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.
«01» 06 2020г.

Рабочая программа дисциплины
Информационная безопасность

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

Для набора 2018, 2019, 2020 года

Квалификация
Экономист

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	4 (2.2)		5 (3.1)		Итого	
Недель	18		18			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	18	18	18	18	36	36
Лабораторные	18	18			18	18
Практические			18	18	18	18
Итого ауд.	36	36	36	36	72	72
Контактная работа	36	36	36	36	72	72
Сам. работа	72	72	72	72	144	144
Часы на контроль			36	36	36	36
Итого	108	108	144	144	252	252

ОСНОВАНИЕ

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

Программу составил(и): к.э.н., доцент Шарыпова Т.Н. _____ 01.06.2020 г.

Зав. кафедрой: к.э.н., доцент Ефимова Е.В. _____ 01.06.2020 г

Методическим советом направления: дэн, профессор Суржиков М.А. _____ 01.06.2020

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры; развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления; привитие стремления к поиску оптимальных, простых и надежных решений; расширение кругозора.

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:

различные информационные ресурсы и технологии;
способы сбора, анализа, систематизации, оценки и интерпретации данных;
стратегии обеспечения экономической безопасности организаций и программы по их реализации;
способы решения профессиональных задач.

Уметь:

применять основные способы получения, хранения, поиска, систематизации информации;
осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных для решения профессиональных задач;
применять различные стратегии обеспечения экономической безопасности организаций и программы по их реализации;
применять возможности лиц, оказывающих содействие органам внутренних дел при решении профессиональных задач.

Владеть:

применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;
методиками проведения анализа научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности;
обеспечения экономической безопасности организаций;
привлечения лиц, оказывающих содействие органам внутренних дел для решении профессиональных задач.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
	Раздел 1. Общие вопросы информационной безопасности				
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/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.2	Тема 1 «Введение в информационную безопасность". Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования с использованием текстового редактора MS Word. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Тема 1 "Введение в информационную безопасность". Правовая защита информации. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

1.4	Тема 2 «Санкционированный и несанкционированный доступ». 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. /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Тема 2 «Санкционированный и несанкционированный доступ». Несанкционированный доступ к информации (НСД). Идентификация. Аутентификация. Выбор паролей с использованием текстового редактора MS Word. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.6	Тема 2 «Санкционированный и несанкционированный доступ». Административная защита информации. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.7	Тема 3 «Понятие угрозы, уязвимости, риска». Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Виды утечки информации в юриспруденции. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников. /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.8	Тема 3 «Понятие угрозы, уязвимости, риска». Технологии организации работы с информацией в среде Windows. Поиск, сохранение информации, проверка на вирусы. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.9	Тема 3. «Понятие угрозы, уязвимости, риска». Уязвимость компьютерных систем. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.10	Тема 4 «Ценность информации». Понятие ценности информации. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации. /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.11	Тема 4 «Ценность информации». Способы защиты информации на ПК. Вирусы, антивирусные программы с использованием текстового редактора MS Word. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.12	Тема 4 «Ценность информации». Административная защита информации. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.13	Тема 5 «Парольные системы идентификации и аутентификации пользователей». Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей. /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.14	Тема 5 «Парольные системы идентификации и аутентификации пользователей». Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.15	Тема 5 «Парольные системы идентификации и аутентификации пользователей». Защита электронной почты. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 2. Методы и средства криптографической защиты				
2.1	Тема 1 «Принципы криптографической защиты информации». Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем. /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	Тема 1 «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Тема 1 «Принципы криптографической защиты информации». Таблица Вижинера. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

2.4	Тема 2 «Элементы криптоанализа». Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для криптографической защиты информации. /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.5	Тема 2 «Элементы криптоанализа». Метод встречи в середине атаки. Вероятностный метод криптоанализа. Анализ возможности возникновения коллизии. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.6	Тема 2 «Элементы криптоанализа». Особенности использования вычислительной техники в криптографии. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.7	Тема 3 «Симметричные криптосистемы». Принцип функционирования симметричных криптосистем. Функциональная схема взаимодействия участников симметричного криптографического обмена. Недостатки симметричных криптосистем. Основные виды симметричных шифров. /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.8	Тема 3 «Симметричные криптосистемы». Система шифрования Цезаря. Шифры перестановки. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.9	Тема 3 «Симметричные криптосистемы». Шифр Гронсфельда. Шифры многоалфавитной замены. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.10	Тема 4 «Асимметричные криптосистемы». Принцип функционирования асимметричных криптосистем, Функциональная схема взаимодействия участников асимметричного криптографического обмена. Достоинства и недостатки асимметричных криптосистем. 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 . /Лек/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.11	Тема 4 «Асимметричные криптосистемы». Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Целостность передаваемых данных. Авторство сообщений с использованием текстового редактора MS Word. /Лаб/	4	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.12	Тема 4 «Асимметричные криптосистемы». Основные математические соотношения, используемые в алгоритме RSA. Технология взлома шифра методом полного перебора. /Ср/	4	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.13	/Зачёт/	4	0	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 3. Основные организационно-технические мероприятия по защите информации				
3.1	Тема 1 «Правовые основы лицензирования в области защиты информации». Структура системы государственного лицензирования. Порядок проведения лицензирования. Государственные органы по лицензированию. /Лек/	5	4	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.2	Тема 1 «Правовые основы лицензирования в области защиты информации». Изучение положений о государственном лицензировании деятельности в области защиты информации. Организационная структура системы государственного лицензирования в области защиты информации. Контроль за деятельностью лицензиатов. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию. /Пр/	5	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.3	Тема 1 «Правовые основы лицензирования в области защиты информации». Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации. Федеральные законы в области информации и информационной безопасности. Указы президента РФ и постановления Правительства РФ в области информации и информационной безопасности. Правовые режимы защиты информации. Правовые вопросы защиты информации с использованием технических средств. /Ср/	5	12	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.4	Тема 2 "Аттестация объектов информации". Система объектов информатизации по требованиям безопасности информации. Виды аттестации объектов информатизации по требованиям безопасности информации. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации. /Лек/	5	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.5	Тема 2 "Аттестация объектов информации". Изучение положения по аттестации объектов информатизации по требованиям безопасности информации. Порядок проведения аттестации и контроля. /Пр/	5	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.6	Тема 2 "Аттестация объектов информации". Функции испытательных центров (лабораторий) и заявителей по аттестации объектов информатизации по требованиям безопасности информации. Система объектов информатизации по требованиям безопасности информации. Виды аттестации помещений по требованиям безопасности информации. Особенности проведения аттестации помещений по требованиям безопасности информации. /Ср/	5	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.7	Тема 3 «Правовые основы сертификации в РФ». Структура системы сертификации. Сущность и содержание сертификации в области защиты информации. /Лек/	5	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.8	Тема 3 «Правовые основы сертификации в РФ». Система сертификации средств защиты информации по требованиям безопасности информации. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации. Виды и схемы сертификации средств защиты информации. Функции ФСТЭК в области сертификации средств защиты информации. Функции органов сертификации средств защиты информации. Функции испытательных лабораторий (центров). Функции заявителей. Порядок проведения сертификации и контроля. Перечень средств защиты информации, подлежащих сертификации. /Ср/	5	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.9	Тема 3 «Правовые основы сертификации в РФ». Изучение положений о сертификации средств защиты информации по требованиям безопасности информации. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации с использованием текстового редактора MS Word. /Пр/	5	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.10	Тема 4 "Категорирование защищаемой информации". Категории конфиденциальности защищаемой информации. Категории целостности информации. Категории доступности информации. Определение типа информации. /Лек/	5	2	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.11	Тема 4 "Категорирование защищаемой информации". Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта. Определение содержания и местонахождения защищаемых ресурсов на объекте. Построение плана объекта. Определениезащищаемых зон на плане. Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты. Построение структурной модели защищаемой информации. Определение категории защищаемого объекта с использованием текстового редактора MS Word. /Пр/	5	4	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

3.12	Тема 4 "Категорирование защищаемой информации". Анализ структуры, деятельности и защищаемых ресурсов объекта. Категорирование объекта защиты. /Ср/	5	8	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 4. Правовые основы защиты государственной тайны и коммерческой тайны				
4.1	Тема 1 «Правовые основы защиты коммерческой тайны». Правовые основы защиты коммерческой тайны. Виды информации, составляющей коммерческую тайну. Объекты защиты коммерческой тайны. Права и обязанности обладателя коммерческой тайны. Основные угрозы коммерческой тайны. Правовая защита коммерческой тайны. /Лек/	5	4	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.2	Тема 1 «Правовые основы защиты коммерческой тайны». Порядок отнесения информации к коммерческой тайне. Изучение и анализ нормативной базы в области защиты государственной тайны. Анализ правовых методов защиты сведений, составляющих государственную тайну, изучение порядка и сущности допуска к защищаемым сведениям. /Пр/	5	4	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.3	Тема 1 «Правовые основы защиты коммерческой тайны». Содержание договорной работы в области передачи охраняемой информации. Условия наступления ответственности за разглашение коммерческой тайны. Гражданско — правовая ответственность за разглашение коммерческой тайны. Уголовная ответственность за разглашение коммерческой тайны. Дисциплинарная и материальная ответственность за разглашение коммерческой тайны. Административная ответственность за разглашение коммерческой тайны. /Ср/	5	18	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.4	Тема 2 «Правовое регулирование и защита государственной тайны". Понятие государственной тайны и принципы засекречивания информации. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. Перечень сведений, составляющих государственную тайну. Ограничения в отнесении информации к государственной тайне. Порядок засекречивания сведений и их носителей и формы допуска граждан к государственной тайне. Органы защиты государственной тайны. Ответственность за нарушение законодательства о государственной тайне. /Лек/	5	4	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.5	Тема 2 «Правовое регулирование и защита государственной тайны". Государственная тайна. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. /Пр/	5	4	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.6	Тема 2 «Правовое регулирование и защита государственной тайны". Правовые основы защиты государственной тайны. Полномочия органов государственной власти в области отнесения сведений к государственной тайне и их защиты. Организационно-правовые основы деятельности подразделений защиты государственной тайны. Реквизиты носителей сведений, составляющих государственную тайну. /Ср/	5	18	ОК-12 ПК-28 ПК-41 ПСК-2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.7	/Экзамен/	5	36	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	https://biblioclub.ru/index.php?page=book&id=438331 неограниченный доступ для зарегистрированных пользователей
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.3	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	http://www.iprbookshop.ru/86938.html 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	https://biblioclub.ru/index.php?page=book&id=230502 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	http://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Справочная правовая система "Консультант Плюс"

ScienceDirect https://www.sciencedirect.com/

Web of Science apps.webofknowledge.com

Библиоклуб.ру http://biblioclub.ru/

ЭБС «IPR Books» http://www.iprbookshop.ru/

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. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

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
ОК-12: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации			
З: различные информационные ресурсы и технологии	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 тестированию, зачету и экзамену	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 тестирования, зачета и экзамена	Т (Раздел 1 тема 2 вопрос 1-2; Раздел 2 тема 3 вопрос 1-3; Раздел 3 тема 3 вопрос 1-2; Раздел 4 тема 1 вопрос 1), З (вопросы 21-28, 39-49), Э (вопросы 1-3, 13-15, 37-42)
У: применять основные способы получения, хранения, поиска, систематизации информации	умеет находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять	сформировавшееся систематическое умение находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения	ЛЗ (Раздел 1 ЛЗ1, ЛЗ5); ПЗ (Раздел 4 ПЗ1); ПОЗЭ (раздел 3 задание 1) ПОЗЗ (раздел 1 задание 1,6)
	уровень достоверности источников информации и давать ей критическую оценку для решения лабораторных, практико-ориентированных и практических заданий	профессиональных задач; определять уровень достоверности источников информации и давать ей критическую оценку при выполнении лабораторных, практико-ориентированных и практических заданий	
В: применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	обладает навыками использования современных информационно-коммуникационных технологий и различных информационных ресурсов для решения лабораторных, практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками использования современных информационно-коммуникационных технологий и различных информационных ресурсов при выполнении лабораторных, практико-ориентированных и практических заданий	ЛЗ (Раздел 2 ЛЗ 1-2); ПЗ (Раздел 3 ПЗ1) ПОЗЭ (раздел 4 задание 1) ПОЗЗ (раздел 2 задание 1)
ПК-28: способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач			
З: способы сбора, анализа, систематизации, оценки и интерпретации данных	знает принципы и критерии сбора, анализа, систематизации, оценки и интерпретации данных при подготовке к тестированию, зачету и экзамену	сформировавшееся систематическое знание принципов и критериев сбора, анализа, систематизации, оценки и интерпретации данных при ответе на вопросы тестирования, зачета и экзамена	Т (Раздел 1 тема 1 вопрос 1-3, тема 5 вопрос 1-2; Раздел 2 тема 4 вопрос 1-2; Раздел 3 тема 2 вопрос 1-3; Раздел 4 тема 2 вопрос 1), З (вопросы 1-8, 29-32, 50- 57), Э (вопросы 29-36, 43-48)
У: осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных для решения профессиональных задач	обобщает информацию и формирует базы данных, обрабатывает эмпирические и экспериментальные	сформированные умения обобщать информацию и формировать базы данных, обрабатывать эмпирические и экспериментальные	ЛЗ (Раздел 2 ЛЗ 3); ПЗ (Раздел 4 ПЗ1); ПОЗЭ (раздел 3 задание 2); ПОЗЗ (раздел 1 задание 2)

	данные при решении лабораторных, практико-ориентированных и практических заданий	данные при выполнении лабораторных, практико-ориентированных и практических заданий	
В: методиками проведения анализа научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности	владеет навыками работы с информационными данными при выполнении лабораторных, практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками работы с информационными данными при выполнении лабораторных, практико-ориентированных и практических заданий	ЛЗ (Раздел 2 ЛЗ4); ПЗ (Раздел 3 ПЗ2) ПОЗЭ (раздел 4 задание 2) ПОЗЗ (раздел 2 задание 2, 5)
ПК-41: способностью принимать участие в разработке стратегии обеспечения экономической безопасности организаций, подготовке программ по ее реализации			
З: стратегии обеспечения экономической безопасности организаций и программы по их реализации	знает методы разработки стратегии обеспечения экономической безопасности организаций при подготовке к тестированию, зачету и экзамену	корректность использования методов разработки стратегии обеспечения экономической безопасности организаций при ответе на вопросы тестирования, зачета и экзамена	Т (Раздел 1 тема 4 вопрос 1-2; Раздел 2 тема 1 вопрос 1-2; Раздел 3 тема 1 вопрос 1-3; Раздел 4 тема 2 вопрос 2-3), З (вопросы 9-17, 58-63), Э (вопросы 16-28, 49-52)
У: применять различные стратегии обеспечения экономической безопасности организаций и программы по их реализации	анализирует угрозы экономической безопасности при планировании и осуществлении стратегии обеспечения экономической безопасности при выполнении лабораторных, практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками анализа угроз экономической безопасности при планировании и осуществлении стратегии обеспечения экономической безопасности при выполнении лабораторных, практико-ориентированных и практических заданий	ЛЗ (Раздел 1 ЛЗ 3); ПЗ (Раздел 4 ПЗ2 задание 1); ПОЗЭ (раздел 3 задание 3) ПОЗЗ (раздел 1 задание 3)
В: обеспечения экономической безопасности организаций	владеет навыками подготовки программ по реализации стратегии экономической безопасности предприятия при выполнении лабораторных, практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками подготовки программ по реализации стратегии экономической безопасности предприятия при выполнении лабораторных, практико-ориентированных и практических заданий	ЛЗ (Раздел 1 ЛЗ 4); ПЗ (Раздел 3 ПЗ3); ПОЗЭ (раздел 4 задание 3); ПОЗЗ (раздел 2 задание 3, 6)
ПСК-2: способностью использовать при решении профессиональных задач возможности лиц, оказывающих содействие органам внутренних дел			
З: способы решения профессиональных задач	знает виды потенциальных и реальных угроз экономической безопасности организации при подготовке к тестированию, зачету и экзамену	сформировавшееся систематическое знание видов потенциальных и реальных угроз экономической безопасности организации при ответе на вопросы тестирования, зачета и экзамена	Т (Раздел 1 тема 3 вопрос 1-2; Раздел 2 тема 2 вопрос 1-2; Раздел 3 тема 4 вопрос 1-2; Раздел 4 тема 1 вопрос 2), З (вопросы 18-20, 33-38, 64-67), Э (вопросы 4-12, 53-54)
У: применять 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 лабораторных, 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 лабораторных, практико-ориентированных и практических заданий	ЛЗ (Раздел 1 ЛЗ 2); ПЗ (Раздел 4 ПЗ2 задание 2); ПОЗЭ (раздел 3 задание 4) ПОЗЗ (раздел 1 задание 4-5)

В: привлечения лиц, оказывающих содействие органам внутренних дел для решения профессиональных задач	владеет навыками привлечения лиц, оказывающих содействие органам внутренних дел для оценки потенциальных и реальных угроз экономической безопасности организации при выполнении лабораторных, практико-ориентированных и практических заданий	сформировавшееся систематическое владение навыками привлечения лиц, оказывающих содействие органам внутренних дел для оценки потенциальных и реальных угроз экономической безопасности организации при выполнении лабораторных, практико-ориентированных и практических заданий	ЛЗ (Раздел 1 ЛЗ1); ПЗ (Раздел 3 ПЗ4); ПОЗЭ (раздел 4 задание 4) ПОЗЗ (раздел 2 задание 4)

Т – тест, ПЗ – практические задания, ЛЗ – лабораторные задания, ПОЗЗ - практико-ориентированные задания к зачету, ПОЗЭ - практико-ориентированные задания к экзамену, *Э – вопросы к экзамену, З- вопросы к зачету.*

1.2 Шкалы оценивания:

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

- 84-100 баллов (оценка «отлично»);
- 67-83 баллов (оценка «хорошо»);
- 50-66 баллов (оценка удовлетворительно);
- 0-49 баллов (оценка неудовлетворительно).

- 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

4 семестр

Вопросы к зачету

1. Понятие информации, защиты информации, информационной системы, информационной безопасности.
2. Цель защиты информации.
3. Базовые свойства информации: конфиденциальность, целостность, доступность.
4. Нормативно-правовая база функционирования систем защиты информации.
5. Российское законодательство по защите информационных технологий.
6. Правовая защита программного обеспечения авторским правом.
7. Компьютерные преступления и особенности их расследования.
8. Правовая защита информации.
9. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя.
10. Неформальная модель нарушителя.
11. Причины несанкционированного доступа к информации.
12. Последствия несанкционированного доступа к информации.
13. Несанкционированный доступ к информации (НСД).
14. Идентификация. Аутентификация. Выбор паролей.
15. Административная защита информации.
16. Понятие угрозы, классификация угроз.
17. Понятие уязвимости, атаки на компьютерную систему.
18. Понятие риска.
19. Виды утечки информации в юриспруденции.
20. Понятие канала утечки информации, основные каналы утечки информации.
21. Классификация злоумышленников.
22. Уязвимость компьютерных систем.
23. Технологии организации работы с информацией в среде Windows.
24. Поиск, сохранение информации, проверка на вирусы.
25. Понятие ценности информации.
26. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.
27. Способы защиты информации на ПК.
28. Вирусы, антивирусные программы.
29. Административная защита информации.
30. Особенности парольных систем, основные типы угроз безопасности парольных систем.
31. Требования к выбору и использованию паролей.
32. Архиваторы. Архивы. Методы сжатия архиваторов.
33. Сегментирование.
34. Возможности ОС по созданию учетной записи пользователя с ограниченными правами.
35. Порядок удаления ограниченной учетной записи.
36. Защита электронной почты.

37. Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма.
38. Принципы функционирования криптографической системы.
39. Классификация криптосистем.
40. Процесс шифрования текста с помощью таблицы Вижинера.
41. Расшифровка текста с помощью таблицы Вижинера.
42. Понятие криптоанализа, криптоаналитической атаки.
43. Основные типы криптоаналитических атак, криптостойкость шифра.
44. Требования к шифрам, используемым для криптографической защиты информации.
45. Метод встречи в середине атаки.
46. Вероятностный метод криптоанализа.
47. Анализ возможности возникновения коллизии.
48. Особенности использования вычислительной техники в криптографии.
49. Принцип функционирования симметричных криптосистем.
50. Функциональная схема взаимодействия участников симметричного криптографического обмена.
51. Недостатки симметричных криптосистем.
52. Основные виды симметричных шифров.
53. Система шифрования Цезаря.
54. Шифры перестановки.
55. Шифр Гронсфельда.
56. Шифры многоалфавитной замены.
57. Принцип функционирования асимметричных криптосистем. Функциональная схема взаимодействия участников асимметричного криптографического обмена.
58. Достоинства и недостатки асимметричных криптосистем.
59. Реализация двустороннего обмена ключевой информацией.
60. Понятие и назначение центра распределения ключей.
61. Требования Диффи и Хеллмана.
62. Алгоритм шифрования RSA.
63. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.
64. Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП).
65. Целостность передаваемых данных.
66. Авторство сообщений. Основные математические соотношения, используемые в алгоритме RSA.
67. Технология взлома шифра методом полного перебора.

Типовые практико-ориентированные задания к зачету

Раздел 1 «Общие вопросы информационной безопасности».

1.Выполнить установку антивирусной программы.
2.Создать учетную запись пользователя с ограниченными правами.
3.Выполнить защиту электронной почты.
4. Выполнить сегментирование.
5.Выполнить установку паролей.
6. Выполнить удаление ограниченной учетной записи.

Раздел 2. «Методы и средства криптографической защиты».

1.С помощью алгоритма RSA зашифровать слово ДЕРЕВО (4.9.5). Для реализации алгоритма использовать числа p=19, q=29.
2.С помощью алгоритма RSA зашифровать слово ОСЕНЬ (2. 6.4). Для реализации алгоритма использовать числа p=17, q=29.
3.С помощью алгоритма RSA зашифровать слово СОЛНЦЕ (5. 6. 3. 1). Для реализации алгоритма использовать числа p=13, q=31.
4.С помощью алгоритма RSA зашифровать слово УТРО (1.9.2.4). Для реализации алгоритма использовать числа p=11, q=19.
5.С помощью алгоритма RSA зашифровать слово КОШКА (6. 5. 1). Для реализации алгоритма использовать числа p=11, q=13.
6. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ГРУША – ЮЛОУЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

Критерии оценки:

- 50-100 (34-66 за ответ на 2 теоретических вопроса, 16-34 за решение 1-го практико-ориентированного задания) баллов (оценка «зачтено») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированных заданий, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 0-49 (0-33 за ответ на 2 теоретических вопроса, 0-16 за решение 1-го практико-ориентированного задания) баллов (оценка «не зачтено») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированных заданий, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

5 семестр

Вопросы к экзамену

1. Структура системы государственного лицензирования.
2. Порядок проведения лицензирования.
3. Государственные органы по лицензированию.
4. Организационная структура системы государственного лицензирования в области защиты информации.
5. Контроль за деятельностью лицензиатов.
6. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.
7. Федеральные законы в области информации и информационной безопасности.
8. Указы президента РФ и постановления Правительства РФ в области информации и информационной безопасности.
9. Правовые режимы защиты информации.
10. Правовые вопросы защиты информации с использованием технических средств.
11. Система объектов информатизации по требованиям безопасности информации.
12. Виды аттестации объектов информатизации по требованиям безопасности информации.
13. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации.
14. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.
15. Порядок проведения аттестации и контроля.
16. Функции испытательных центров (лабораторий) и заявителей по аттестации объектов информатизации по требованиям безопасности информации.
17. Особенности проведения аттестации помещений по требованиям безопасности информации.
18. Структура системы сертификации.
19. Сущность и содержание сертификации в области защиты информации.
20. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
21. Система сертификации средств защиты информации по требованиям безопасности информации.
22. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
23. Виды и схемы сертификации средств защиты информации.
24. Функции ФСТЭК в области сертификации средств защиты информации.
25. Функции органов сертификации средств защиты информации.
26. Функции испытательных лабораторий (центров).
27. Функции заявителей.
28. Порядок проведения сертификации и контроля.
29. Перечень средств защиты информации, подлежащих сертификации.
30. Категории конфиденциальности защищаемой информации.
31. Категории целостности информации.
32. Категории доступности информации.
33. Определение типа информации.
34. Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач.
35. Определение функционально-отраслевой принадлежности объекта.
36. Определение содержания и местонахождения защищаемых ресурсов на объекте.
37. Характеристика технической укрепленности объекта.
38. Анализ структуры, деятельности и защищаемых ресурсов объекта.
39. Категорирование объекта защиты.
40. Правовые основы защиты коммерческой тайны.
41. Виды информации, составляющей коммерческую тайну.
42. Объекты защиты коммерческой тайны.
43. Права и обязанности обладателя коммерческой тайны.
44. Основные угрозы коммерческой тайны.
45. Правовая защита коммерческой тайны.
46. Порядок отнесения информации к коммерческой тайне.
47. Изучение и анализ нормативной базы в области защиты государственной тайны.
48. Анализ правовых методов защиты сведений, составляющих государственную тайну, изучение порядка и сущности допуска к защищаемым сведениям.
49. Содержание договорной работы в области передачи охраняемой информации.
50. Условия наступления ответственности за разглашение коммерческой тайны.
51. Гражданско - правовая ответственность за разглашение коммерческой тайны.
52. Уголовная ответственность за разглашение коммерческой тайны.
53. Дисциплинарная и материальная ответственность за разглашение коммерческой тайны.
54. Административная ответственность за разглашение коммерческой тайны.

Типовые практико-ориентированные задания к экзамену

Раздел 3 «Основные организационно-технические мероприятия по защите информации».

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. Создать учетную запись пользователя с ограниченными правами.

Задание 3. Выполнить защиту электронной почты.

Задание 4. Разработать систему защиту информации в информационной системе на предприятии.

Раздел 4 «Правовые основы защиты государственной тайны и коммерческой тайны».

Задание 1. Центральный банк РФ для анализа экономической ситуации запросил у АО «Тюмень Нефть» информацию о количестве полученной прибыли за прошедший год и о прогнозах объёма 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 2 . 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 3. 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 4 . 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 проведении контртеррористической операции по ликвидации бандформирования;

– сведения о размерах золотого запаса и государственных валютных резервах РФ;

– экономические показатели военного завода.

Критерии оценивания:

- 84-100 (56-66 за ответ на 2 теоретических вопроса, 28-34 за решение 1-го практико-ориентированного задания) баллов (оценка «отлично») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (44-56 за ответ на 2 теоретических вопроса, 23-27 за решение 1-го практико-ориентированного задания) (оценка «хорошо») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 (34-44 за ответ на 2 теоретических вопроса, 16-22 за решение 1-го практико-ориентированного задания) баллов (оценка удовлетворительно) - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 (0-33 за ответ на 2 теоретических вопроса, 0-16 за решение 1-го практико-ориентированного задания) баллов (оценка неудовлетворительно) - 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.

4 семестр

Лабораторные задания

1.Тематика лабораторных работ по разделам и темам

Раздел 1 «Общие вопросы информационной безопасности».

Тема 1 «Введение в информационную безопасность».

Лабораторное задание 1 «Нормативно-правовая база функционирования систем защиты информации». Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования с использованием текстового редактора MS Word.

Тема 2 «Санкционированный и несанкционированный доступ».

Лабораторное задание 2 «Несанкционированный доступ к информации (НСД)». Идентификация. Аутентификация. Выбор паролей с использованием текстового редактора MS Word.

Тема 3 «Понятие угрозы, уязвимости, риска».

Лабораторное задание 3 «Технологии организации работы с информацией в среде Windows». Поиск, сохранение информации, проверка на вирусы.

Тема 4 «Ценность информации».

Лабораторное задание 4 «Способы защиты информации на ПК». Вирусы, антивирусные программы с использованием текстового редактора MS Word.

Тема 5 «Парольные системы идентификации и аутентификации пользователей».

Лабораторное задание 5 «Архиваторы». Архивы. Методы сжатия архиваторов. Сегментирование. Возможности ОС по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи.

Раздел 2 «Методы и средства криптографической защиты»

Тема 1. «Принципы криптографической защиты информации».

Лабораторное задание 1 «Процесс шифрования текста с помощью таблицы Вижинера». Расшифровка текста с помощью таблицы Вижинера.

Тема 2 «Элементы криптоанализа».

Лабораторное задание 2 «Метод встречи в середине атаки». Вероятностный метод криптоанализа. Анализ возможности возникновения коллизии.

Тема 3 «Симметричные криптосистемы».

Лабораторное задание 3 «Система шифрования Цезаря». Шифры перестановки.

Тема 4 «Асимметричные криптосистемы».

Лабораторное задание 4 «Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП)». Целостность передаваемых данных. Авторство сообщений с использованием текстового редактора MS Word.

2. Критерии оценки:

Критерий оценки: 72 балльная шкала.

Каждая задача оценивается максимум в 8 баллов.

8 б. – задание выполнено верно;

7-6 б. – при выполнении задания были допущены неточности, не влияющие на результат;

5-3 б. – при выполнении задания были допущены ошибки;

2-1 б. – при выполнении задания были допущены существенные ошибки.

0 б. – задание не выполнено.

5 семестр

Практические задания

1.Тематика практических заданий по разделам и темам

Раздел 3 «Основные организационно-технические мероприятия по защите информации»

Тема 1 «Правовые основы лицензирования в области защиты информации»

Практическое задание 1 «Изучение положений о государственном лицензировании деятельности в области защиты информации». Организационная структура системы государственного лицензирования в области защиты информации. Контроль за деятельностью лицензиатов. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию.

Тема 2 «Аттестация объектов информации».

Практическое задание 2 «Изучение положения по аттестации объектов информатизации по требованиям безопасности информации». Порядок проведения аттестации и контроля.

Тема 3 «Правовые основы сертификации в РФ».

Практическое задание 3 «Изучение положений о сертификации средств защиты информации по требованиям безопасности информации». Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации с использованием текстового редактора MS Word.

Тема 4 «Категорирование защищаемой информации».

Практическое задание 4 «Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач». Определение функционально-отраслевой принадлежности объекта. Определение содержания и местонахождения защищаемых ресурсов на объекте. Построение плана объекта. Определение защищаемых зон на плане. Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты. Построение структурной модели защищаемой информации. Определение категории защищаемого объекта с использованием текстового редактора MS Word.

Раздел 4 «Правовые основы защиты государственной тайны и коммерческой тайны».

Тема 1 «Правовые основы защиты коммерческой тайны».

Практическое задание 1 «Порядок отнесения информации к коммерческой тайне». Изучение и анализ нормативной базы в области защиты государственной тайны. Анализ правовых методов защиты сведений, составляющих государственную тайну, изучение порядка и сущности допуска к защищаемым сведениям.

Тема 2 «Правовое регулирование и защита государственной тайны».

Практическое задание 2 «Государственная тайна». Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.

2. Критерии оценки:

Критерий оценки: 72 балльная шкала.

Каждая задача оценивается максимум в 12 баллов.

12 б. – задание выполнено верно;

11-9 б. – при выполнении задания были допущены неточности, не влияющие на результат;

8-5 б. – при выполнении задания были допущены ошибки;

4-1 б. – при выполнении задания были допущены существенные ошибки.

0 б. – задание не выполнено.

Тесты

1. Банк тестов по разделам и (или) темам

4 семестр

Раздел 1 «Общие вопросы информационной безопасности».

Тема 1 «Введение в информационную безопасность».

1.К правовым методам, обеспечивающим информационную безопасность, относятся:

a) разработка аппаратных средств обеспечения правовых данных

b) разработка и установка во всех компьютерных правовых сетях журналов учета действий

c) разработка и конкретизация правовых нормативных актов обеспечения безопасности

2.Виды информационной безопасности:

a) персональная, корпоративная, государственная

b) клиентская, серверная, сетевая

c)локальная, глобальная, смешанная

3. Основные объекты информационной безопасности:

a) компьютерные сети, базы данных

b) информационные системы, психологическое состояние пользователей

c) бизнес-ориентированные, коммерческие системы

Тема 2 «Санкционированный и несанкционированный доступ».

1.Угроза информационной системе (компьютерной сети) – это:

a) вероятное событие

b) детерминированное (всегда определенное) событие

c) событие, происходящее периодически

2. Наиболее распространены средства воздействия на сеть офиса:

a) слабый трафик, информационный обман, вирусы в интернет

b) вирусы в сети, логические мины (закладки), информационный перехват

c) компьютерные сбои, изменение администрирования, топологии.

Тема 3 «Понятие угрозы, уязвимости, риска».

1. Основными источниками угроз информационной безопасности являются все указанное в списке:

a) хищение жестких дисков, подключение к сети, инсайдерство

b) перехват данных, хищение данных, изменение архитектуры системы

c) хищение данных, подкуп системных администраторов, нарушение регламента работы

2. Угроза информационной системе (компьютерной сети) – это:

a) вероятное событие

b) детерминированное (всегда определенное) событие

c) событие, происходящее периодически

Тема 4 «Ценность информации».

1.Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

a) программные, технические, организационные, технологические

b) серверные, клиентские, спутниковые, наземные

c) личные, корпоративные, социальные, национальные

2. К основным принципам обеспечения информационной безопасности относится:

a) экономической эффективности системы безопасности

b) многоплатформенной реализации системы

c) усиления защищенности всех звеньев системы

Тема 5 «Парольные системы идентификации и аутентификации пользователей».

1. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

a) целостность
b) доступность
c) актуальность

2. Наиболее распространены угрозы информационной безопасности сети:

a) распределенный доступ клиент, отказ оборудования
b) моральный износ сети, инсайдерство
c) сбой (отказ) оборудования, нелегальное копирование данных.

Раздел 2 «Методы и средства криптографической защиты»

Тема 1. «Принципы криптографической защиты информации».

1.Что представляет собой криптографическая система?

a)семейство T преобразований открытого текста, члены его семейства индексируются символом k
b) программу
c)систему

2.Требования, предъявляемые к современным криптографическим системам защиты информации:

a)знание алгоритма шифрования не должно влиять на надежность защиты
b) структурные элементы алгоритма шифрования должны быть неизменными
c)не должно быть простых и легко устанавливаемых зависимостью между ключами
d) последовательно используемыми в процессе шифрования

Тема 2 «Элементы криптоанализа».

1.Цель криптоанализа:

a)определение стойкости алгоритма
b) увеличение количества функций замещения в криптографическом алгоритме
c)уменьшение количества функций подстановок в криптографическом алгоритме
d) определение использованных перестановок

2. Выберите правильное определение термина «криптоанализ»

a)криптоанализ – это наука о преодолении криптографической защиты информации
b) криптоанализ – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи
c)криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия
d) криптоанализ изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации

Тема 3 «Симметричные криптосистемы».

1.Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:

a) 1
b) 2
c) 3

2. Какой алгоритм не используется при симметричном шифровании:

a)поточное шифрование
b) побитовое шифрование
c)блочное шифрование
d) алгоритм Эль-Гамаля

3. Какие из режимов шифрования данных не включает в себя отечественный стандарт симметричного шифрования:

a)режим гаммировани
b) режим простой замены
c)режим обратной связи по шифротексту
d) режим гаммирования с обратной связью

Тема 4 «Асимметричные криптосистемы».

1.Асимметричные алгоритмы шифрования по-другому называются

a) алгоритмами шифрования с открытым ключом
b) симметричными алгоритмами шифрования
c) односторонними алгоритмами шифрования
d) помехоустойчивыми алгоритмами шифрования

2.Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для формирования электронной цифровой подписи?

a)отправитель использует для шифрования открытый ключ получателя, а получатель использует для расшифрования свой закрытый ключ
b) отправитель использует для шифрования закрытый ключ получателя, а получатель использует для расшифрования свой открытый ключ
c)отправитель использует для шифрования свой открытый ключ, а получатель использует для расшифрования закрытый ключ отправителя
d) отправитель использует для шифрования свой закрытый ключ, а получатель использует для расшифрования открытый ключ отправителя

5 семестр

Раздел 3 «Основные организационно-технические мероприятия по защите информации»

Тема 1 «Правовые основы лицензирования в области защиты информации»

1. Какой государственный орган занимается рассмотрением и подготовкой законопроектов по вопросам безопасности государства и граждан?

a) Министерство внутренних дел Российской Федерации
b) Комитет Государственной думы по безопасности
c) Служба внешней разведки Российской Федерации
d) Министерство обороны Российской Федерации

2. Какой орган государственной власти проводит государственную политику и осуществляет государственное управление в области обороны?
a) Министерство внутренних дел Российской Федерации
b) Комитет Государственной думы по безопасности
c) Служба внешней разведки Российской Федерации
d) Министерство обороны Российской Федерации

3. Какой орган исполнительной власти проводит лицензирование деятельности по оказанию услуг в области защиты государственной тайны в части, касающейся противодействия техническим разведкам и/или технической защиты информации?
a)ФСТЭК России
b) ФСБ России
c)МВД России
d) Роскомнадзор

Тема 2 «Аттестация объектов информации».

1. Какой орган государственной власти осуществляет аттестацию объектов информатизации по требованиям безопасности?
a)Роскомнадзор
b) МВД России
c)ФСТЭК России
d) СВР России

2. Расходы за проведение аттестации объекта информатизации по требованиям безопасности возлагаются на:
a)орган по аттестации
b) ФСТЭК
c)заказчика
d) испытательную лабораторию

3. В каких случаях из перечисленных ниже аттестация объекта информатизации является обязательной?
a)техническая защита конфиденциальной информации
b) государственная тайна
c)управление социально значимыми объектами
d) управление экологически опасными объектами
e)ведение секретных переговоров

Тема 3 «Правовые основы сертификации в РФ».

1. Что такое сертификация?
a)подтверждение соответствия продукции или услуг установленным требованиям или стандартам;
b) подтверждение соответствия продукции, но не услуг установленным требованиям или стандартам;
c)подтверждение соответствия услуг, но не продукции установленным требованиям или стандартам.

2. Что такое сертификат?
a)документ, подтверждающий соответствие средства зашиты информации требованиям по безопасности информации;
b) документ, подтверждающий соответствие средства зашиты информации требованиям по хранению информации;
c)документ, подтверждающий соответствие средства зашиты информации требованиям по обработке информации.

Тема 4 «Категорирование защищаемой информации».

1.Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:
a)отнесенные к государственной тайне
b) отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн)
c)отнесенные к информации о прогнозах погоды
d) все верны ответы

2.Разделение информации на категории свободного и ограниченного доступа, причем информации ограниченного доступа подразделяются на:
a)отнесенные к государственной тайне
b) отнесенные к служебной тайне (информации для служебного пользования), персональные данные (и другие виды тайн)
c)отнесенные к информации о прогнозах погоды
d) все верны ответы

Раздел 4 «Правовые основы защиты государственной тайны и коммерческой тайны».

Тема 1 «Правовые основы защиты коммерческой тайны».

1.При передаче документов, содержащих коммерческую тайну, в органы государственной власти и органы местного самоуправления гриф «Коммерческая тайна» или «Конфиденциально» проставляется:
a)в обязательном порядке
b) в желательном порядке
c)в не обязательном порядке

2.Объектом правового режима коммерческой тайны является:
a)только научно-техническая и технологическая (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны

b) только производственная и финансово-экономическая информация (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны

c)научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства — ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны

Тема 2 «Правовое регулирование и защита государственной тайны».

1. Какой орган исполнительной власти наделен полномочием выдавать лицензии на деятельность по созданию средств защиты информации, предназначенные для защиты (сохранения) государственной тайны?

a)ФСТЭК России
b) ФСБ России
c)МВД России
d) Роскомнадзор

2. Государственная тайна — это:

a)защищаемые государственные сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации

b) защищаемые государственные сведения только в области военной и внешнеполитической деятельности, распространение которой может нанести ущерб безопасности Российской Федерации

c)защищаемые государственные сведения только в области экономической и разведывательной деятельности, распространение которой может нанести ущерб безопасности Российской Федерации

3.К носителям сведений, составляющих государственную тайну относятся:

a)материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отражение в виде символов, образов, сигналов, технических решений и процессов

b) материальные объекты, за исключением физических полей, в которых сведения, составляющие государственную тайну, находят свое отражение в виде символов, образов, сигналов, технических решений и процессов

c)нет верного ответа

2. Инструкция по выполнению

Тестовое задание выполняется на отдельном листе. Лист подписывается ФИО, номер группы, номер зачетной книжки, указывается вариант тестового задания. Ниже обучающийся указывает цифрой номер вопроса и рядом ставит номер правильного, на его взгляд, варианта ответа. Тестовое задание содержит 14 вопросов с вариантами ответов. Если обучающийся до сдачи преподавателю тестового задания и листа с ответами, считает, что не правильно ответил на тот или иной вопрос теста, то зачеркивает предыдущий вариант ответа и рядом указывает новый. За ошибку это не считается. Время прохождения тестирования 40 минут. После окончания выполнения тестового задания обучающийся сдает преподавателю вариант тестового задания и лист с ответами.

3. Критерии оценки:

(для каждого семестра)

Критерий оценки: 28 бальная шкала.

27-28 баллов: дано 14 верных ответов
25-26 баллов: дано 13 верных ответов
23-24 баллов: дано 12 верных ответов
21-22 баллов: дано 11 верных ответов
19-20 баллов: дано 10 верных ответов
17-18 баллов: дано 9 верных ответов
15-16 баллов: дано 8 верных ответов
13-14 баллов: дано 7 верных ответов
11-12 баллов: дано 6 верных ответов
9-10 баллов: дано 5 верных ответов
7-8 баллов: дано 4 верных ответов
5-6 баллов: дано 3 верных ответов
3-4 баллов: дано 2 верных ответов
1-2 баллов: дан 1 верный ответ
0 баллов: нет верных ответов

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 и экзамена.

Зачет проводится по окончанию теоретического обучения до начала экзаменационной сессии в соответствии с расписанием. Количество вопросов в задании – 3: два теоретических вопроса и одно практико-ориентированное задание. Объявление результатов производится в день зачета. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 3: два теоретических вопроса и одно практико-ориентированное задание. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия;
- лабораторные занятия.

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

В ходе практических и лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки получения, хранения, переработки информации и работы с компьютером как со средством управления информацией.

При подготовке к практическим и лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме.

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

Вопросы, не рассмотренные на практических и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом тестирования. 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 лабораторному 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.