


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»
Документ подписан простой электронной подписью
Информация о документе
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 04.10.2023 15:46:25
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

УТВЕРЖДАЮ
Начальник отдела лицензирования и
аккредитации

Чаленко К.Н.
« 04 » 10 2023 г.

**Рабочая программа дисциплины
Методы защиты информации в юриспруденции**

Специальность 40.05.03 Судебная экспертиза специализация 40.05.03.04 "Экономические экспертизы"

Для набора 2017, 2018, 2019, 2020 года

Квалификация
Судебный эксперт

КАФЕДРА Информационные технологии и защита информации

Распределение часов дисциплины по семестрам

Семестр (<Курс>. <Семестр на курсе>)	2 (1.2)		Итого	
	18			
Неделя	18			
Вид занятий	уп	рп	уп	рп
Лекции	18	18	18	18
Практические	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

ОСНОВАНИЕ

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

Программу составил(и): к.э.н., доц., Т.Н. Шарыпова

Шарыпова 01.06.2020

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

Ефимова 01.06.2020

Методическим советом направления: д.ю.н., проф., А.Н. Позднышов

Позднышов

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.	Знание основ применения инфокоммуникационных технологий для решения задач профессиональной деятельности, основных терминов, понятий, определения в области информационной безопасности; умение защитить компьютерную информацию от несанкционированного разглашения, обеспечивать правовую защиту компьютерной информации в профессиональной деятельности; владеть навыками самостоятельной работы на компьютере и в компьютерных сетях, способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества.
----	---

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-9: способностью соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

В результате освоения дисциплины обучающийся должен:

Знать:

основы применения инфокоммуникационных технологий для решения задач профессиональной деятельности; основные термины, понятия, определения в области информационной безопасности.

Уметь:

защитить компьютерную информацию от несанкционированного разглашения; обеспечивать правовую защиту компьютерной информации в профессиональной деятельности.

Владеть:

навыками самостоятельной работы на компьютере и в компьютерных сетях; способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
	Раздел 1. Общие вопросы защиты информации в юриспруденции				
1.1	Тема 1.1 «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации». Понятие информации, защиты информации, информационной системы, безопасности автоматизированных систем обработки информации. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность. /Лек/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.2	Тема 1.1 «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации. 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. /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.3	Тема 1.1 «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации». Правовая защита информации /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.4	Тема 1.2. «Санкционированный и несанкционированный доступ». Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации. /Лек/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

1.5	Тема 1.2. «Санкционированный и несанкционированный доступ». Несанкционированный доступ к информации (НСД). Идентификация. Аутентификация. Выбор паролей. /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.6	Тема 1.2. «Санкционированный и несанкционированный доступ». Административная защита информации. /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.7	Тема 1.3. «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/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.8	Тема 1.3. «Понятие угрозы, уязвимости, риска». Технологии организации работы с информацией в среде Windows. Поиск, сохранение информации, проверка на вирусы. /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.9	Тема 1.3. «Понятие угрозы, уязвимости, риска». Уязвимость компьютерных систем. /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.10	Тема 1.4. «Ценность информации». Понятие ценности информации. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации /Лек/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.11	Тема 1.4. «Ценность информации». Способы защиты информации на ПК. Вирусы, антивирусные программы. /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.12	Тема 1.4. «Ценность информации». Административная защита информации. /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.13	Тема 1.5. «Парольные системы идентификации и аутентификации пользователей». Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей. /Лек/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.14	Тема 1.5. «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. /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.15	Тема 1.5. «Парольные системы идентификации и аутентификации пользователей». Защита электронной почты /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
Раздел 2. Методы и средства криптографической защиты					

2.1	Тема 2.1. «Принципы криптографической защиты информации». Понятие криптографии, шифрования и дешифрования, ключа шифрования, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем. /Лек/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.2	Тема 2.1. «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.3	Тема 2.1. «Принципы криптографической защиты информации». Таблица Вижинера. /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.4	Тема 2.2. «Элементы криптоанализа». Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для криптографической защиты информации. /Лек/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.5	Тема 2.2. «Элементы криптоанализа». Метод встречи в середине атаки. Вероятностный метод криптоанализа. Анализ возможности возникновения коллизии. /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.6	Тема 2.2. «Элементы криптоанализа». Особенности использования вычислительной техники в криптографии. /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.7	Тема 2.3. «Симметричные криптосистемы». Принцип функционирования симметричных криптосистем. Функциональная схема взаимодействия участников симметричного криптографического обмена. Недостатки симметричных криптосистем. Основные виды симметричных шифров /Лек/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.8	Тема 2.3. «Симметричные криптосистемы». Система шифрования Цезаря. Шифры перестановки /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.9	Тема 2.3. «Симметричные криптосистемы». Шифр Гронсфельда. Шифры многоалфавитной замены. /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.10	Тема 2.4. «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/	2	2	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.11	Тема 2.4. «Асимметричные криптосистемы». Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Целостность передаваемых данных. Авторство сообщений /Пр/	2	4	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

2.12	Тема 2.4. «Асимметричные криптосистемы». Основные математические соотношения, используемые в алгоритме RSA. Технология взлома шифра методом полного перебора. /Ср/	2	6	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.13	/Зачёт/	2	0	ОК-12 ПК-9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

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	Петров, А. А.	Компьютерная безопасность. Криптографические методы защиты	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87998.html неограниченный доступ для зарегистрированных пользователей
Л1.2	Ревнивых, А. В.	Информационная безопасность в организациях: учебное пособие	Новосибирск: Новосибирский государственный университет экономики и управления «НИНХ», 2018	http://www.iprbookshop.ru/95200.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Костин, В. Н.	Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей: учебное пособие	Москва: Издательский Дом МИСиС, 2018	http://www.iprbookshop.ru/98200.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва Берлин: Директ-Медиа, 2020	http://biblioclub.ru/index.php?page=book&id=571485 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, 2013	http://biblioclub.ru/index.php?page=book&id=226269 неограниченный доступ для зарегистрированных пользователей
Л2.2		Информационная безопасность: журнал	Москва: Гротек, 2014	http://biblioclub.ru/index.php?page=book&id=364894 неограниченный доступ для зарегистрированных пользователей
Л2.3	Фомин, Д. В.	Информационная безопасность: учебно-методическое пособие по дисциплине «информационная безопасность» для студентов экономических специальностей заочной формы обучения	Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/77320.html неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.4		Информационная безопасность: журнал	Москва: Гротек, 2014	https://biblioclub.ru/index.php?page=book&id=364894 неограниченный доступ для зарегистрированных пользователей
Л2.5	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2013	https://biblioclub.ru/index.php?page=book&id=226269 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Справочная правовая система "Гарант"

Справочная правовая система "Кодекс"

Справочная правовая система "Консультант Плюс"

Общероссийский математический портал (информационная система)<http://www.mathnet.ru/>

Microsoft Developer Network <https://msdn.microsoft.com/ru-ru/>

5.4. Перечень программного обеспечения

MS Windows

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. Практические 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: основы применения инфокоммуникационных технологий для решения задач профессиональной деятельности	знает основные источники и правила доступа, а также использования информации, в том числе в профессиональных целях, основные методы хранения и обработки информации, а также ее трансляции при подготовке к опросу и зачету	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 опроса и зачета	О (Раздел 1: Тема 1 вопрос 1-6, Тема 2 вопрос 1-6, Тема 3 вопрос 1-6, Тема 4 вопрос 1-2, Тема 5 вопрос 1-3); 3 (вопрос 1-30)
У: защитить компьютерную информацию от несанкционированного разглашения	умеет находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять уровень достоверности источников информации и давать ей критическую оценку для	сформировавшееся систематическое умение находить, систематизировать, обрабатывать и хранить необходимую информацию, в том числе для решения профессиональных задач; определять уровень достоверности источников информации и давать ей	ПЗ (Раздел 1: ПЗ 1 - ПЗ 3); ПОЗЗ (раздел 1 задание 1-3)

	решения практико-ориентированных и практических заданий	критическую оценку при выполнении практико-ориентированных и практических заданий	
В: навыками самостоятельной работы на компьютере и в компьютерных сетях	обладает навыками использования современных информационно-коммуникационных технологий и различных информационных 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 (Раздел 1: ПЗ 4 - ПЗ 5); ПОЗЗ (раздел 2 задание 1-3)
ПК-9 – способностью соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности			
З: основные термины, понятия, определения в области информационной безопасности	поиск и сбор информации по методам реализации политики информационной безопасности в зависимости от типа объекта защиты	полнота собранной информации и соответствие ее типу объекта защиты	О (Раздел 2: Тема 1 вопрос 1-6, Тема 2 вопрос 1-5, Тема 3 вопрос 1-4, Тема 4 вопрос 1-8); 3 (вопрос 31-60)
У: обеспечивать правовую защиту компьютерной информации в профессиональной деятельности	анализ текущего состояния политики безопасности и выявление ее уязвимых мест	соответствие результатов анализа текущему состоянию политики безопасности	ПЗ (Раздел 2: ПЗ 1 - ПЗ 2); ПОЗЗ (раздел 1 задание 4-6)
В: способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества	конфигурирование политики безопасности объекта защиты с учетом комплексного подхода	отсутствие выявленных при первоначальном анализе уязвимостей политики безопасности	ПЗ (Раздел 2: ПЗ 3 - ПЗ 4); ПОЗЗ (раздел задание 4-6)

О – опрос; З – вопросы к зачету; ПЗ – практические задания; ПОЗЗ – проектно-ориентированные задания

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

Вопросы к зачету

1. Информация как объект защиты. Цели защиты информации.
2. Информационная безопасность. Понятие. Аспекты. Угрозы информационной безопасности.
3. Защита информации. Основные термины и определения. Последствия нарушения безопасности.
4. Три базовых аспекта информационной безопасности. Доступность, целостность и конфиденциальность.
5. Угрозы безопасности информации. Классификация угроз.
6. Виды типичных атак на информационную систему.
7. Несанкционированный доступ и утечка информации. Классификация каналов несанкционированного доступа.
8. Методы и средства информационной защиты. Определение и система мер, направленных на обеспечение информационной безопасности.
9. Уровни системы защиты информации.
10. Основные принципы формирования политики информационной безопасности. Организация доступа к информационным ресурсам.
11. Анализ рисков нарушения защиты информации. Ущерб, вероятность атаки, таблица рисков.
12. Программные средства оценки рисков. Этапы осуществления анализа в системе ГРИФ.
13. Правовое обеспечение защиты информации с ограниченным доступом.
14. Информационное право и информационные отношения. Основные положения Конституции России в области защиты информации.
15. Основные понятия и структура Федерального Закона Российской Федерации «Об информации, информатизации и защите информации».
16. Режимные ограничения на доступ к информационным ресурсам. Задачи, решаемые при ограничении доступа.

17. Классификация информации с ограниченным доступом. Государственная, коммерческая и банковская тайны.
18. Преступления в сфере компьютерной безопасности. Положения ст. ст. 272, 273 и 274 УК РФ.
19. Организационные (неформальные) методы защиты информации, особенности их использования.
20. Принципы организации работ по защите информации. Перечень организационных мер.
21. Компьютерные вирусы: основные понятия.
22. Файловые вирусы и схемы их функционирования.
23. Полиморфные вирусы и схемы их функционирования.
24. Пути проникновения вирусов в компьютер.
25. Механизм распределения вирусных программ.
26. Способы несанкционированного доступа к информации.
27. Аутентификация пользователей на основе паролей и модели «рукопожатия».
28. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью.
29. Аутентификация пользователей при удаленном доступе.
30. Физические средства охраны объектов информатизации.
31. Возможные воздействия при физическом доступе.
32. Предотвращение утечки информации за счет побочных электромагнитных излучений и наводок..
33. Основные понятия криптологии.
34. Криптография и криптоанализ.
35. Задачи криптографии. Основные термины и определения.
36. Криптограмма, шифр, ключ.
37. Криптосистемы с секретным ключом.
38. Криптосистемы с секретным ключом.
39. Криптосистемы с открытым ключом.
40. Алгоритм шифрования RSA.
41. Системы аутентификации электронных данных.
42. Загрузочные вирусы и схемы их функционирования.
43. Количество ключей в алгоритмах электронной подписи
44. Используемые алгоритмы при формировании электронной подписи
45. Определение понятия «удостоверяющий центр»
46. Юридическая значимость электронной подписи.
47. Типы однонаправленных функций в RSA.
48. Количество ключей в RSA.
49. Тип зависимости ключей в RSA.
50. Исходная информация для атаки на RSA.
51. Решаемая задача криптоаналитиком при атаке на RSA.
52. Типы однонаправленных функций в ГОСТ Р 34.10-2001.
53. Количество ключей в ГОСТ Р 34.10-2001.
54. Исходная информация для атаки на ГОСТ Р 34.10-2001.

55. Решаемая задача криптоаналитиком при атаке на ГОСТ Р 34.10-2001.
56. Достоинства и недостатки криптоалгоритмов с открытым ключом.
57. Определение понятия «симметричный криптоалгоритм».
58. Количество и размер подблоков разбиения основного блока в ГОСТ 28147-89.
59. Тип алгоритма и длина ключа в DES.
60. Режимы функционирования DES

Типовые практико-ориентированные задания к зачету

Раздел 1 «Общие вопросы защиты информации в юриспруденции».

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 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 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.

Вопросы для опроса

Раздел 1 Общие вопросы защиты информации в юриспруденции Тема 1.1. «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации».

1. Понятие информации.
2. Понятие защиты информации.
3. Понятие информационной системы.
4. Понятие безопасности автоматизированных систем обработки информации.
5. Цель защиты информации.
6. Базовые свойства информации: конфиденциальность, целостность, доступность.

Тема 1.2. «Санкционированный и несанкционированный доступ».

1. Понятие доступа к информации.
2. Понятие субъекта и объекта доступа.
3. Понятие санкционированного и несанкционированного доступа.
4. Понятие нарушителя.
5. Причины несанкционированного доступа к информации.
6. Последствия несанкционированного доступа к информации.

Тема 1.3. «Понятие угрозы, уязвимости, риска».

1. Понятие угрозы, классификация угроз.
2. Понятие уязвимости, атаки на компьютерную систему.
3. Понятие риска.
4. Виды утечки информации в юриспруденции.
5. Понятие канала утечки информации. Основные каналы утечки информации.
6. Классификация злоумышленников.

Тема 1.4. «Ценность информации».

1. Понятие ценности информации.
2. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.

Тема 1.5. «Парольные системы идентификации и аутентификации пользователей».

1. Особенности парольных систем.
2. Основные типы угроз безопасности парольных систем.
3. Требования к выбору и использованию паролей.

Раздел 2. Методы и средства криптографической защиты.

Тема 2.1. «Принципы криптографической защиты информации».

1. Понятие криптографии.
2. Понятие шифрования и дешифрования,
3. Понятие ключа шифрования, шифротекста,
4. Понятие криптоалгоритма.
5. Принципы функционирования криптографической системы.
6. Классификация криптосистем.

Тема 2.2. «Элементы криптоанализа».

1. Понятие криптоанализа,
2. Понятие криптоаналитической атаки.
3. Основные типы криптоаналитических атак.
4. Криптостойкость шифра.
5. Требования к шифрам, используемым для криптографической защиты информации.

Тема 2.3. «Симметричные криптосистемы».

1. Принцип функционирования симметричных криптосистем.
2. Функциональная схема взаимодействия участников симметричного криптографического обмена.
3. Недостатки симметричных криптосистем.
4. Основные виды симметричных шифров.

Тема 2.4. «Асимметричные криптосистемы».

1. Принцип функционирования асимметричных криптосистем.
2. Функциональная схема взаимодействия участников асимметричного криптографического обмена.
3. Достоинства и недостатки асимметричных криптосистем.
4. Реализация двустороннего обмена ключевой информацией.
5. Понятие и назначение центра распределения ключей.
6. Требования Диффи и Хеллмана.
7. Алгоритм шифрования RSA.
8. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.

Критерии оценки:

Критерий оценки: 55 бальная шкала.

Каждый вопроса оценивается максимум в 11 баллов.

Во время опроса обучаемому задаются 5 вопросов.

За один ответ обучаемый получает:

11 б. – за правильный ответ;

10 б. – 8 б. – при ответе были допущены неточности, не влияющие на результат;

7 б. - 4 б. – при ответе были допущены ошибки;

3 - 1 б. – при ответе были допущены существенные ошибки.

0 б. – не ответил на вопрос.

Практические задания

1. Тематика практических заданий по разделам и темам

Раздел 1 Общие вопросы защиты информации в юриспруденции

Тема 1. «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации».

Практическое задание 1 «Нормативно-правовая база функционирования систем защиты информации». Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и их особенности.

Тема 1.2. «Санкционированный и несанкционированный доступ».

Практическое задание 2 «Несанкционированный доступ к информации (НСД)». Идентификация. Аутентификация. Выбор паролей.

Тема 1.3. «Понятие угрозы, уязвимости, риска».

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

Тема 1.4. «Ценность информации».

Практическое задание 4 «Способы защиты информации на ПК». Вирусы, антивирусные программы.

Тема 1.5. «Парольные системы идентификации и аутентификации пользователей».

Практическое 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 2.1. «Принципы криптографической защиты информации».

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

Тема 2.2. «Элементы криптоанализа».

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

Тема 2.3. «Симметричные криптосистемы».

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

Тема 2.4. «Асимметричные криптосистемы».

Практическое задание 2. «Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП)». Целостность передаваемых данных. Авторство сообщений.

3. Критерии оценки:

Критерий оценки: 45 бальная шкала.

Каждое задание оценивается максимум в 5 баллов.

5 б. – задание выполнено верно;

4 б. – при выполнении задания были допущены неточности, не влияющие на результат;

3 б. – при выполнении задания были допущены ошибки;

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

0 б. – задание не выполнено.

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 – 3.

Результаты аттестации заносятся в экзаменационную 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.

В ходе лекционных занятий рассматриваются методы защиты информации, применяемые в юридической деятельности, 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 комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем.

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

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.