗ (1, 2, 3) ПОЗ (1, 2, 3, 4, 5, 6, 7, 8)
В: информационными возможностями лицам, оказывающих содействие органам внутренних дел при	владеет навыками привлечения лиц, оказывающих содействие органам внутренних дел для оценки	сформировавшееся систематическое владение навыками привлечения лиц, оказывающих содействие органам	ПЗ (1, 2, 3) ПОЗ (1, 2, 3, 4, 5, 6, 7, 8)

решении профессиональных задач	потенциальных и реальных угроз экономической безопасности организации при выполнении практико-ориентированных и практических заданий	внутренних дел для оценки потенциальных и реальных угроз экономической безопасности организации при выполнении практико-ориентированных и практических заданий	
--------------------------------	--	--	--

*ПЗ – практические задания, ПОЗ - практико-ориентированные задания к зачету, З – вопросы к зачету, УО- устный опрос*

### 1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

50-100 баллов (зачет)  
0-49 баллов (незачет)

## 2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

В разделе приводятся типовые варианты оценочных средств: вопросы к зачету, практико-ориентированные задания к зачету, практические задания, вопросы для устного опроса

### Вопросы к зачету по дисциплине

1. Понятие информации, защиты информации, информационной системы, информационной безопасности. Базовые свойства информации
2. Нормативно-правовая база функционирования систем защиты информации.
3. Российское законодательство по защите информационных технологий.
4. Правовая защита программного обеспечения авторским правом.
5. Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование.
6. Правовые основы лицензирования в области защиты информации.
7. Сущность и содержание сертификации в области защиты информации.
8. Правовые основы защиты коммерческой тайны.
9. Правовые основы защиты конфиденциальной информации.
10. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.

11. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации.
12. Понятие угрозы, классификация угроз.
13. Понятие уязвимости, атаки на компьютерную систему.
14. Понятие канала утечки информации, виды утечки, основные каналы утечки информации.
15. Классификация злоумышленников.
16. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
17. Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей.
18. Защита электронной почты.
19. Понятие криптографии, шифрования и дешифрования, ключа шифрования, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы.
20. Классификация криптосистем.
21. Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера.
22. Система шифрования Цезаря.
23. Шифры перестановки.
24. Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра.
25. Требования к шифрам, используемым для криптографической защиты информации.
26. Особенности использования вычислительной техники в криптографии.
27. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
28. Понятие и назначение центра распределения ключей.
29. Требования Диффи и Хеллмана.
30. Алгоритм шифрования RSA.
31. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA

### Типовые практико-ориентированные задания к зачету

Задание 1. Определить вероятности реализации угроз в ИСПДн. По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы.

Задание 2. Центральный банк РФ для анализа экономической ситуации запросил у АО «Тюмень Нефть» информацию о количестве полученной прибыли за прошедший год и о прогнозах объема добычи нефти на текущий год. Однако АО не предоставило и с требуемой информации, мотивировав

тем, что информация отнесена к коммерческой тайне. Проанализируйте ч. 4 ст. 57 ФЗ РФ «О Центральном банке Российской Федерации (Банке России)» и определите, имеет ли право Банк России получать данную информацию, и несёт ли ответственность Банк России, а также его должностные лица и работники за разглашение коммерческой тайны.

Задание 3. Член-корреспондент Академии наук разработал теорию, которая позволила разработать в конструкторском бюро техническое устройство и внедрить его на производстве металлообрабатывающего завода. Свою теорию и возможности её практического применения учёный доложил на международной конференции. Новое техническое устройство позволило металлообрабатывающему заводу увеличить свои доходы и занять лидирующее положение в данном производстве. Руководство завода приняло решение отнести информацию о техническом устройстве к коммерческой тайне. Соответствует ли это законодательству о коммерческой тайне?

Задание 4. В научно-исследовательской лаборатории одного ВУЗа была разработана антикоррозионная присадка защиты корпуса автомобиля от ржавчины. Разработчики не стали подавать заявку на получение патента на изобретение, а решили данную разработку использовать как секрет производства (НОУ-ХАУ) и самостоятельно изготавливать и продавать присадку потребителям. Какие меры должны быть приняты в данной лаборатории для обеспечения защиты этой разработки. Если аналогичная присадка будет самостоятельно разработана другими лицами, будет ли оставаться данная разработка в режиме коммерческой тайны.

Задание 5. Определите, какие степени секретности должны быть установлены в отношении следующих групп сведений:

- сведения в отношении системы противоракетной защиты РФ;
- сведения в области научно-технической деятельности Министерства юстиции;
- показатели, которые составляют расходную часть бюджета на текущий год;
- информация, которая составляет сведения о военных разработках завода;
- разработка ФСБ по проведению контртеррористической операции по ликвидации бандформирования;
- сведения о размерах золотого запаса и государственных валютных резервах РФ;
- экономические показатели военного завода.

Задание 6. Выполнить следующие действия:

- создать учетную запись пользователя с ограниченными правами.

- выполнить защиту электронной почты.
- выполнить сегментирование.
- выполнить установку паролей.
- выполнить удаление ограниченной учетной записи.

Задание 7. С помощью алгоритма RSA зашифровать слово КОШКА (6. 5. 1). Для реализации алгоритма использовать числа  $p=11$ ,  $q=13$ .

Задание 8. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ГРУША – ЮЛОУЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

#### Критерии оценивания:

- 50-100 баллов (зачет) – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе; практико-ориентированное задание выполнено правильно и прокомментировано; наличие твердых и достаточно полных знаний, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, неуверенность и неточность ответов на дополнительные и наводящие вопросы; практико-ориентированное задание выполнено правильно, но не прокомментировано; при неполном ответе на вопросы; затрудняется ответить на дополнительные вопросы; практико-ориентированное задание выполнено с ошибками и отсутствуют комментарии;

30 баллов за 1 теоретический вопрос

30 баллов за 2 теоретический вопрос

40 баллов за выполненное практико-ориентированное задание

- 0-49 баллов (незачет) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы; практико-ориентированное задание не выполнено.

#### Практические задания

##### 1. Тематика практических заданий по разделам и темам

**Раздел 1 «Общие вопросы информационной безопасности. Правовые основы защиты коммерческой тайны и конфиденциальной информации»**

## Перечень вопросов для устного опроса

### Раздел 1. Общие вопросы информационной безопасности. Правовые основы защиты коммерческой тайны и конфиденциальной информации

1. Понятие информации, защиты информации, информационной системы, информационной безопасности
2. Базовые свойства информации: конфиденциальность, целостность, доступность.
3. Нормативно-правовая база функционирования систем защиты информации.
4. Российское законодательство по защите информационных технологий.
5. Правовая защита программного обеспечения авторским правом.
6. Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование.
7. Правовые основы лицензирования в области защиты информации.
8. Сущность и содержание сертификации в области защиты информации.
9. Правовые основы защиты коммерческой тайны.
10. Правовые основы защиты конфиденциальной информации.
11. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
12. Неформальная модель нарушителя.
13. Причины несанкционированного доступа к информации.
14. Последствия несанкционированного доступа к информации.
15. Понятие угрозы, классификация угроз.
16. Понятие уязвимости, атаки на компьютерную систему.
17. Понятие риска.
18. Виды утечки информации.
19. Понятие канала утечки информации, основные каналы утечки информации.
20. Классификация злоумышленников.
21. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
22. Особенности парольных систем, основные типы угроз безопасности парольных систем.
23. Требования к выбору и использованию паролей.
24. Защита электронной почты.

### Раздел 2. Методы и средства криптографической защиты

1. Понятие криптографии, шифрования и дешифрования, ключа шифрования, шифротекста, криптоалгоритма.
2. Принципы функционирования криптографической системы.
3. Классификация криптосистем.
4. Процесс шифрования текста с помощью таблицы Вижинера.
5. Расшифровка текста с помощью таблицы Вижинера.
6. Система шифрования Цезаря.
7. Шифры перестановки.

Практическое занятие 1 (14 баллов). «Введение в информационную безопасность. Работа с документами в системе Консультант Плюс». Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом.

#### Критерии оценивания:

Правильно выполненное задание – 11-14 баллов

При выполнении задания были допущены незначительные ошибки - 5-10 баллов;

При выполнении задания были допущены существенные ошибки – 1-4 балла;

Неправильно выполненное задание – 0 баллов

Практическое занятие 2 (20 баллов). «Парольные системы идентификации и аутентификации пользователей». Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС Windows по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи.

#### Критерии оценивания:

Правильно выполненное задание – 16-20 баллов

При выполнении задания были допущены незначительные ошибки - 7-15 баллов;

При выполнении задания были допущены существенные ошибки – 1-6 баллов;

Неправильно выполненное задание – 0 баллов

### Раздел 2 «Методы и средства криптографической защиты».

Практическое занятие 3 (30 баллов). «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. Система шифрования Цезаря. Шифры перестановки

#### Критерии оценивания:

Правильно выполненное задание – 21-30 баллов

При выполнении задания были допущены незначительные ошибки - 8-20 баллов;

При выполнении задания были допущены существенные ошибки – 1-7 баллов;

Неправильно выполненное задание – 0 баллов

Максимальное количество баллов по практическим заданиям – 64

8. Понятие криптоанализа, криптоаналитической атаки.
9. Основные типы криптоаналитических атак, криптостойкость шифра.
10. Требования к шифрам, используемым для криптографической защиты информации.
11. Особенности использования вычислительной техники в криптографии.
12. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
13. Понятие и назначение центра распределения ключей.
14. Требования Диффи и Хеллмана.
15. Алгоритм шифрования RSA.
16. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA

**Критерии оценивания:**

Для каждого вопроса:

- 2 балла дан полный ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное;
- 1 балл – в ответе на поставленный вопрос были неточности;
- 0 баллов – обучающийся не владеет материалом по заданному вопросу.

Максимальное количество баллов – 36

**3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

**Текущий контроль** успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

**Промежуточная аттестация** проводится в форме зачета.

Зачет проводится по окончании теоретического обучения до начала экзаменационной сессии. Количество вопросов в задании – 3 (2 теоретических вопроса и 1 практико-ориентированное задание к зачету). Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке

## МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия;

В ходе лекционных занятий рассматриваются вопросы информационной безопасности в системе экономической безопасности государства, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки применения различных информационных ресурсов и технологий, применяемых при получении, хранении, систематизации, обработки и передачи информации в профессиональной деятельности.

При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на практических должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий посредством устного опроса. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.