

ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОРДОВСКИЙ ГУМАНИТАРНЫЙ ИНСТИТУТ»
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА ТЕОРИИ И ИСТОРИИ ГОСУДАРСТВА И ПРАВА

УТВЕРЖДЕНО

на Научно-методическом совете
протокол № 1 от 29 августа 2017 г.

Председатель  Л.А. Коханец

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(2015 год поступления)

Направление подготовки

38.03.01 «Экономика»

Профиль подготовки

«Бухгалтерский учет, анализ и аудит»

Квалификация выпускника

Бакалавр

Форма обучения

очная, заочная

Саранск 2017 г.

1 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, ОБЕСПЕЧИВАЮЩИЕ ДОСТИЖЕНИЕ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель изучения дисциплины.

Целью изучения дисциплины «Информационная безопасность» является формирование знаний, умений и навыков решения стандартных задач профессиональной деятельности по сохранности информационных ресурсов с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

1.2. Задачи освоения дисциплины

Задачами освоения дисциплины «Информационная безопасность» являются:

- изучение основных направлений деятельности по обеспечению информационной безопасности и защите информации;
- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности
- усвоение сущности и значение информации в развитии современного информационного общества;
- формирование способности понимать, сознать опасности и угрозы, возникающие в информационном процессе, соблюдать основные требования информационной безопасности.

1.3. Планируемые результаты обучения по дисциплине – перечень формируемых компетенций

Изучение дисциплины обеспечивает овладение следующими компетенциями:

способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1).

способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-8)

В результате освоения дисциплины обучающийся должен

знать: правовые основы защиты информации, сущность информационной безопасности; виды угроз, методы и основные требования обеспечения информационной безопасности; технологии защиты информации и алгоритмы традиционных методов шифрования данных.

уметь: выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации; применять действующую законодательную базу в области информационной безопасности и стандартные средства защиты информации, использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии;

владеть: навыками обеспечения информационной безопасности предприятия на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения информационной безопасности; а также методами и средствами технической защиты информации.

2.МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ:

В соответствии с ФГОС ВО дисциплина Б1.В.04 «Информационная безопасность» отнесена к вариативной части блока 1 «Дисциплины» образовательной программы высшего образования - программы бакалавриата 38.03.01 «Экономика», профиль «Бухгалтерский учет, анализ и аудит».

Дисциплина логически взаимосвязана с дисциплинами: «Методы оптимальных решений», «Информационные системы в экономике».

Освоение компетенций в процессе изучения дисциплины способствует формированию знаний, умений и навыков, позволяющих осуществлять эффективную работу по следующим видам профессиональной деятельности: аналитическая, научно-исследовательская.

3. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

Дисциплина изучается:

- очная форма обучения – 4 семестр;
- заочная форма обучения – 3 семестр.

Вид промежуточной аттестации: экзамен

Объем дисциплины по видам учебных занятий и учебной работы

Виды учебных занятий и учебной работы	Всего часов	
	Очная форма	Заочная форма
Общее количество часов	144	144
<i>Контактная работа (всего), в том числе:</i>	58	14
Аудиторные занятия (всего)	56	12
Лекции	18	4
Практические, семинарские занятия	38	8
<i>Индивидуальные консультации</i>	1	1
<i>Групповые консультации</i>	1	1
<i>Самостоятельная работа</i>	59	121
<i>Промежуточная аттестация (контроль)</i>	27	9

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

4.1. Темы (разделы) с указанием отведенного на них количества академических часов и видов учебных занятий

№ п/п	Темы (разделы) дисциплины	Виды учебных занятий, час.								Коды компетенций	Активные и интерактивные формы занятий	Оценочные материалы
		Лекции		Практическое, семинарские занятия		Самостоятельная работа		Всего				
		Очная форма	Заочная форма	Очная форма	Заочная форма	Очная форма	Заочная форма	Очная форма	Заочная форма			
1.	Информационная безопасность как составляющая общественной безопасности	2	1	4	1	8	15	14	17	ОПК-1 ПК-8		опрос тестирование
2.	Виды и особенности угроз информационной безопасности	2	1	6	1	8	16	16	18	ОПК-1 ПК-8		опрос доклад
3.	Правовые методы обеспечения информационной безопасности	2		6	1	9	18	17	19	ОПК-1 ПК-8		опрос контрольная работа
4.	Организационные основы защиты информации	2		6	1	9	18	17	19	ОПК-1 ПК-8	коллоквиум	Опрос, задачи тестирование коллоквиум
5.	Электронный документооборот и электронная подпись	2		4	1	9	18	15	19	ОПК-1 ПК-8	дискуссия	опрос дискуссия
6	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	4	1	6	1	9	18	19	20	ОПК-1 ПК-8	дискуссия	опрос дискуссия

7.	Правовая характеристика преступлений против информационной безопасности по законодательству Российской Федерации	4	1	6	2	7	18	17	21	ОПК-1 ПК-8		опрос доклад итоговое тестирование
	<i>Индивидуальные консультации</i>							1	1			
	<i>Групповые консультации</i>							1	1			
	Вид (виды) промежуточной аттестации: (экзамен)							27	9	ОПК-1 ПК-8		
Всего:		18	4	38	8	59	121	144	144	2		

4.2. Содержание дисциплины, структурированное по темам (разделам)

Тема 1. Информационная безопасность как составляющая общественной безопасности

1. Понятие информационной безопасности как системы общественных отношений и объекта правовой охраны
2. Нормативно-правовые аспекты обеспечения информационной безопасности и её правовой защиты
3. Доктрина информационной безопасности Российской Федерации и Стратегия национальной безопасности Российской Федерации до 2020 года.
4. Информационные ресурсы

Понятие безопасности. Место информационной безопасности в системе национальной безопасности РФ. Информационное общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Место, цели и задачи информационной безопасности в бизнесе. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения. Соотношение понятий информационной безопасности и безопасности информации. Взаимосвязь понятий информационной безопасности и защиты информации. Концепция защиты информации. Понятие и цели защиты информации, формирование и эволюция понятия. Обеспечивающий технологический аспект защиты информации.

Концепция национальной безопасности РФ. Доктрина информационной безопасности РФ. Жизненно важные интересы личности, общества и государства в информационной сфере. Основные задачи в области обеспечения информационной безопасности. Международные договоры, доктрины в области информационной безопасности. Информационная безопасность как институт информационного права. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг. Законодательство о безопасности и защите информации, его структура и содержание. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание. Безопасность функционирования предпринимательской структуры. Основные задачи и уровни реализации информационной безопасности.

Понятие информационных ресурсов. Информационные ресурсы и информационные системы. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. Правовое двуединство документированных информационных ресурсов. Ценность и полезность информации. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации. Взаимосвязь критериев ценности и необходимости обеспечения безопасности информации. Понятие уязвимости информации. Типовые классификационные группы

ценной предпринимательской информации. Информационные ресурсы государственные и негосударственные. Классификация информационных продуктов и услуг. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования.

Ключевые термины и понятия: информационная безопасность, Информационные ресурсы, ценность и полезность информации, концепция национальной безопасности РФ. доктрина информационной безопасности

Задания для практического занятия

1. Понятие информационной безопасности как системы общественных отношений и объекта правовой охраны.
2. Цели, задачи, направления исследования и практической реализации информационной безопасности.
3. Понятие и цели защиты информации, формирование и эволюция понятия
4. Нормативно-правовые аспекты обеспечения информационной безопасности и её правовой защиты
- 5 Доктрина информационной безопасности Российской Федерации и Стратегия национальной безопасности Российской Федерации до 2020 года.
6. Информационные ресурсы

Литература: [1-6]

Тема 2. Виды и особенности угроз информационной безопасности

1. Основные виды каналов утечки информации.
2. Классификация угроз безопасности информационных систем.
3. Виды нарушений информационной безопасности.

Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Правомерные методы получения предпринимательской информации, их состав. Предпосылки и причины утраты информационных ресурсов ограниченного доступа. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Понятие и методы аналитической работы. Виды недобросовестной конкуренции. Промышленный и экономический шпионаж, его сущность, история и сфера распространения. Легальные способы получения ценной и конфиденциальной информации, их состав. Нелегальные (противоправные, незаконные) способы получения ценной и конфиденциальной информации, их состав. Понятия злоумышленника, постороннего и случайного лица.

Понятие и классификация источников конфиденциальной информации. Характеристика каждого источника. Классификация каналов объективного распространения конфиденциальной информации. Характеристика каждого канала. Уязвимость информации. Интерес к информации как предпосылка возникновения угрозы. Понятие угрозы (опасности) информации, виды угроз. Риск угрозы и механизм реализации угрозы. Понятие несанкционированного канала утраты конфиденциальной информации. Случайные и преднамеренные условия возникновения этого канала. Поиск или формирование такого канала злоумышленником. Последствия образования канала несанкционированного доступа к информации: утрата носителя и конфиденциальности информации, разрушение информации, ее кража, модификация, подмена, фальсификация и др. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной

информации. Характеристика каждого канала. Классификация технических каналов утечки конфиденциальной информации. Характеристика каждого канала. Комплексность использования организационных и технических каналов. Особенности структуры каналов распространения информации в компьютерах, локальных сетях, оргтехнике и средствах связи.

Назначение и классификация технических средств промышленного шпионажа. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений.

Ключевые термины и понятия: угроза информационной безопасности, разглашение и утечка информации, промышленный и экономический шпионаж, нелегальные способы получения ценной и конфиденциальной информации, злоумышленник, модификация.

Задания для практического занятия

1. Понятие «угроза информационной безопасности» и ее классификация.
2. Понятие и классификация источников конфиденциальной информации.
3. Классификация каналов объективного распространения конфиденциальной информации.
4. Утрата конфиденциальной информации.
5. Назначение и классификация технических средств промышленного шпионажа.
6. Каналы несанкционированного доступа к информации
7. Технические каналы утечки информации
8. Представить схематически и раскрыть электрические, параметрические и электромагнитные каналы утечки информации
9. Привести пример наиболее частых и опасных угроз нарушения доступности информации.
10. Основные угрозы нарушения целостности информации
11. Основные угрозы нарушения конфиденциальности информации. Перехват данных.
12. Раскрыть алгоритмы вызова программ в ОС MS DOS, а также принципы действия атак переполнения буфера ("buffer-overflow"). Реализация на практике модели атаки переполнения буфера в ОС MS DOS.
13. Применение основ информационной безопасности для нахождения путей противодействия угрозе.
14. Объясните понятие аудита в контексте безопасности вычислительных систем.
15. С помощью какого механизма ОС MS-DOS поддерживает одновременную работу нескольких программ?
16. Как реализовать перехват прерывания средствами языка Си?
17. В чем заключается задача аудита клавиатуры?
18. Как реализовать аудит клавиатуры в ОС MS-DOS?
19. Какие проблемы возникают при записи информации в файл аудита?
20. Для чего необходима аутентификация пользователя?
21. Какие методы обработки данных аудита клавиатуры Вы знаете?
22. В чем заключается метод анализа командной строки в ОС MS-DOS?

Литература: [1-6]

Тема 3. Правовые методы обеспечения информационной безопасности

1. Характеристика информации, как объекта обеспечения безопасности в Российской

Федерации

2. Правовое регулирование открытых информационных ресурсов
3. Правовая защита информационных ресурсов ограниченного доступа
4. Защита информации институтом тайны в РФ
5. Конфиденциальная информация. Персональные данные.

Правовое регулирование открытых информационных ресурсов

Защита информации институтом интеллектуальной собственности. Информационный характер интеллектуальной и материальной собственности. Охрана результатов творческой деятельности. Объекты интеллектуальной собственности. Промышленная собственность. Промышленные образцы. Информация о происхождении товара. Собственность на результаты творческого труда. Российский и зарубежный опыт охраны интеллектуальной собственности. Международные правовые акты. Реализация интеллектуальной собственности на документированную информацию. Характеристика норм патентного права. Характеристика норм авторского права и смежных прав. Торговый знак, знак обслуживания, торговая марка, фирменное наименование, эмблема предприятия. Страхование ценной информации. Законодательные акты, охраняющие вещную собственность на документированную информацию. Правовая защита субъектов в области массовой информации, обеспечение гарантий свободы массовой информации. Организация деятельности средств массовой информации. Отношения средств массовой информации с гражданами и организациями. Ответственность за нарушение законодательства о средствах массовой информации.

Правовая защита информационных ресурсов ограниченного доступа

Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в дореволюционной России и зарубежных странах. Институт тайн в законодательстве Российской Федерации. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области государственной тайны. Отнесение сведений к государственной тайне и их засекречивание. Распоряжение сведениями, составляющими государственную тайну. Рассекречивание сведений и их носителей. Защита государственной тайны. Предпринимательская (коммерческая) тайна как форма защиты ценной деловой и производственной предпринимательской информации. Производственная тайна. Служебная тайна. Профессиональная тайна. Банковская тайна. Тайны личная и семейная. Понятия - "фирменные секреты", "технологические секреты (ноу-хау)", "научные секреты (ноу-ноу)". Документированная информация (документы) секретная и несекретная. Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа. Правовые и технологические аспекты присвоения информации категории конфиденциальной. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной. Понятие конфиденциального документа, его особенности. Общая классификация конфиденциальных документов. Сроки (период) конфиденциальности. Деление документов на документы кратковременного и длительного периода конфиденциальности. Конфиденциальность информации в вычислительных системах и сетях.

Ключевые термины и понятия: информационные ресурсы, защита информации, конфиденциальность, засекречивание, государственная тайна, документированная информация.

Задания для практического занятия

1. Характеристика информации, как объекта обеспечения безопасности в Российской Федерации

2. Правовое регулирование открытых информационных ресурсов
3. Правовая защита информационных ресурсов ограниченного доступа
4. Защита информации институтом тайны в РФ
5. Конфиденциальная информация. Персональные данные.

Литература: [1-6]

Тема 4. Организационные основы защиты информации

1. Основные направления, принципы и условия организационной защиты безопасности
2. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия
3. Методологические основы системы безопасности предприятия (фирмы)
4. Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов
5. Особенности работы с персоналом, владеющим конфиденциальной информацией. Доступ персонала к конфиденциальным сведениям, документам и базам данных
6. Защищенный документооборот. Принципы учета конфиденциальных документов.

Основные направления и этапы работ по созданию комплексной системы безопасности предприятия

Аналитическая работа по выявлению каналов несанкционированного доступа к информации. Аналитическая работа с источником конфиденциальной информации. Аналитическая работа с источником угрозы конфиденциальной информации.

Понятие, цели и задачи системы защиты конфиденциальной информации. Принципы построения системы, ее технологичность, иерархичность и факторы эффективности. Принцип разграничения доступа. Принцип регламентации состава защищаемой информации. Принцип персональной ответственности. Принцип коллегиальности контроля. Принципы надежности и превентивности. Принцип эволюции структуры системы в условиях реальных угроз информации. Обязательная совокупность простейших (несистемных) методов и средств защиты конфиденциальной предпринимательской информации. Преимущества и недостатки. Компьютерные технологии и формирование основ системы защиты информации. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях. Комплексность системы защиты. Структура комплексной системы защиты информации (КСЗИ). Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны. Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом предпринимательской структуры и видами угроз. Система защиты информации в малом бизнесе. Стоимость системы и критерии выбора системы. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Методологические основы системы безопасности предприятия (фирмы)

Разработка и ведение перечня сведений, составляющих предпринимательскую тайну. Цели и задачи перечня сведений, составляющих предпринимательскую тайну. Состав сведений, которые не могут быть тайной. Место перечня в системе защиты информации. Классификация ценной информации в предпринимательских структурах различного типа. Принципы определения состава ценных сведений, подлежащих защите в конкретной фирме. Перечни инвентарные и матричные. Структура перечней различных

типов. Перечни списочные и проблемно-ориентированные. Организационные формы составления и ведения перечней. Содержание процедуры разработки перечня. Существующие методики сбора, анализа и обобщения сведений. Место маркетингового исследования в процедуре разработки перечня. Разграничение уровня конфиденциальности сведений, определение срока конфиденциальности, регламентация места документирования, использования и хранения, состава сотрудников, которым эти сведения необходимы для работы.

Назначение нормативно-методических материалов по регламентации системы защиты информации. Регламентация права предпринимательской структуры на защиту своей тайны. Регламентация структуры и содержания комплексной системы защиты информации фирмы. Регламентация технологии защиты информации от потенциальных и реальных угроз. Регламентация технологии обработки, движения и хранения конфиденциальных документов на традиционных и технических носителях. Регламентация технологии работы персонала фирмы с документами, вычислительной и организационной техникой, средствами связи. Регламентация работы с персоналом. Регламентация системы охраны фирмы. Регламентация защиты информации в экстремальных ситуациях. Состав методических указаний, правил, памяток, схем и иных наглядных пособий.

Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов

Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности. Задачи службы безопасности, основные функции. Руководство и подчиненность. Типовая структура службы безопасности. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации. Задачи и функции аналитического подразделения. Задачи и функции подразделения охраны и пропускного режима. Задачи и функции подразделения инженерно-технической защиты информации. Задачи и функции других подразделений. Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе. Профессиональные и психологические требования к сотрудникам службы безопасности. Плановая и контрольная работа в службе безопасности. Назначение и взаимосвязь плановой и контрольной работы службы безопасности. Их место в построении и функционировании комплексной системы защиты информации фирмы. Анализ и оценка надежности и эффективности применяемой системы защиты. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций.

Особенности работы с персоналом, владеющим конфиденциальной информацией. Доступ персонала к конфиденциальным сведениям, документам и базам данных

Защищенный документооборот. Принципы учета конфиденциальных документов.

Ключевые термины и понятия: несанкционированный доступ к информации, структура комплексной системы защиты информации (КСЗИ), информация общего пользования, Инженерно-техническая защита (ИТЗ), служба безопасности.

Задания для практического занятия

1. Основные направления защиты информации
2. Основные направления по созданию комплексной системы безопасности предприятия
3. Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов.

4. Особенности работы с персоналом, владеющим конфиденциальной информацией.
5. Защищенный документооборот
6. Принципы учета конфиденциальных документов.

Литература: [1-6]

Тема 5. Электронный документооборот и электронная подпись

1. Понятие электронного обмена данными и электронного документооборота.
2. Понятие электронного документа и его особенности.
3. Электронная подпись как один из способов защиты информации.

Понятие электронного обмена данными и электронного документооборота. Понятие электронного документа и его особенности.

Электронный документооборот в юридической сфере в форме: электронных доказательств; электронной системы, оценивающей эти доказательства. Электронными доказательствами являются аудио- и видеозаписи, электронные переписки, SMS-сообщения и т. д.

Понятие цифровой подписи. Электронная цифровая подпись как реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Виды электронной подписи: простая, усиленная неквалифицированная, усиленная квалифицированная. Криптографическое обеспечение электронной подписи. Аппаратные и программные средства электронной подписи.

Удостоверяющие центры. Требования к удостоверяющим центрам. Аккредитация удостоверяющих центров.

Ключевые термины и понятия: электронный обмен данными, электронный документооборот, электронный документ, электронная подпись, удостоверяющие центры.

Задания для практического занятия

1. Понятие электронного обмена данными и электронного документооборота.
2. Понятие электронного документа и его особенности.
3. Виды электронной подписи
4. Удостоверяющие центры

Литература: [1-6]

Тема 6. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи

1. Средства защиты информации
2. Программные средства защиты информации.
3. Криптографическое закрытие информации.

Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и

аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Критерии оценки защищённости систем информационной безопасности. Международные критерии. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макро-вирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ.

Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи.

Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.

Ключевые термины и понятия: идентификация, аутентификация, программные средства, протоколирование, аудит, шифр.

Задания для практического занятия

1. Средства защиты информации.
2. Программные средства защиты информации.
3. Характеристика основных видов компьютерных вирусов.
4. Криптографические средства защиты и типы.
5. Режимы шифрования. Особенности шифрования данных в режиме реального времени.
6. Составить «одноразовый шифровальный блокнот», зашифровав в нем информацию объемом 1стр.
7. Зашифровать информацию о рынке ценных бумаг «одноалфавитным методом».
8. Провести шифрование методом перестановки символов информации о валютном рынке

Литература: [1-6]

Тема 7. Правовая характеристика преступлений против информационной безопасности по законодательству Российской Федерации

1. Понятия «компьютерное преступление» и «информационная безопасность».
2. Компьютерные мошенничества
3. Методы защиты информации при использовании компьютерных сетей

Понятия «компьютерное преступление» и «информационная безопасность». Виды компьютерных преступлений. Подделка компьютерной информации. Хищение

компьютерной информации. Несанкционированный доступ и перехват информации. Компьютерные мошенничества. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Способы и методы предупреждения компьютерных преступлений. Методы защиты информации при использовании компьютерных сетей. Метод «интеллектуального перебора паролей».

Ключевые термины и понятия: «компьютерное преступление», «информационная безопасность», компьютерные мошенничества.

Задания для практического занятия

1. Понятие «компьютерное преступление» и ее виды.
2. Компьютерные мошенничества и хакерство.
3. Неправомерный доступ к компьютерной информации по УК РФ
4. Создание, использование и распространение вредоносных компьютерных программ по УК РФ
5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
6. Уголовная ответственность за компьютерные преступления.
7. Компьютерный терроризм.
8. Методы обнаружения и предупреждения преступлений в информационной среде
9. Методы защиты информации при использовании компьютерных сетей.
10. Метод «интеллектуального перебора паролей».

Литература: [1-6]

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1 Задания для самостоятельной работы и учебно-методическое обеспечение

№ п/п	Тема	Вопросы и задания для самостоятельной работы	Учебно-методическое обеспечение	Оценочные материалы
1	Информационная безопасность как составляющая общественной безопасности	1.Понятие информационной безопасности как системы общественных отношений и объекта правовой охраны 2.Нормативно-правовые аспекты обеспечения информационной безопасности и её правовой защиты 3.Информационные ресурсы	Литература по теме из списка в рабочей программе. Официальный интернет-портал правовой информации (адрес доступа: http://pravo.gov.ru/index.html) Общероссийская сеть публичных центров правовой информации (адрес доступа: http://www.pcpi.ru/manage/page/)	опрос тестирование
2	Виды и особенности угроз информационно й безопасности	1.Основные виды каналов утечки информации. 2.Классификация угроз безопасности информационных систем. 3.Виды нарушений информационной безопасности.	Литература по теме из списка в рабочей программе. Официальный интернет-портал правовой информации (адрес доступа: http://pravo.gov.ru/index.html) Общероссийская сеть публичных центров правовой информации (адрес доступа: http://www.pcpi.ru/manage/page/)	опрос доклад
3	Правовые методы обеспечения информационно й безопасности	1.Характеристика информации, как объекта обеспечения безопасности в Российской Федерации 2.Правовое регулирование открытых информационных ресурсов 3.Защита информации институтом тайны в РФ 4.Конфиденциальная информация. Персональные данные.	Литература по теме из списка в рабочей программе. Официальный интернет-портал правовой информации (адрес доступа: http://pravo.gov.ru/index.html) Сервер органов государственной власти "Официальная Россия" (адрес доступа: http://www.gov.ru/)	опрос контрольная работа
4	Организационные основы защиты информации	1.Основные направления, принципы и условия организационной защиты безопасности 2.Методологические основы системы	Литература по теме из списка в рабочей программе. Доктрина информационной безопасности Российской Федерации http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n	опрос задачи тестирование коллоквиум

		безопасности предприятия (фирмы) 2.Защищенный документооборот. Принципы учета конфиденциальных документов.	=28679 Сервер органов государственной власти "Официальная Россия" (адрес доступа: http://www.gov.ru/)	
5	Электронный документооборот и электронная подпись	1. Понятие электронного обмена данными и электронного докумен- тооборота. 2. Понятие электронного документа и его особенности. 3.Электронная подпись как один из способов защиты информации.	Литература по теме из списка в рабочей программе. Общероссийская сеть публичных центров правовой информации (адрес доступа: http://www.pscri.ru/manage/page/) Единый портал электронной подписи (адрес доступа: http://iesp.ru/)	опрос дискуссия
6	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	1.Средства защиты информации 2.Программные средства защиты информации. 3. Криптографическое закрытие информации.	Литература по теме из списка в рабочей программе. Общероссийская сеть публичных центров правовой информации (адрес доступа: http://www.pscri.ru/manage/page/) Официальный интернет-портал правовой информации (адрес доступа: http://pravo.gov.ru/index.html) Информационно-правовой портал «КонсультантПлюс» (адрес доступа: http://www.consultant.ru)	опрос дискуссия
7	Правовая характеристика преступлений против информационно й безопасности по законодательств у Российской федерации	1.Понятия «компьютерное преступление» и «информационная безопасность». 2.Компьютерные мошенничества 3.Методы защиты информации при использовании компьютерных сетей	Литература по теме из списка в рабочей программе. Информационно-правовой портал «КонсультантПлюс» (адрес доступа: http://www.consultant.ru)	опрос доклад итоговое тестирование

5.2 Методические указания для обучающихся по выполнению самостоятельной работы

Самостоятельная работа, предусмотренная по дисциплине, необходима для углубления и закрепления знаний обучающихся, развития мышления, способности анализировать и обобщать факты, и включает в себя следующие виды работ:

1) предварительная подготовка к аудиторным занятиям. Такая подготовка предполагает изучение рабочей программы учебной дисциплины, установление связи с ранее полученными знаниями, выделение наиболее значимых и актуальных проблем, на изучении которых следует обратить особое внимание;

2) самоподготовка после прослушивания лекций, обобщение информации, сообщаемой преподавателем, при необходимости доработка конспектов лекций;

3) выяснение наиболее сложных, непонятных вопросов и их уточнение в дополнительной литературе;

4) подготовка к занятиям, экзамену;

6) самостоятельное ознакомление с электронными материалами, публикуемыми в сети Интернет.

Студенты выполняют задания, самостоятельно обращаясь к учебной, справочной и нормативной литературе. Проверка выполнения заданий осуществляется как на практических занятиях с помощью устных выступлений студентов и их коллективного обсуждения, так и с помощью письменных самостоятельных (контрольных) работ.

При подготовке к занятию необходимо:

– уяснить содержание каждого учебного вопроса;

– изучить рекомендованную литературу;

– ознакомиться с задачами, документами, подлежащими практическому оформлению;

– законспектировать в рабочих тетрадях учебный материал;

– составить примерный план ответов.

Подготовка докладов для выступлений на практических занятиях прививает студентам навыки научной, творческой работы, воспитывает самостоятельность мышления. Выступление с докладом может идти по следующей схеме: выступление – вопросы к выступающему – обсуждение содержания доклада – заключительное слово докладчика – заключение преподавателя.

Самостоятельная работа по подготовке к практическим занятиям предполагает, прежде всего, основательное, детальное изучение теоретических вопросов темы, существа и содержания правовых норм. Поэтому сначала надо дать четкие, определенные ответы на вопросы плана практических занятий. Только после этого можно приступить к решению задач или тестов по темам.

При подготовке к экзамену не стоит пытаться заучивать отрывочно ответы на отдельные вопросы, приведенные в программе курса. Студенту следует изучать каждую тему системно и комплексно, чтобы иметь цельное представление о ее содержании. После надлежащего усвоения содержания всех тем курса целесообразно еще раз обратить внимание на отдельные вопросы, изучение которых требует дополнительных усилий.

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6. 1. Оценочные и методические материалы для проведения текущего контроля успеваемости обучающихся по дисциплине

Оценочные и методические материалы приведены в приложении 1

6.2 Оценочные и методические материалы для проведения промежуточной аттестации обучающихся по дисциплине

Оценочные и методические материалы приведены в приложении 2.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Лекционные занятия по дисциплине ориентированы на получение основных теоретических сведений по дисциплине, уяснение студентами понятия информации, ее сущности в качестве объекта правового регулирования, что позволит более четко осмыслить проблемы современного состояния информационного обеспечения России, исследовать тенденции и перспективы развития законодательства в этой области,

определить цели, задачи, принципы и основные направления информационного обеспечения в современных условиях.

Для подготовки к лекционному занятию необходимо ознакомиться с темой занятия, списком литературы, рекомендуемой по теме, чтобы составить представление о содержании предстоящей лекции.

Практические занятия предназначены для закрепления теоретического материала, изложенного на лекции и получения определенных навыков решения практических задач с использованием компьютерной техники. Для подготовки к практическому занятию необходимо повторить лекционный материал, а также желательно подготовить вопросы для обсуждения в начале практического занятия.

Текущий контроль. В течение семестра студенты выполняют различные формы отчетности, которые являются обязательными для всех студентов. Результаты выполнения этих работ являются основанием для выставления оценок текущего контроля.

В ходе лекционных занятий следует вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Промежуточная аттестация. Для контроля усвоения дисциплины учебным планом предусмотрен экзамен. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач.

8. ИЗДАНИЯ ЭЛЕКТРОННЫХ БИБЛИОТЕЧНЫХ СИСТЕМ: ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

8.1. Нормативные правовые акты

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».
2. Федеральный закон от 06.04.2011 N 63 "Об электронной подписи" // СПС «КонсультантПлюс».
3. Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СПС «КонсультантПлюс».
4. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СПС «КонсультантПлюс».
5. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // СПС «КонсультантПлюс».
6. Информационное сообщение ФСТЭК России от 06.03.2015 N 240/22/879 "О банке данных угроз безопасности информации" http://www.consultant.ru/document/cons_doc_LAW_176456/
7. Доктрина информационной безопасности Российской Федерации <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=28679>

8.2. Основная литература

1. Партыка Т.Л., Попов И.И.. Информационная безопасность: Учебное

пособие. - М.: Форум: НИЦ ИНФРА-М, 2016. - 432 с. Адрес доступа <http://znanium.com/bookread2.php?book=516806>

2. Информационная безопасность и защита информации: Учебное пособие/ под ред. Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. Адрес доступа <http://znanium.com/bookread2.php?book=495249>

3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. Адрес доступа <http://znanium.com/bookread2.php?book=491597>

8.3. Дополнительная литература

4. Ищeyнов В.Я, Мещатунян М.В. Основные положения информационной безопасности: Учебное пособие. - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с. Адрес доступа <http://znanium.com/bookread2.php?book=508381>

5. Кабашов С.Ю. Электронное правительство. Электронный документооборот. Термины и определения: Учебное пособие. - М.: НИЦ ИНФРА-М, 2013. - 320 с. Адрес доступа <http://znanium.com/bookread2.php?book=410730>

6. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. Адрес доступа <http://znanium.com/bookread2.php?book=423927>

9. ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ, НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

9.1. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Сервер органов государственной власти "Официальная Россия" (адрес доступа: <http://www.gov.ru/>)

2. Специализированный сайт по тематике информационной безопасности (адрес доступа: <http://all-ib.ru/>)

3. Институт проблем информационной безопасности (адрес доступа: <http://www.iisi.msu.ru/>)

4. Информационная безопасность (адрес доступа: <http://dorlov.blogspot.ru/>)

5. Сервер компании НИП «Информзащита» (адрес доступа: <http://www.infosec.ru/>)

6. Документы по информационной безопасности (адрес доступа: SecurityPolicy.ru)

7. Журнал "Information Security/Информационная безопасность (адрес доступа: <http://www.itsec.ru/imag/>)

8. Научная электронная библиотека «eLIBRARY.RU» (адрес доступа: <http://elibrary.ru>),

9.2. Профессиональные базы данных и информационно-справочные системы

1. Информационно-правовой портал «КонсультантПлюс» (адрес доступа: <http://www.consultant.ru>)

2. Сайт Информационно-правовой системы «Законодательство России» (адрес доступа: <http://www.pravo.msk.rsnet.ru>)

3. Единый портал электронной подписи (адрес доступа: <http://iecp.ru/>)

10. ЛИЦЕНЗИОННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1. Microsoft Office 2003; Microsoft Office 2010 Standart; Microsoft Office 2010 Professional Plus

2. Microsoft Imagine

3. Eset Nod 32 Antivirus 4

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Занятия лекционного и семинарского типов, выполнение курсовых работ, групповые и индивидуальные консультации, текущий контроль и промежуточная аттестация проводятся в учебных аудиториях.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Института.

Аудитории укомплектованы специализированной мебелью и техническими средствами обучения, компьютерной техникой, видеопроекторами, демонстрационными экранами, интерактивными досками.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации: презентации к темам лекций, слайды.

Для проведения тестирования используются компьютерные классы (201 или 205 аудитории) оснащенные персональными компьютерами с лицензионным программным обеспечением и набор тестовых заданий).

12. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья институт обеспечивает:

- 1) для инвалидов и лиц с ограниченными возможностями здоровья по зрению:
 - размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий;
 - присутствие ассистента, оказывающего обучающемуся необходимую помощь;
 - выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);
- 2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху:
 - надлежащими звуковыми средствами воспроизведение информации;
- 3) для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:
 - возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Категории студентов	Формы
С нарушением слуха	- в печатной форме; - в форме электронного документа;
С нарушением зрения	- в печатной форме увеличенным шрифтом; - в форме электронного документа; - в форме аудиофайла;
С нарушением опорно-двигательного аппарата	- в печатной форме; - в форме электронного документа; - в форме аудиофайла;

Методические указания для обучающихся по освоению дисциплины

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

Оценочные и методические материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности:

– для студентов с ограниченными возможностями здоровья предусмотрены следующие оценочные материалы:

Категории студентов	Виды оценочных материалов	Формы контроля и оценки результатов обучения
С нарушением слуха	тест	преимущественно письменная проверка
С нарушением зрения	собеседование	преимущественно устная проверка (индивидуально)
С нарушением опорно-двигательного аппарата	решение дистанционных тестов, контрольные вопросы	организация контроля с помощью электронной образовательной среды, проверка письменной работы

– студентам с ограниченными возможностями здоровья увеличивается время на подготовку ответов к зачёту (экзамену), разрешается готовить ответы с использованием дистанционных образовательных технологий.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности:

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены институтом или могут использоваться собственные технические средства;

– процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Категории студентов	Формы
С нарушением слуха	- в печатной форме; - в форме электронного документа;

С нарушением зрения	- в печатной форме увеличенным шрифтом; - в форме электронного документа; - в форме аудиофайла;
С нарушением опорно-двигательного аппарата	- в печатной форме; - в форме электронного документа; - в форме аудиофайла;

– перечень может быть конкретизирован в зависимости от контингента обучающихся.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. Инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, устно с использованием услуг сурдопереводчика);

2. Доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

3. Доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

Издания электронных библиотечных систем: перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья предоставляются основная и дополнительная учебная литература в виде электронного документа в электронно-библиотечных системах. А также предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература и специальные технические средства обучения коллективного и индивидуального пользования, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения:

– учебные аудитории для проведения занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – мультимедийное оборудование, специальное оборудование для студентов с нарушениями слуха; источники питания для индивидуальных технических средств;

– учебная аудитория для самостоятельной работы – стандартные рабочие места с персональными компьютерами; рабочее место с персональным компьютером и специальным оборудованием для студентов с нарушениями зрения.

В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, должно быть предусмотрено соответствующее количество мест для обучающихся с учётом ограничений их здоровья.

В учебные аудитории должен быть обеспечен беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья.

Автор-составитель:



О.Е. Шабает

Рецензент:

к.ю.н., зав. кафедрой
правовых дисциплин Мордовского
государственного педагогического
института им. М.Е. Евсевьева



Ю.Е. Паулова

Зав. библиотекой



С.Н. Астайкина

Программа одобрена на заседании кафедры теории и истории государства
и права «29» августа 2017 года, протокол № 1 .

Зав. кафедрой



Е.Ф. Усманова

ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОРДОВСКИЙ ГУМАНИТАРНЫЙ ИНСТИТУТ»

Кафедра теории и истории государства и права

УТВЕРЖДЕНО
на Научно-методическом совете
протокол № 1 от 29 августа 2017 г.

Председатель  Л.А. Коханец

**ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ
ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
38.03.01 «Экономика»

Профиль подготовки
«Бухгалтерский учет, анализ и аудит»

Квалификация выпускника
Бакалавр

Форма обучения
очная, заочная

Саранск 2017

1. ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

№ п/п	Контролируемые разделы (темы) дисциплины	Контролируемая компетенция Код	Оценочные материалы	
			Наименование	Уровень сложности
1	Информационная безопасность как составляющая общественной безопасности	ОПК-1 ПК-8	опрос тестирование	Репродуктивный
2	Виды и особенности угроз информационной безопасности	ОПК-1 ПК-8	опрос доклад	Репродуктивный Реконструктивный
3	Правовые методы обеспечения информационной безопасности	ОПК-1 ПК-8	опрос контрольная работа	Репродуктивный Реконструктивный Творческий
4	Организационные основы защиты информации	ОПК-1 ПК-8	опрос задачи тестирование коллоквиум	Репродуктивный Реконструктивный Творческий
5	Электронный документооборот и электронная подпись	ОПК-1 ПК-8	опрос дискуссия	Репродуктивный Реконструктивный
6	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	ОПК-1 ПК-8	опрос дискуссия	Репродуктивный Реконструктивный
7	Правовая характеристика преступлений против информационной безопасности по законодательству Российской Федерации	ОПК-1 ПК-8	опрос доклад итоговое тестирование	Репродуктивный Реконструктивный Творческий

2. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Вопросы для коллоквиумов

Тема 4. Организационные основы защиты информации

1. Основные направления, принципы и условия организационной защиты безопасности
2. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия
3. Методологические основы системы безопасности предприятия (фирмы)
4. Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов
5. Особенности работы с персоналом, владеющим конфиденциальной информацией.
6. Доступ персонала к конфиденциальным сведениям, документам и базам данных
7. Защищенный документооборот.
8. Принципы учета конфиденциальных документов.

Шкалы и критерии оценки:

- оценка «отлично» (10 баллов) выставляется студенту, если он глубоко и прочно усвоил программный материал, дает полные, последовательные, грамотные и логически выверенные ответы.
- оценка «хорошо» (7 баллов) выставляется студенту, если он знает программный материал, грамотно излагает свои мысли, без существенных неточностей в ответе на вопрос.
- оценка «удовлетворительно» (5 баллов) выставляется студенту, если он усвоил основной материал по теме, при ответе допускаются неточности, недостаточно правильные формулировки.
- оценка «неудовлетворительно» (0 баллов) выставляется студенту, если он не знает программный материал, при ответе возникают ошибки и затруднения.

Перечень вопросов для контроля успеваемости обучающихся в форме опроса

Опрос проводится по вопросам к практическому занятию, представленным в разделе 4.2. «Содержание дисциплины, структурированное по темам (разделам) рабочей программы» по каждой теме.

Шкалы и критерии оценки:

- оценка «отлично» (5 баллов) выставляется студенту, если он четко и логически правильно отвечает на вопросы, обосновывает ответ примерами и убедительно доказывает свою точку зрения;
- оценка «хорошо» (2 балла) выставляется студенту, если он знает материал, грамотно его излагает, но допускает неточности в ответе на вопросы, может привести примеры и обосновать свои выводы;
- оценка «удовлетворительно» (1 балл) выставляется студенту, если он допускает неточности, недостаточно правильные формулировки в изложении материала, испытывает затруднения при ответе на вопросы, не всегда способен подкрепить свои выводы примерами;

- оценка «неудовлетворительно» (0 баллов) выставляется студенту, который не знает программного материала, допускает существенные ошибки при ответе на вопросы, не способен подкрепить свой ответ примером.

Типовые задачи по курсу

По теме 4 «Организационные основы защиты информации»

1. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации. Охарактеризуйте основные принципы системной классификации угроз безопасности информации. Рассмотрите возможности несанкционированного получения информации в следующем случае:

- в рассматриваемой АС возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС;

- в качестве компонентов, являющихся объектами несанкционированных действий, рассматриваются магнитные носители информации (дискеты), видеотерминалы ввода-вывода информации и принтеры;

Каковы, с вашей точки зрения, в этом случае вероятности несанкционированного получения информации?

2. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?

3. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

4. Сравните различные известные вам модели защиты от несанкционированного доступа к информации. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

5. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями? Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным? Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере? Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

6. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности. Дайте определение компьютерного вируса. Приведите примеры и случаев заражения компьютеров вирусами.

7. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков

информации как основных принципов защиты информации от несанкционированного доступа?

8. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием? Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

9. Раскройте основное содержание алгоритма электронной цифровой подписи.

10. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ? Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами? Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

11. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов. Какой, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала. Дайте классификацию источников утечки информации по техническим каналам.

12. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности. Изложите кратко основное содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

13. Проведите анализ защищенности объекта защиты информации. Для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

- 1 виды угроз;
- 2 характер происхождения угроз;
- 3 классы каналов несанкционированного получения информации;
- 4 источники появления угроз;
- 5 причины нарушения целостности информации;

14. Определите возможных нарушителей объекта защиты информации. Классифицируйте их в соответствии с двумя группами: внешние нарушители и внутренние нарушители. Заполните на основе собственных полученных данных таблицу «Типы угроз и возможные внутренние нарушители объекта.»

15. Придумайте, компанию, для которой вы будете разрабатывать нормативное и административно-организационное обеспечение информационной безопасности. Это может быть:

- вымышленная компания;
- компания, где вы работаете;
- компания, по которой планируете выполнять дипломный проект;
- компания, где вы проходили практику;
- компания, описание и данные по которой вы использовали в рамках другого курса;
- Приведите краткое описание компании:
- название, организационно-правовая форма, учредители
- краткая история компании (год основания, основные этапы развития)
- сфера деятельности
- миссия
- количество сотрудников
- организационная структура (представить в виде рисунка)

- способы ведения бизнеса
- основные конкуренты и конкурентная стратегия
- основные поставщики и потребители (клиенты)
- цели компании на ближайшие год (не менее 5 целей), три года (не менее 5 целей), пять лет (не менее 5 целей).

16. На предприятии созданы и используются базы данных различных видов (маркетинговые исследования, данные о предприятиях-смежниках, техническая документация и т.д.). Каким образом можно защитить эти данные исходя из норм российского законодательства? Может ли к корпоративной базе данных применяться правовой режим персональных данных, объектов авторского права, коммерческой тайны?

17. В Word, Excel, Power Point и других программах MS Office есть возможность защиты файлов от несанкционированных изменений. Назовите и раскройте не менее трех вариантов такой защиты

Шкалы и критерии оценки:

Оценка «отлично» (10 баллов) выставляется, если задача решена правильно. студент правильно изложил все варианты решения, аргументировав их, со ссылкой на нормы действующего законодательства

Оценка «хорошо» (7 баллов) выставляется, если частично правильное решение задачи, недостаточная аргументация своего решения, со ссылками на норму закона. Алгоритм решения задачи корректен. Имеются ошибки или неточности в применении норм права.

Оценка «удовлетворительно» (3 балла) выставляется, если рассуждения в процессе решения задачи корректны, но не получен ответ.

Оценка «неудовлетворительно» (0 баллов) выставляется, если задача не решена.

Темы докладов

По теме 2 «. Виды и особенности угроз информационной безопасности»

1. Основные виды каналов утечки информации.
2. Классификация угроз безопасности информационных систем.
3. Виды нарушений информационной безопасности.
4. Утрата конфиденциальной информации.
5. Назначение и классификация технических средств промышленного шпионажа.

По теме 7 «Правовая характеристика преступлений против информационной безопасности по законодательству Российской Федерации»

1. Понятие «компьютерное преступление» и ее виды.
10. Понятие «информационная безопасность»
11. Компьютерные мошенничества
12. Методы защиты информации при использовании компьютерных сетей.
5. Метод «интеллектуального перебора паролей».

Шкалы и критерии оценки:

Оценка «отлично» (5 баллов) выставляется студенту, если содержание доклада соответствует заявленной теме, и всем предъявляемым требованиям, обнаружено

отличное знание и понимание темы, а также умение давать оценку излагаемым фактам, логически последовательно и аргументировано излагать свои мысли. Выводы корректны.

Оценка «хорошо» (2 балла) выставляется студенту в том случае, если доклад содержит недостаточное количество фактов по излагаемой теме, хотя теоретическое знание проблемы присутствует.

Оценка «удовлетворительно» (3 балла) выставляется тогда, когда частично раскрыта тема доклада и наблюдаются пробелы в знании представленного материала.

Оценка «неудовлетворительно» (0 баллов) выставляется, если содержание доклада не соответствует заявленной теме, либо не представлено.

Вопросы для дискуссии

По теме 5 «Электронный документооборот и электронная подпись»

1. Источники правового регулирования электронного документооборота: тенденции международно-правового и национального регулирования
2. Юридические требования к электронному документообороту
3. Проблемы осуществления электронного документооборота в открытых системах

По теме 6 «Программные средства защиты информации в компьютерах, локальных сетях и средствах связи»

1. Программно-технические методы обеспечения информационной безопасности.
2. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации.
3. Криптографические средства защиты.
4. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.

Шкалы и критерии оценки:

- оценка «отлично» (5 баллов) выставляется студенту, если он владеет источниками, оперирует специальными терминами и понятиями, дает полные и аргументированные ответы на поставленные вопросы.

- оценка «хорошо» (4 балла) выставляется студенту, если он понимает проблемы по заявленной теме дискуссии, полно и конкретно отвечает на поставленные вопросы.

- оценка «удовлетворительно» (3 балла) выставляется за недостаточно аргументированные ответы на поставленные вопросы. Студент не принимает активного участия в дискуссии.

- оценка «неудовлетворительно» (0 баллов) выставляется в том случае, когда студент не готов к дискуссии, не принимал участия в работе.

Тестовые задания

По теме 1 «Информационная безопасность как составляющая общественной безопасности»

Задание 1 (укажите один вариант ответа)

Информация, к которой ограничен доступ:

- 1) конфиденциальная;

- 2) противозаконная;
- 3) открытая;
- 4) недоступная.

Задание 2 (укажите один вариант ответа)

Компьютерные системы, в которых обеспечивается безопасность информации:

- 1) защищенные КС;
- 2) небезопасные КС;
- 3) само достаточные КС;
- 4) саморегулирующиеся КС.

Задание 3 (укажите один вариант ответа)

Основной документ, на основе которого проводится политика информационной безопасности:

- 1) программа информационной безопасности;
- 2) регламент информационной безопасности;
- 3) политическая информационная безопасность;
- 4) протекторат.

Задание 4 (укажите один вариант ответа)

Наиболее распространенными являются следующие классы угроз:

- 1) ошибки эксплуатации и изменения режима работы системы;
- 2) непреднамеренные действия;
- 3) продажа нелегального программного обеспечения;
- 4) использование старой техники.

Задание 5 (укажите один вариант ответа)

Программные средства защиты информации:

- 1) технические средства защиты информации;
- 2) средства архивации данных, антивирусные программы;
- 3) источники бесперебойного питания (UPS);
- 4) смешанные средства защиты информации.

Задание 6 (укажите один вариант ответа)

Основной документ информатизации в РФ:

- 1) концепция информатизации общества;
- 2) закон об информатизации общества;
- 3) кодекс информатизации общества;
- 4) программа информатизации общества.

Задание 7 (укажите один вариант ответа)

Конфиденциальной информацией будут:

- 1) условия авторского договора автора и редакции;
- 2) тираж изданной книги автора;
- 3) данные о самолете и местах пассажиров при покупке билета;
- 4) данные об экологической обстановке во время аварии.

Задание 8 (укажите один вариант ответа)

В зависимости от формы представления информация может быть разделена на:

- 1) речевую, документированную и телекоммуникационную;
- 2) мысль, слово и речь;
- 3) цифровая, звуковая и тайная;

4) цифровая, звуковая.

Задание 9 (укажите один вариант ответа)

Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе:

- 1) информационная безопасность;
- 2) защитные технологии;
- 3) заземление;
- 4) конфиденциальность.

Задание 10 (укажите один вариант ответа)

Процессы сбора, обработки, накопления, хранения, поиска и распространения информации относятся к:

- 1) информационным процессам;
- 2) мыслительным процессам;
- 3) машинным процессам;
- 4) микропроцессам.

Задание 11 (укажите один вариант ответа)

Основные предметные направления Защиты Информации:

- 1) охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности;
- 2) охрана золотого фонда страны;
- 3) определение ценности информации;
- 4) усовершенствование скорости передачи информации.

по теме 4 «Организационные основы защиты информации»

1. Какой этап решения проблем защиты информации характеризовался тем, что под этой деятельностью подразумевалось предупреждение несанкционированного получения защищаемой информации?

- 1) Начальный этап.
- 2) Этап развития.
- 3) Этап совершенствования.
- 4) Современный этап.

2. Какой этап решения проблем защиты информации характеризовался формированием на основе аналитико-синтетической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты научно-методологического базиса защиты информации?

- 1) Начальный этап.
- 2) Этап развития.
- 3) Этап совершенствования.
- 4) Современный этап.

3. Порядок и правила определения степени секретности сведений, указания грифа секретности на носителях информации, а также рассекречивания информации или снижения степени ее секретности являются элементами:

- 1) Структурной части системы защиты информации.
- 2) Организационной части системы защиты информации.
- 3) Функциональной части системы защиты информации.
- 4) Архитектурной части системы защиты информации.

4. Система правовых, организационных, технических и иных мер, федеральных органов власти, местного самоуправления, предприятий, организаций и учреждений, направленных на обеспечение безопасности Российской Федерации, сохранения ее государственной, служебной, коммерческой, других видов тайн и сведений ограниченного доступа, информационных ресурсов, систем, технологий и средств их обеспечения, называется:

- 1) Системой информационной безопасности.
- 2) Доктриной информационной безопасности.
- 3) Государственной системой защиты информации.
- 4) Режимом секретности.

5. Какой орган при осуществлении своей деятельности имеет право подготавливать и представлять в установленном порядке Президенту и в Правительство РФ предложения по правовому регулированию вопросов защиты государственной тайны, совершенствованию системы защиты государственной тайны?

- 1) Государственная техническая комиссия при Президенте РФ.
- 2) Межведомственная комиссия по защите государственной тайны.
- 3) Федеральная служба безопасности России.
- 4) Федеральное агентство правительственной связи и информации.

6. Какой орган при осуществлении своей деятельности рассматривает и представляет на утверждение правительству проекты государственных программ по защите информации?

- 1) Федеральное агентство правительственной связи и информации.
- 2) Межведомственная комиссия по защите государственной тайны.
- 3) Федеральная служба безопасности России.
- 4) ФСТЭК РФ.

7. Определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организаций в этой области обеспечивает:

1. Государственная система защиты информации.
2. Система информационной безопасности.
3. Организационно-правовая база защиты информации.
4. Организационно-функциональная система защиты информации.

8. Защита персональных данных, страхование информации и информационных систем осуществляется:

1. Комплексной системой информационной безопасности.
2. Организационно-правовой системой защиты информации.
3. Государственной системой организационно-правового обеспечения информационной безопасности.
4. Организационно-функциональной системой защиты информации.

9. Какой нормативный акт устанавливает порядок обмена между государствами конфиденциальной и массовой информацией?

1. Федеральный закон «Об информации, информационных технологиях и защите информации».
2. Федеральный закон «Об участии в международном информационном обмене».
3. Соглашение между странами СНГ о взаимном обеспечении сохранности межгосударственных секретов.

4. Закон Российской Федерации «О средствах массовой информации».

10. Система защиты информации состоит из двух частей:

1. Теоретической и практической.
2. Социальной и гуманитарной.
3. Общей и специальной.
4. Структурной и функциональной.

11. Поддерживаемые на объекте режим секретности, внутриобъектовый режим и режим охраны, соответствующие степени секретности накапливаемой и используемой на объекте информации являются элементами:

1. Структурной части системы защиты информации.
2. Организационной части системы защиты информации.
3. Архитектурной части системы защиты информации.
4. Функциональной части системы защиты информации.

12. Основным органом, координирующим действия государственных структур по вопросам защиты информации, является:

1. Гостехкомиссия России.
2. Межведомственная комиссия по защите государственной тайны.
3. Федеральная служба безопасности России.
4. Федеральное агентство правительственной связи и информации.

13. Какой орган при осуществлении своей деятельности имеет право подготавливать и представлять в установленном порядке Президенту и в Правительство РФ предложения по порядку определения размеров ущерба, который может быть нанесен безопасности России вследствие несанкционированного распространения секретных сведений или засекречивания информации, находящейся в собственности предприятий?

1. Государственная техническая комиссия при Президенте РФ.
2. Федеральная служба безопасности России.
3. Межведомственная комиссия по защите государственной тайны.
4. Федеральное агентство правительственной связи и информации.

14. Какой орган при осуществлении своей деятельности заслушивает руководителей министерств и ведомств, государственных предприятий и объединений, главных конструкторов по вопросам, связанным с защитой информации?

1. Федеральная служба безопасности России.
2. Межведомственная комиссия по защите государственной тайны.
3. Государственная техническая комиссия при Президенте РФ.
4. Федеральное агентство правительственной связи и информации.

15. Создание полного комплекса нормативно-правовых руководящих и методических документов, регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте обеспечивает:

1. Государственная система защиты информации.
2. Система информационной безопасности.
3. Организационно-правовая база защиты информации.
4. Организационно-функциональная система защиты информации.

Шкалы и критерии оценки:

Оценка «отлично» (5 баллов) выставляется, если правильно сделано 90% тестовых заданий.

Оценка «хорошо» (2 балла) выставляется, если правильно сделано 70% тестовых заданий.
Оценка «удовлетворительно» (1 балл) выставляется, если правильно сделано 50% тестовых заданий.
Оценка «неудовлетворительно» (0 баллов) выставляется, если правильно сделано менее 50% тестовых заданий.

Задания для контрольной работы

По теме 3 «Правовые методы обеспечения информационной безопасности»

Вариант 1

1. Правовая защита информационных ресурсов ограниченного доступа
2. Какие сведения не могут составлять коммерческую тайну?
3. В чем заключается отличие между деятельностью ФСБ и ФСТЭК в сфере нормативно-правового регулирования защиты информации? Обоснуйте ответ.

Вариант 2

1. Какие безотлагательные для решения задачи в информационной сфере определяет Доктрина информационной безопасности РФ?
2. Какие предъявляются требования к информации, составляющей коммерческую тайну? Обоснуйте ответ.
3. «В современных условиях недостаточно «владеть информацией» для выработки грамотного управленческого решения. Оперативное внедрение информационных и информационно-аналитических технологий позволит преодолеть информационный барьер между органами власти и населением и в перспективе создаст условия для перехода от реактивной политики государства к превентивной». Подтвердите или опровергните данное утверждение практическими примерами.

Вариант 3

1. Защита информации институтом интеллектуальной собственности.
2. Защита информации институтом государственной тайны.
3. Что относится к информационным активам организации, и какие информационные активы являются наиболее ценным для организаций, осуществляющих различные виды деятельности (3-4 примера)? Обоснуйте ответ.

Шкалы и критерии оценки:

Оценка «отлично» (10 баллов) выставляется, если на все вопросы даны правильные и точные ответы. Показано безупречное знание базовой терминологии, умение раскрыть и прокомментировать содержание терминов.

Оценка «хорошо» (7 баллов) выставляется, если ответы на вопросы даны в целом правильно, однако неполно. Логика ответов достаточно хорошо выстроена. Пропущен ряд важных деталей или, напротив, в ответе затрагивались посторонние вопросы.

Оценка «удовлетворительно» (5 баллов) выставляется, если до конца не раскрыт ни один вопрос, студент путается в основных базовых понятиях, не в состоянии раскрыть содержание основных категорий, в знаниях имеются существенные пробелы, логика ответов недостаточно хорошо выстроена.

Оценка «неудовлетворительно» (0 баллов) выставляется студенту, который обнаружил существенные пробелы в знаниях основного учебно-программного материала по темам, не смог решить задачу.

3. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Локальные нормативные акты института, регламентирующие процедуры оценивания

1. Положение о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации студентов.
2. Положение о рейтинговой системе оценки знаний студентов.
3. Положение о проведении компьютерного тестирования студентов.
4. Положение о самостоятельной работе студентов.
5. Положение о рабочей программе
6. Положение об оценочных и методических материалах для проведения текущего контроля, промежуточной аттестации и ГИА

Процедура оценивания знаний, умений и навыков обучающихся

В начале изучения дисциплины преподаватель доводит до сведения обучающихся информацию о формах, сроках проведения, шкалах и критериях оценки конкретных заданий; в течение семестра ведет учет текущей успеваемости каждого обучающегося.

Максимальное количество баллов по видам оценочных материалов

	Наименование оценочного материала								Итого
	Доклад	дискуссия	Коллоквиум	Решение задач	Тестирование по темам	Контрольная работа	Опрос, работа на практическом занятии	Итоговое тестирование	
Количество баллов	10	10	10	10	10	10	35	5	100

Обучающийся освобождается от экзамена с оценкой:

- «отлично» – если, имеет не менее 85 баллов;
- «хорошо» – если, имеет от 70 до 84 баллов;
- «удовлетворительно» – если, имеет от 55 до 69 баллов.

Обучающийся, имеющий менее 55 рейтинговых баллов, сдает экзамен по дисциплине.

Обучающийся, желающий получить более высокую оценку, чем оценка полученная в результате учета текущей успеваемости обучающегося в балльно-рейтинговой системе – сдает экзамен.

**ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОРДОВСКИЙ ГУМАНИТАРНЫЙ ИНСТИТУТ»**

Кафедра теории и истории государства и права

УТВЕРЖДЕНО
на Научно-методическом совете
протокол № 1 от 29 августа 2017 г.

Председатель  Л.А. Коханец

**ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
38.03.01 «Экономика»

Профиль подготовки
«Бухгалтерский учет, анализ и аудит»

Квалификация выпускника
Бакалавр

Форма обучения
очная, заочная

Саранск 2017

1. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

1.1. Перечень типовых контрольных вопросов для оценки знаний на экзамене

1. Понятие информационной безопасности как системы общественных отношений и объекта правовой охраны.
2. Цели, задачи, направления исследования и практической реализации информационной безопасности.
3. Понятие и цели защиты информации, формирование и эволюция понятия
4. Нормативно-правовые аспекты обеспечения информационной безопасности и её правовой защиты
5. Доктрина информационной безопасности Российской Федерации и Стратегия национальной безопасности Российской Федерации до 2020 года.
6. Понятие «угроза информационной безопасности» и ее классификация.
7. Понятие и классификация источников конфиденциальной информации.
8. Классификация каналов объективного распространения конфиденциальной информации.
9. Утрата конфиденциальной информации.
10. Назначение и классификация технических средств промышленного шпионажа.
11. Информационная безопасность человека и общества. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
12. Компьютерные преступления. Основные технологии, используемые при совершении компьютерных преступлений.
13. Характеристика информации, как объекта обеспечения безопасности в Российской Федерации
14. Правовое регулирование открытых информационных ресурсов
15. Правовая защита информационных ресурсов ограниченного доступа
16. Защита информации институтом тайны в РФ
17. Конфиденциальная информация. Персональные данные.
18. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.
19. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
20. Реализация методов и средств защиты информации.
21. Средства опознавания и разграничения доступа к информации.
22. Криптография. Симметричные криптосистемы.
23. Криптография. Асимметричные криптосистемы.
24. Обзор и классификация методов шифрования информации.
25. Понятие электронного обмена данными и электронного документооборота.
26. Понятие электронного документа и его особенности.
27. Электронная подпись как один из способов защиты информации.
28. Основные алгоритмы шифрования данных: RSA.
29. Основные алгоритмы шифрования данных: DES.
30. Основные алгоритмы шифрования данных: ГОСТ.
31. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
32. Защита данных в автономном компьютере.
33. Защита данных в вычислительных сетях. Разработка сетевых аспектов политики безопасности.

34. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
35. Показатели оценки достоверности (безошибочности) передачи данных в сетях.
36. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
37. Парольная защита операционных систем. Парольные взломщики.
38. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
39. Структуризация методов обеспечения информационной безопасности. Основные методы реализации угроз информационной безопасности.
40. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
41. Причины, виды и каналы утечки информации.
42. Методы построения защищенных автоматизированных систем.
43. Политика безопасности. Основные типы политики безопасности.
44. Стандарты информационной безопасности.
45. Основные направления, принципы и условия организационной защиты безопасности
46. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия
47. Методологические основы системы безопасности предприятия (фирмы)
48. Основные направления деятельности службы безопасности предприятия (фирмы) по защите информационных ресурсов
49. Особенности работы с персоналом, владеющим конфиденциальной информацией. Доступ персонала к конфиденциальным сведениям, документам и базам данных
50. Защищенный документооборот. Принципы учета конфиденциальных документов.
51. Разрушающие программные воздействия: вирусы и закладки. Антивирусные средства.
52. Психологические аспекты информационной безопасности организации.
53. Понятие «компьютерное преступление» и ее виды.
54. Понятие «информационная безопасность»
55. Компьютерные мошенничества
56. Методы защиты информации при использовании компьютерных сетей. Метод «интеллектуального перебора паролей».

1.2. Типовые контрольные задачи для оценки знаний, умений, навыков или опыта деятельности на экзамене

1. Какие вам известны подходы к классификации угроз безопасности информации? Сравните их между собой с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации. Охарактеризуйте основные принципы системной классификации угроз безопасности информации. Рассмотрите возможности несанкционированного получения информации в следующем случае:

- в рассматриваемой АС возможны нарушители двух категорий: внешние, не имеющие отношения к системе, и внутренние, входящие в состав персонала, обслуживающего АС;

- в качестве компонентов, являющихся объектами несанкционированных действий, рассматриваются магнитные носители информации (дискеты), видеотерминалы ввода-вывода информации и принтеры;

Каковы, с вашей точки зрения, в этом случае вероятности несанкционированного получения информации?

2. В чем, с вашей точки зрения, состоит опасность разработки и применения информационного оружия? Какие необходимо было бы применить меры международного характера в целях предотвращения информационных войн?

3. Представьте следующую ситуацию: министры внутренних дел и экономики имеют одинаковую (наивысшую) форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования экономических преступлений. Каковы, на ваш взгляд, должны быть возможности их доступа к этой информации? Рассмотрите все возможные ситуации и последствия, к которым приведут принимаемые решения по доступу с точки зрения обеспечения безопасности информации.

4. Сравните различные известные вам модели защиты от несанкционированного доступа к информации. Приведите наиболее распространенную на сегодняшний день классификацию средств защиты информации. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств защиты информации?

5. Дайте определения идентификации и аутентификации пользователей. В чем разница между этими понятиями? Назовите основные способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным? Приведите примеры известных вам систем аутентификации, построенных по принципу «пользователь имеет». Что вы можете сказать о преимуществах и недостатках методов аутентификации пользователей пластиковых карт, широко используемых в банковской сфере? Каковы основные характеристики устройств аутентификации? Сравните известные вам устройства по каждой из этих характеристик. Раскройте основные особенности известных вам методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.

6. Охарактеризуйте «вредительские» программы как один из видов угроз информационной безопасности. Дайте определение компьютерного вируса. Приведите примеры и случаев заражения компьютеров вирусами.

7. Раскройте содержание принципов обоснованности доступа и персональной ответственности как основных принципов защиты от несанкционированного доступа. В чем состоит суть принципов достаточной глубины контроля и разграничения потоков информации как основных принципов защиты информации от несанкционированного доступа?

8. Какие методы криптографического закрытия информации вы знаете? В чем разница между шифрованием и кодированием? Расскажите об особенностях симметричных и несимметричных шифров. Попробуйте привести примеры этих способов шифрования. Объясните, почему основными требованиями, предъявляемыми к криптосистемам, являются наличие очень большого числа возможных ключей и равная вероятность их генерации.

9. Раскройте основное содержание алгоритма электронной цифровой подписи.

10. Охарактеризуйте известные вам основные классы антивирусных программ. В чем смысл комплексного применения нескольких программ? Каковы, на ваш взгляд, должны быть основные правила работы с компьютером, предупреждающие возможное заражение его вирусами? Охарактеризуйте перспективные методы защиты компьютеров от программ-вирусов.

11. Дайте определение понятию «технический канал утечки информации». Назовите основные виды технических каналов. Какой, технический канал утечки информации можно отнести к наиболее часто используемым техническими разведками для получения конфиденциальной информации? Раскройте особенности этого канала. Дайте классификацию источников утечки информации по техническим каналам.

12. Опишите систему органов государственного управления Российской Федерации, осуществляющих управление и координацию деятельности в области защиты информации и обеспечения информационной безопасности. Изложите кратко основное

содержание деятельности ФСТЭК России в области обеспечения информационной безопасности.

Шкалы и критерии оценки на экзамене

Оценка «отлично» выставляется студенту, который усвоил программный материал в полном объеме, знает правовые основы защиты информации, виды угроз и методы обеспечения информационной безопасности; основные требования информационной безопасности. Умеет уверенно выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации; применять программно-технические средства защиты и криптографические протоколы, способен использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии. Свободно владеет навыками применения политики безопасности предприятия; навыками работы с программными комплексами защиты информации. Задание выполнено правильно.

Оценки «хорошо» заслуживает студент, который усвоил программный материал, знает правовые основы защиты информации, виды угроз и методы обеспечения информационной безопасности; основные требования информационной безопасности. Умеет с небольшими затруднениями выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации; применять программно-технические средства защиты и криптографические протоколы, использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии.. Владеет навыками применения политики безопасности предприятия; навыками работы с программными комплексами защиты информации. Задание выполнено правильно.

Оценки «удовлетворительно» заслуживает студент, который демонстрирует фрагментарные знания правовых основ защиты информации, виды угроз и методы обеспечения информационной безопасности; основные требования информационной безопасности. На минимальном уровне умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации; применять программно-технические средства защиты и криптографические протоколы, не способен использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии. Вызывает сложность работа с программными комплексами защиты информации. Задание выполнено с ошибками.

Оценка «неудовлетворительно» выставляется студенту, который обнаружил существенные пробелы в знаниях основного учебно-программного материала по курсу. Не знает правовые основы защиты информации, виды угроз и методы обеспечения информационной безопасности; основные требования информационной безопасности. Не умеет выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации; применять программно-технические средства защиты и криптографические протоколы, не способен использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии. Не владеет навыками применения политики безопасности предприятия и навыками работы с программными комплексами защиты информации. Задание не выполнено.

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ

Локальные нормативные акты института, регламентирующие процедуры оценивания

1. Положение о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации студентов.
2. Положение о рейтинговой системе оценки знаний студентов.
3. Положение о самостоятельной работе студентов.
4. Положение о проведении компьютерного тестирования студентов.
5. Положение об оценочных и методических материалах для проведения текущего контроля, промежуточной аттестации и ГИА.

Процедура оценивания знаний, умений и навыков обучающихся

В ходе экзамена студент имеет право пользоваться рабочей программой.

Во время экзамена допускается присутствие в аудитории не более 6 обучающихся, запрещается иметь при себе и использовать средства связи.

Экзамен проводится по одному экзаменационному билету. Каждый обучающийся самостоятельно выбирает экзаменационный билет один раз посредством произвольного извлечения. В экзаменационные билеты включаются два теоретических вопроса и задача. При подготовке к ответу в устной форме студенты делают необходимые записи по каждому вопросу. На подготовку ответа первому студенту предоставляется 20 минут, остальные экзаменуемые сменяют друг друга и отвечают в порядке очереди. После ответа на все вопросы билета и выполнения задания экзаменуемому могут быть заданы дополнительные уточняющие вопросы.

Оценки «отлично», «хорошо», «удовлетворительно» означают успешную сдачу экзамена.