Аккредитованное образовательное частное учреждение высшего образования
«Московский финансово-юридический университет МФЮА»

Рассмотрено и одобрено на заседании учебно-методического совета

Протокол № 10 от 21.06.2021

Председатель совета

_____ В.В. Шутенко
личная подпись инициалы, фамилия

УТВЕРЖДАЮ

Проректор по учебной работе

_____ В.В. Шутенко
личная подпись инициалы, фамилия

« 21 » июня 2021 г.

Бычков Игорь Николаевич
(уч. звание, степень, ФИО авторов программы)

Рабочая программа дисциплины (модуля)

Системы защиты информации в ведущих зарубежных странах
(наименование дисциплины (модуля))

Направление подготовки (специальность): 40.05.01 Правовое обеспечение национальной безопасности
(код, наименование без кавычек)

ОПОП: Уголовно-правовая
(наименование)

Форма освоения ОПОП: очная, заочная
(очная, очно-заочная, заочная)

Общая трудоемкость: 4 (з.е.)

Всего учебных часов: 144 (ак. час.)

Формы промежуточной аттестации	СЕМЕСТР		
	очная	очно-заочная	заочная
Экзамен	8		10

Москва 2021 г.

Год начала подготовки студентов - 2017

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины	рассмотрение систем защиты информации в ведущих зарубежных странах, особенностей их современной организации и функционирования, перспектив развития и возможностей использования зарубежного опыта в России.
Задачи дисциплины	изучить процесс формирования и развития систем защиты информации; изучить современный опыт организации систем защиты информации; изучить правовые основы защиты информации; изучить состав органов защиты информации; изучить особенности классификации защищаемой информации; изучить особенности и направления международного сотрудничества в данной области.

2. Место дисциплины в структуре ОПОП

Блок 1 «Дисциплины (модули)»	
Дисциплины и практики, знания и умения по которым необходимы как "входные" при изучении данной дисциплины	Информатика и информационные технологии в профессиональной деятельности Правовое обеспечение информационной безопасности
Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как предшествующее	Правовые и криминологические проблемы обеспечения информационной безопасности

3. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины. Степень сформированности компетенций

Компетенции/ ЗУВ	Планируемые результаты обучения	Критерии оценивания	ФОС
ОК12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации			
Знать	основные информационные ресурсы и технологии; способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации; основные методы получения, хранения, поиска, систематизации, обработки и передачи информации	знает основные информационные ресурсы и технологии; способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации; основные методы получения, хранения, поиска, систематизации, обработки и передачи информации	Тест

Уметь	работать с различными информационными ресурсами и технологиями; применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации; решать конкретные задачи при работе с информационными ресурсами	умеет работать с различными информационными ресурсами и технологиями; применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации; решать конкретные задачи при работе с информационными ресурсами	Практическое задание
Владеть	навыками в области компьютерных технологий; современными базами данных; навыками решения поставленных задач в при работе с компьютерными сетями и базами данных	владеет навыками в области компьютерных технологий; современными базами данных; навыками решения поставленных задач в при работе с компьютерными сетями и базами данных	Выполнение реферата
ПК16 способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности			
Знать	требования, установленные нормативными правовыми актами в области защиты государственной тайны; основы разработки, оформления и ведения служебных документов; основы информационной безопасности, способы соблюдения режима секретности	знает требования, установленные нормативными правовыми актами в области защиты государственной тайны; основы разработки, оформления и ведения служебных документов; основы информационной безопасности, способы соблюдения режима секретности	Тест
Уметь	соблюдать режим секретности; использовать нормативные правовые документы в своей профессиональной деятельности; анализировать и обобщать служебную информацию по степени ее конфиденциальности	умеет соблюдать режим секретности; использовать нормативные правовые документы в своей профессиональной деятельности; анализировать и обобщать служебную информацию по степени ее конфиденциальности	Практическое задание
Владеть	навыками применять действующее законодательство в профессиональной деятельности; приемами обеспечения и соблюдения режима секретности; способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности	владеет навыками применять действующее законодательство в профессиональной деятельности; приемами обеспечения и соблюдения режима секретности; способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности	Выполнение реферата

4. Структура и содержание дисциплины

Тематический план дисциплины

№	Название темы	Содержание	Литера-тура	Формируемые компетенции
1.	Введение	Предмет, содержание и задачи курса, методы его изучения. Особенности формирования терминологии защиты информации в зарубежных странах. Методы исследования зарубежного опыта защиты информации.	9.1.1, 9.2.1, 9.2.2, 9.1.2, 9.1.3, 9.1.4	ОК12 Знать ПК16 Знать ПК16 Уметь ПК16 Владеть ОК12 Уметь
2.	Становление и развитие систем защиты информации в ведущих зарубежных странах	Становление систем, формирование основных понятий, выработка принципов, методов, основных подходов и направлений защиты информации. Истоки разделения и классификации видов тайн. Создание первых европейских государственных секретных служб (на примере Англии, Франции, Германии). Методы защиты коммерческих сведений. Банковская тайна и особенности ее защиты. Формирование особенностей политики защиты государственных секретов и коммерческой тайны в странах Западной Европы, США и Японии в 18-начале 20 вв. Промышленный шпионаж: его значение для формирования систем защиты информации. Формирование авторского и патентного права. Особенности формирования современных систем защиты информации в ведущих зарубежных странах в 20 в. Влияние исторического опыта защиты информации на последующее формирование и развитие современных ос-нов защиты информации в зарубежных странах.	9.1.1, 9.2.1, 9.2.2, 9.1.2, 9.1.3, 9.1.4	ОК12 Знать ОК12 Уметь ОК12 Владеть ПК16 Знать ПК16 Уметь ПК16 Владеть

3.	Организация защиты информации в США	Особенности государственного устройства США. Государственная политика в области защиты информации. Организация защиты информации по национальной безопасности (государственных секретов). Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности и координирующих режимно-секретную деятельность. Структура разведывательного сообщества США и его роль в осуществлении политики защиты информации по национальной безопасности. Особенности организации защиты информации в национальной промышленности США. Защита секретной информации, используемой в международных программах. Защита информации в ходе деловых визитов и встреч. Классификация защищаемой информации. Состав грифов ограничения доступа к документам. Право первоначальной классификации информации. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США. Правовые основы защиты информации по национальной безопасности. Ответственность за компьютерные преступления. Ответственность за разглашение секретных сведений. Организация защиты коммерческой тайны. Функции по защите коммерческой тайны частных охранно-сыскных агентств и служб промышленной и коммерческой безопасности. Координация деятельности частных служб безопасности и правоохранительных органов. Создание системы коллективной безопасности предпринимательской деятельности. Ассоциации частных охранно-сыскных агентств и служб безопасности, Организация и основные направления деятельности служб безопасности фирм. Классификация информации, составляющей коммерческую тайну. Правовые основы защиты коммерческой тайны. Регламентация процедур обеспечения защиты коммерческой тайны. Организация контроля надежности функционирования системы защиты коммерческой тайны фирмы.	9.1.1, 9.2.1, 9.2.2, 9.1.2, 9.1.3, 9.1.4	ОК12 Знать ОК12 Уметь ОК12 Владеть ПК16 Знать ПК16 Уметь ПК16 Владеть

4.	Организация защиты информации в Германии	Особенности государственного устройства Германии. Государственная политика в области защиты информации. Организация системы специальных служб Германии. Основные звенья системы специальных служб. Особенности и основные принципы организации их деятельности. Функции разведывательных, контрразведывательных и полицейских органов в области защиты информации. Парламентско-правительственный контроль за деятельностью специальных служб. Состав, структура и основные направления деятельности служб безопасности Германии. Основные категории служб безопасности. Агентства, предоставляющие частным фирмам, банкам и государственным учреждениям услуги по обеспечению безопасности зданий, объектов и лиц, подлежащих охране. Частные промышленные и коммерческие службы безопасности. Подразделения внутренней охраны, создаваемые частными предприятиями, фирмами, финансово-кредитными организациями. Роль специальных служб в подборе, проверке персонала и контроле коммерческой деятельности совместных фирм. Добывание информации, контроль иностранных граждан на территории Германии. Взаимодействие системы специальных служб и правоохранительных органов с частными промышленными и коммерческими службами безопасности.	9.1.1, 9.2.1, 9.2.2, 9.1.2, 9.1.3, 9.1.4	ОК12 Знать ОК12 Уметь ОК12 Владеть ПК16 Знать ПК16 Уметь ПК16 Владеть

5.	Организация защиты информации в Великобритании	Особенности государственного устройства Великобритании. Государственная политика в области защиты информации. Организация системы специальных служб Великобритании. Основные звенья системы специальных служб. Высшие органы разведки и контрразведки. Центральные органы разведки и контрразведки. Организация и координация их деятельности. Основные функции специальных служб Великобритании в области защиты информации. Состав, структура и основные направления деятельности служб безопасности Великобритании. Основные категории служб безопасности. Службы по борьбе с коммерческими преступлениями, создаваемые на государственном уровне. Функции специальных подразделений министерства торговли и промышленности по предупреждению коммерческих преступлений. Службы безопасности предприятий и фирм. Частные фирмы и консультанты, занимающиеся вопросами безопасности и защиты коммерческой тайны. Основные функции служб безопасности. Основные направления совершенствования работы служб безопасности. Особенности защиты информации и предупреждение компьютерных преступлений в банковской сфере. Ответственность за компьютерные преступления.	9.1.1, 9.2.1, 9.2.2, 9.1.2, 9.1.3, 9.1.4	ПК16 Знать ПК16 Уметь ПК16 Владеть ОК12 Знать ОК12 Уметь ОК12 Владеть

6.	Организация защиты информации во Франции	Особенности государственного устройства Франции. Государственная политика в области защиты информации. Организация системы специальных служб Франции. Основные звенья системы специальных служб. Организация и координация их деятельности. Основные функции специальных служб Франции в области защиты информации. Состав, структура и основные направления деятельности служб безопасности Франции. Основные категории служб безопасности. Службы безопасности в промышленно-торговых фирмах и финансовых учреждениях (банках, страховых компаниях, инвестиционных фирмах). Службы безопасности в фирмах, выполняющих государственные заказы в сфере оборонной промышленности, космических и ядерных исследований, новых видов вооружений, средств связи и транспорта. Частные службы безопасности и частные охранно-сыскные бюро, основная сфера их деятельности. Профессиональные объединения частных служб промышленной и коммерческой безопасности и частных охранных бюро, цели их создания. Основные функции служб безопасности. Методы и основные направления совершенствования работы служб безопасности. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов. Коммерческая тайна и организация доступа к информации, принадлежащей частным предприятиям. Ответственность за компьютерные преступления. Ответственность за нарушение требований к организации деятельности частных служб безопасности.	9.1.1, 9.2.1, 9.2.2, 9.1.2, 9.1.3, 9.1.4	ПК16 Знать ПК16 Уметь ПК16 Владеть ОК12 Знать ОК12 Уметь ОК12 Владеть

7.	Международное сотрудничество в области защиты информации	Научно-техническое сотрудничество с зарубежными партнерами. Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др. Регламентация процедур обеспечения защиты информации в ходе посещения представителями зарубежных фирм охраняемых объектов. Система контроля. Порядок предоставления защищаемой информации другим странам. Международный опыт защиты информации в процессе банковской деятельности. Международный опыт стандартизации в области защиты информации. Международная защита интеллектуальной собственности. Международные договоры и иные международно-правовые документы (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах, Договор об образовании Европейского экономического сообщества и др.) о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства, предупреждении компьютерных преступлений.	9.1.1, 9.2.1, 9.2.2, 9.1.2, 9.1.3, 9.1.4	ПК16 Знать ПК16 Уметь ПК16 Владеть ОК12 Знать ОК12 Уметь ОК12 Владеть
8.	Системы защиты информации в Китайской народной республике	Представление об информационном противоборстве в Китае Законодательство в сфере информационной безопасности в Китае Организационная структура спецслужб Китае «Великая стена» информационной безопасности Китае	9.1.5, 9.1.6, 9.1.7, 9.1.1, 9.1.2, 9.2.3	ОК12 Знать ОК12 Уметь ОК12 Владеть ПК16 Знать ПК16 Уметь ПК16 Владеть
9.	Международные стандарты информационной безопасности	Международный стандарт ISO 17799 Международный стандарт ISO 15408 «Общий критерий» Международные стандарты серии 27000	9.1.5, 9.1.6, 9.1.7, 9.1.1, 9.1.2, 9.2.3	ОК12 Знать ОК12 Уметь ОК12 Владеть ПК16 Знать ПК16 Уметь ПК16 Владеть
10.	Термины и определения	Основные термины и их определения, которые используются по данной дисциплине	9.1.5, 9.1.6, 9.1.7, 9.1.1, 9.1.2, 9.2.3	ОК12 Знать ОК12 Уметь ОК12 Владеть ПК16 Знать ПК16 Уметь ПК16 Владеть

Распределение бюджета времени по видам занятий с учетом формы обучения

Форма обучения: очная, 8 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	3	1	0	2	6

2.	3	1	0	2	6
3.	3	1	0	2	6
4.	3	1	0	2	6
5.	6	2	0	4	6
6.	6	2	0	4	6
7.	6	2	0	4	6
8.	6	2	0	4	6
9.	6	2	0	4	6
10.	6	2	0	4	6
	Промежуточная аттестация				
	4	0	0	0	32
	Консультации				
	0	0	0	0	0
Итого	52	16	0	32	92

Форма обучения: заочная, 10 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	0.5	0.5	0	0	10
2.	0.5	0.5	0	0	10
3.	0.5	0.5	0	0	10
4.	0.5	0.5	0	0	10
5.	1.5	0.5	0	1	10
6.	1.5	0.5	0	1	10
7.	1.5	0.5	0	1	10
8.	1.5	0.5	0	1	10
9.	1	0	0	1	10
10.	1	0	0	1	8
	Промежуточная аттестация				
	4	0	0	0	32
	Консультации				
	0	0	0	0	0
Итого	14	4	0	6	130

5. Методические указания для обучающихся по освоению дисциплины

В процессе освоения дисциплины студенту необходимо посетить все виды занятий, предусмотренные рабочей программой дисциплины и выполнить контрольные задания, предлагаемые преподавателем для успешного освоения дисциплины. Также следует изучить рабочую программу дисциплины, в которой определены цели и задачи дисциплины, компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения. Рассмотреть содержание тем дисциплины; взаимосвязь тем лекций и практических занятий; бюджет времени по видам занятий; оценочные средства для текущей и промежуточной аттестации; критерии итоговой оценки результатов освоения дисциплины. Ознакомиться с методическими материалами, программно-информационным и материально техническим обеспечением дисциплины.

Работа на лекции

Лекционные занятия включают изложение, обсуждение и разъяснение основных направлений и вопросов изучаемой дисциплины, знание которых необходимо в ходе реализации всех остальных видов занятий и в самостоятельной работе студентов. На лекциях студенты получают самые необходимые знания по изучаемой проблеме. Непременным условием для глубокого и прочного усвоения учебного материала является умение студентов сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения. Внимательное слушание лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, конспектирование их помогает усвоить материал. Конспект является полезным тогда, когда записано самое существенное, основное. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями. Работая над конспектом лекций, всегда следует использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал лектор.

Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, студенту следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов студентов.

Самостоятельная работа

Студент в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Самостоятельная работа студентов играет важную роль в воспитании сознательного отношения самих студентов к овладению теоретическими и практическими знаниями, привитии им привычки к направленному интеллектуальному труду. Самостоятельная работа проводится с целью углубления знаний по дисциплине. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в рабочей программе. Изучение литературы следует начинать с освоения соответствующих разделов дисциплины в учебниках, затем ознакомиться с монографиями или статьями по той тематике, которую изучает студент, и после этого – с брошюрами и статьями, содержащими материал, дающий углубленное представление о тех или иных аспектах рассматриваемой проблемы. Для расширения знаний по дисциплине студенту необходимо использовать Интернет-ресурсы и специализированные базы данных: проводить поиск в различных системах и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

Подготовка к сессии

Основными ориентирами при подготовке к промежуточной аттестации по дисциплине являются конспект лекций и перечень рекомендуемой литературы. При подготовке к сессии студенту следует так организовать учебную работу, чтобы перед первым днем начала сессии были сданы и защищены все практические работы. Основное в подготовке к сессии – это повторение всего материала курса, по которому необходимо пройти аттестацию. При подготовке к сессии следует весь объем работы распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы.

6. Фонды оценочных средств для текущего контроля успеваемости, промежуточной аттестации и самоконтроля по итогам освоения дисциплины

Технология оценивания компетенций фондами оценочных средств:

- формирование критериев оценивания компетенций;
- ознакомление обучающихся в ЭИОС с критериями оценивания конкретных типов оценочных средств;
- оценивание компетенций студентов с помощью оценочных средств;
- публикация результатов освоения ОПОП в личном кабинете в ЭИОС обучающегося;

Тест для формирования «Знать» компетенции ОК12

Вопрос №1 .

Защита информации обеспечивается применением антивирусных средств

Варианты ответов:

1. да
2. нет
3. не всегда
4. в том числе

Вопрос №2 .

Какая разведывательная спецслужба Германии занимается выявлением антиконституционных политических устремлений, обнаружение шпионов, защита государственной тайны?

Варианты ответов:

1. DRM
2. MAD
3. УР
4. АНБ
5. БНД

Вопрос №3 .

В какой разведывательной спецслужбе Германии главной задачей является разоблачение фактов военного шпионажа, предотвращение диверсий, борьба с агентурой, внедряемой в Бундесвер?

Варианты ответов:

1. УРО
2. НУВКР
3. МАД
4. БФФ
5. БНД

Вопрос №4 .

Какое управление Франции отвечает за предоставление политическому и военному руководству страны аналитической информации, адекватно отражающей обстановку в мире и необходимой для принятия важных решений.

Варианты ответов:

1. разведывательное
2. стратегическое
3. техническое
4. оперативное
5. адмнистративное

Вопрос №5 .

Разведка какого государства имеет достаточно сложную структуру, которая заслужила славу хоть и эффективной, но достаточно грубой?

Варианты ответов:

1. США
2. Германии
3. Великбритании
4. Израиля
5. Франции

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Практическое задание для формирования «Уметь» компетенции ОК12

Постройте иерархическую пирамиду защищаемых ресурсов информационной системы, обозначив 1 - наиболее защищаемый ресурс, 4 - наименее защищаемый ресурс.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «Уметь» компетенции ОК12

1. Оцените суммарную максимальную и суммарную минимальную величину ущерба от реализации совокупности следующих угроз: 1) неумышленные действия (ошибки) персонала; 2) атаки злоумышленников; 3) другие угрозы. При этом первая угроза может возникнуть с вероятностью 20% (потери от её реализации с наибольшей вероятностью могут составить максимально от 1 млн. руб. до минимально 200 тыс. руб.), а соответствующие финансовые потери от каждой последующей угрозы составляют 40% от соответствующих максимальных и минимальных потерь от реализации предыдущей угрозы. Вероятность второй и третьей угрозы составляет соответственно 10% и 5%.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Выполнение реферата для формирования «Владеть» компетенции ОК12

Методы несанкционированного доступа к информации.

Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

Способы наблюдения с использованием технических средств.

Каналы утечки информации. Технические каналы утечки

Классификация технических каналов утечки по физической природе носителя.

Классификация технических каналов утечки по информативности.

Классификация технических каналов утечки по времени функционирования.

Классификация технических каналов утечки по структуре.

Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.

Перехват электромагнитных излучений.

Акустическое подслушивание. Эффекты, возникающие при подслушивании.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Тест для формирования «Знать» компетенции ПК16

Вопрос №1 .

Назовите инструмент, который используется для того, чтобы донести до аудитории полноценную информацию об объекте исследования в удобной для нее форме.

Варианты ответов:

1. презентация
2. тест
3. практикум
4. эссе

Вопрос №2 .

К опросным методам при разработке учебно-методического обеспечения экономических дисциплин относят:

Тип ответа: Многие из многих
Варианты ответов:

1. беседа
2. интервьюирование
3. анкетирование
4. сценарии
5. мозговой штурм
6. древо целей

Вопрос №3 .

Министерство обороны (МО) США занимается вопросами:

Варианты ответов:

1. обеспечения внешней безопасности США (разведка)
2. сбором секретных данных из технических средств связи (электронной почты) американских и зарубежных фирм.
3. технической и информационной разведкой, реализации доктрины информационных войн (ИВ) в военной сфере.
4. по реализации доктрины ИВ и защита инфраструктуры США (контрразведка). обеспечения внешней безопасности США (разведка)

Вопрос №4 .

Национальная ассоциация компьютерной безопасности (National Computer Security Association, NCSA) США занимается:

Варианты ответов:

1. по реализации доктрины ИВ и защита инфраструктуры США (контрразведка). обеспечения внешней безопасности США (разведка)
2. сбором секретных данных из технических средств связи (электронной почты) американских и зарубежных фирм
3. обеспечения внешней безопасности США (разведка)
4. технической и информационной разведкой, реализации доктрины информационных войн (ИВ) в военной сфере

Вопрос №5 .

Центральному разведывательному управлению (ЦРУ) США занимается вопросами:

Варианты ответов:

1. обеспечения внешней безопасности США (разведка)
2. по реализации доктрины ИВ и защита инфраструктуры США (контрразведка).
3. технической и информационной разведкой, реализации доктрины информационных войн (ИВ) в военной сфере.
4. сбором секретных данных из технических средств связи (электронной почты) американских и зарубежных фирм.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Практическое задание для формирования «Уметь» компетенции ПК16

В программе «IT Advisor for risk management» построить матрицу рисков ИБ для ИС.

Пояснение к заданию:

на основе готового шаблона (например, Infrastructure Deployment – развертывание ИТ-инфраструктуры), исключить из рассмотрения все «лишние» факторы риска (нужно отметить пункт N/A) и в секции Custom описать интересующие нас риски в сфере ИБ.

1. По изученной методике оценить риски ИБ данной ИС. Результаты представьте по аналогичной форме, как в таблице «Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей».

Показатель ценности ресурса (для каждого ресурса и угрозы)	Уровень угрозы (вероятность ее осуществления)								
	Низкий (Н)			Средний (С)			Высокий (В)		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
		1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Таблица. Уровни рисков, соответствующие показателям ценности ресурсов, угроз и уязвимостей.

1. По пройденной методике на занятии выполните ранжирование угроз ИБ вашей ИС. Результаты представьте аналогично таблице «Ранжирование угроз».

I Описание угрозы	II Показатель негативного воздействия	III Вероятность реализации угрозы	IV Показатель риска	V Ранг угрозы
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Таблица. Ранжирование угроз.

1. По пройденной методике определите показатель частоты повторяемости риска. Результаты представьте по аналогичной форме, как в таблице «Показатель частоты повторяемости риска».

Уровень угрозы (вероятность ее осуществления)								
Низкий			Средний			Высокий		
Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
Н	С	В	Н	С	В	Н	С	В
	1	2	1	2	3	2	3	4

Таблица. Показатель частоты повторяемости риска.

1. По пройденной методике определите показатели пары ресурс/угроза. Результаты представьте по аналогичной форме, как в таблице «Показатели пары ресурс/угроза».

	Показатель частоты повторяемости риска
Показатель ценности ресурса	

		1	2	3	4
		1	2	3	4
1	1	2	3	4	5
2	2	3=2+1	4	5	6
3	3	4	5=3+2	6	7
4	4	5	6	7	8

Таблица. Показатели пары ресурс/угроза.

1. По пройденной методике выполните разделение рисков ИБ на приемлемые и неприемлемые. Результаты представьте по аналогичной форме, как в «Разделение рисков на приемлемые и неприемлемые».

Показатель ценности ресурса	Показатель частоты повторяемости риска				
		1	2	3	4
	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Таблица. Разделение рисков на приемлемые и неприемлемые.

1. По пройденной методике от Digital Security выполните оценку риска ИБ для каждого информационного ресурса вашей ИС.
2. Реализуйте алгоритм расчета рисков по методике от Digital Security в MS Excel.
3. Реализуйте алгоритм расчета рисков методике от Digital Security на любом доступном языке программирования.
4. «Реализуйте» (опишите) контрмеры против некоторых из имеющихся уязвимостей и рассчитайте эффективность введенных контрмер.
5. Составьте и внесите в таблицу:
    1. Перечни типов угроз ИБ и вероятности их возникновения, на качественной шкале «высокая», «средняя», «низкая», а также укажите точную, числовую вероятность. Угрозы разбейте по категориям нарушения конфиденциальности, целостности и доступности.
    2. Информационные ресурсы и их ценность, выраженную на количественной шкале (в деньгах) и качественной (по шкале «высокая», «средняя», «низкая»).
6. Оцените риски по методике предложенной Microsoft с использованием «матрицы рисков». Внесите составленные матрицы рисков для каждого элемента ИС и общую матрицу рисков для ИС в таблицу.
7. Составьте отчет о проведенном аудите ИС в программе COBRA.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «Уметь» компетенции ПК16

Рассчитайте, какой криптографический ключ наименее устойчив к взлому при его длине в 0,1 пико-йоттабайт, 10 микро-зеттабайт или 100 нано-эксабайт.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Выполнение реферата для формирования «Владеть» компетенции ПК16

Классификация информации. Виды данных и носителей.

Ценность информации. Цена информации.

Количество и качество информации.

Виды защищаемой информации.

Демаскирующие признаки объектов защиты.

Классификация источников и носителей информации.

мероприятия по управлению доступом к информации.

Функциональные источники сигналов. Опасный сигнал.

Основные средства и системы, содержащие потенциальные источники опасных сигналов.

Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.

Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

Виды угроз безопасности информации.

Основные принципы добывания информации.

Процедура идентификации, как основа процесса обнаружения объекта.

Методы синтеза информации.

Критерии оценки выполнения задания

Оценка	Критерии оценивания

Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Вопросы для проведения промежуточной аттестации по итогам освоения дисциплины

Тема 1. Введение

1. Метод изучения нормативно-правовых актов в области защиты информации;
2. Метод интерактивного участия в системе (внедрение агентов, заключение международных договоров с организациями, где циркулирует информация ограниченного распространения);
3. Метод изучения научно-технического потенциала стран через открытые источники (исследование патентной базы, научных публикаций, рекламных проспектов и т.п. в сфере за-щиты информации).

Тема 2. Становление и развитие систем защиты информации в ведущих зарубежных странах

4. Формирование подходов к защите информации в Древнем мире.
5. Становление систем, методов и принципов защиты информации в зарубежных странах в новое время.
6. Принципы формирования в XYII - XYIII вв. элементов системы организационной защиты информации (принцип дробления информации, отсутствие письменного изложения секретной технологии работ, дезинформация, материальное стимулирование, создание профессиональных служб безопасности и др.).
7. Методы противодействия промышленному шпионажу в Европе в XIX в.
8. Правовая регламентация процесса защиты информации в зарубежных странах в XIX - начале XX вв.
9. Становление системы защиты информации в странах Западной Европы.
10. Становление системы защиты информации в США.
11. Защита информации, содержащейся в торговых книгах, в XIX - начале XX вв.

Тема 3. Организация защиты информации в США

12. Состав и основные функции органов, осуществляющих защиту информации по национальной безопасности и координирующих режимно-секретную деятельность.
13. Структура разведывательного сообщества США и его роль в осуществлении политики защиты информации по национальной безопасности.
14. Особенности организации защиты информации в национальной промышленности США.
15. Защита секретной информации, используемой в международных программах. Защита информации в ходе деловых визитов и встреч.
16. Классификация защищаемой информации. Состав грифов ограничения доступа к документам. Право первоначальной классификации информации. Доступ к правительственной информации. Порядок предоставления доступа к информации лицам, не являющимся гражданами США.

17. Правовые основы защиты информации по национальной безопасности.
18. Ответственность за компьютерные преступления. Ответственность за разглашение секретных сведений.
19. Организация защиты коммерческой тайны. Функции по защите коммерческой тайны частных охранно-сыскных агентств и служб промышленной и коммерческой безопасности.
20. Координация деятельности частных служб безопасности и правоохранительных органов. Создание системы коллективной безопасности предпринимательской деятельности. Ассоциации частных охранно-сыскных агентств и служб безопасности,
21. Организация и основные направления деятельности служб безопасности фирм. Извлечения из государственных законов США, используемых в процессе осуществления режимно-секретной деятельности.
22. Нормативные документы, регламентирующие вопросы обеспечения защиты информации по национальной безопасности в США.

Тема 4. Организация защиты информации в Германии

23. Особенности государственного устройства Германии. Государственная политика в области защиты информации.
24. Организация системы специальных служб Германии. Основные звенья системы специальных служб. Особенности и основные принципы организации их деятельности.
25. Функции разведывательных, контрразведывательных и полицейских органов в области защиты информации.
26. Парламентско-правительственный контроль за деятельностью специальных служб. Состав, структура и основные направления деятельности служб безопасности Германии.
27. Основные категории служб безопасности. Агентства, предоставляющие частным фирмам, банкам и государственным учреждениям услуги по обеспечению безопасности зданий, объектов и лиц, подлежащих охране.
28. Частные промышленные и коммерческие службы безопасности. Подразделения внутренней охраны, создаваемые частными предприятиями, фирмами, финансово-кредитными организациями.
29. Роль специальных служб в подборе, проверке персонала и контроле коммерческой деятельности совместных фирм.
30. Добывание информации, контроль иностранных граждан на территории Германии.
31. Взаимодействие системы специальных служб и правоохранительных органов с частными промышленными и коммерческими службами безопасности.

Тема 5. Организация защиты информации в Великобритании

32. Особенности государственного устройства Великобритании. Государственная политика в области защиты информации.
33. Организация системы специальных служб Великобритании. Основные звенья системы специальных служб.
34. Высшие органы разведки и контрразведки. Центральные органы разведки и контрразведки. Организация и координация их деятельности.
35. Основные функции специальных служб Великобритании в области защиты информации. Состав, структура и основные направления деятельности служб безопасности Великобритании. Основные категории служб безопасности.
36. Службы по борьбе с коммерческими преступлениями, создаваемые на государственном уровне. Функции специальных подразделений министерства торговли и промышленности по предупреждению коммерческих преступлений.
37. Службы безопасности предприятий и фирм. Частные фирмы и консультанты, занимающиеся вопросами безопасности и защиты коммерческой тайны. Основные функции служб безопасности. Основные направления совершенствования работы служб безопасности.
38. Особенности защиты информации и предупреждение компьютерных преступлений в банковской сфере.
39. Ответственность за компьютерные преступления.

Тема 6. Организация защиты информации во Франции

40. Особенности государственного устройства Франции. Государственная политика в области защиты информации.
41. Организация системы специальных служб Франции. Основные звенья системы специальных служб. Организация и координация их деятельности. Основные функции специальных служб Франции в области защиты информации. Состав, структура и основные направления деятельности служб безопасности Франции. Основные категории служб безопасности.
42. Службы безопасности в промышленно-торговых фирмах и финансовых учреждениях (банках, страховых компаниях, инвестиционных фирмах). Службы безопасности в фирмах, выполняющих государственные заказы в сфере оборонной промышленности, космических и ядерных исследований, новых видов вооружений, средств связи и транспорта.
43. Частные службы безопасности и частные охранно-сыскные бюро, основная сфера их деятельности. Профессиональные объединения частных служб промышленной и коммерческой безопасности и частных охранных бюро, цели их создания. Основные функции служб безопасности. Методы и основные направления совершенствования работы служб безопасности.
44. Правовые основы защиты информации. Государственная тайна и организация доступа к правительственной информации, парламентским заседаниям, публикация парламентских документов.
45. Коммерческая тайна и организация доступа к информации, принадлежащей частным предприятиям.
46. Ответственность за компьютерные преступления. Ответственность за нарушение требований к организации деятельности частных служб без-опасности.

Тема 7. Международное сотрудничество в области защиты информации

47. Научно-техническое сотрудничество с зарубежными партнерами. Организация защиты информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др.
48. Регламентация процедур обеспечения защиты информации в ходе посещения представителями зарубежных фирм охраняемых объектов.
49. Система контроля.
50. Порядок предоставления защищаемой информации другим странам. Международный опыт защиты информации в процессе банковской деятельности. Международный опыт стандартизации в области защиты информации.
51. Международная защита интеллектуальной собственности.
52. Международные договоры и иные международно-правовые документы (Всеобщая декларация прав человека, Международный пакт о гражданских и политических правах,
53. Договор об образовании Европейского экономического сообщества и др.) о защите информации, предупреждении недобросовестной конкуренции в процессе международного предпринимательства, предупреждении компьютерных преступлений. Порядок предоставления защищаемой информации другим странам.
54. Организация защиты информации в процессе проведения международных конференций, обмена специалистами и др.
55. Особенности защиты информации в ЕС.

Тема 8. Системы защиты информации в Китайской народной республике

56. Что представляет собой концепция ИВ Китая.
57. Назовите основные мероприятия, осуществляемые руководством Китая, направленные на повышение ИБ страны.
58. Какие задачи решаются в Китае в рамках интеграции в мировые информационные системы.
59. Каковы основные мероприятия по обеспечению ИБ Китая, осуществляемые в процессе интеграции в глобальную сеть Интернет.
60. Охарактеризуйте нормативно-правовую базу Китая в сфере ИБ и ответственность за компьютерные преступления в Китае.
61. Каковы основные элементы правовой системы ИБ Китая.
62. Перечислите основные спецслужбы Китая, какие функции они выполняют.
63. Что такое «Великая стена» информационной безопасности Китая? Какие задачи ей присущи.

64. Каковы особенности поддержки Интернет-ресурсов частными лицами в Китае.

Тема 9. Международные стандарты информационной безопасности

65. С какой целью разрабатывались международные стандарты ИБ.
66. Назовите основные международные стандарты ИБ.
67. Какие критерии определяют степень доверия в стандарте «Оранжевая книга».
68. Определите назначения и виды классов безопасности в «Оранжевой книге».
69. Как определяются составляющие ИБ в гармозированных критериях Европейских стран.
70. Назовите составляющие германского стандарта BSI.
71. Почему Британский стандарт BS 7799 используется наиболее часто.
72. В чем отличие применения международных стандартов ISO 15408 и ISO 17799.
73. Назовите основные этапы проведения аудита ИБ при использовании стандарта CoBiT.

Тема 10. Термины и определения

74. Дайте определение информации.
75. Дайте определение понятию информационная безопасность и обеспечение информационной безопасности.
76. Дайте определение понятию информационное воздействие, его методы и способы.
77. Дайте определение понятию информационные войны, в чем состоят цели информационной войны.
78. Назовите основные формы информационной войны.
79. Дайте определение понятию «информационное оружие» и назовите основные виды информационного оружия.

Уровни и критерии итоговой оценки результатов освоения дисциплины

	Критерии оценивания	Итоговая оценка
Уровень1. Недостаточный	Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий	Неудовлетворительно/Незачтено
Уровень 2. Базовый	Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Удовлетворительно/зачтено
Уровень 3. Повышенный	Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Хорошо/зачтено
Уровень 4. Продвинутый	Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения	Отлично/зачтено

7. Ресурсное обеспечение дисциплины

Лицензионное программно-информационное обеспечение	1. Microsoft Windows (лицензионное программное обеспечение) 2. Microsoft Office (лицензионное программное обеспечение) 3. Google Chrome (свободно-распространяемое программное обеспечение) 4. Браузер Спутник (свободно-распространяемое программное обеспечение отечественного производста) 5. Kaspersky Endpoint Security (лицензионное программное обеспечение) 6. «Антиплагиат.ВУЗ» (лицензионное программное обеспечение)
Современные профессиональные базы данных	1. Консультант+ (лицензионное программное обеспечение отечественного производства) 2. http://www.garant.ru (ресурсы открытого доступа)
Информационные справочные системы	1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа) 2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа) 3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа) 4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)
Интернет-ресурсы	1. http://window.edu.ru - Информационная система "Единое окно доступа к образовательным ресурсам" 2. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)
Материально-техническое обеспечение	Учебные аудитории для проведения: занятий лекционного типа, обеспеченные наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации, помещения для хранения и профилактического обслуживания учебного оборудования.

8. Учебно-методические материалы

№	Автор	Название	Издательство	Год издания	Вид издания	Кол-во в библио-теке	Адрес электронного ресурса	Вид доступа
1	2	3	4	5	6	7	8	9
9.1 Основная литература								
9.1.1	Аверченков В.И. Рытов М.Ю. Кондрашин Г.В. Рудановский М.В.	Системы защиты информации в ведущих зарубежных странах	Брянский государственный технический университет	2012	учебное пособие	-	http://www.iprbookshop.ru/7007.html	по логину и паролю
9.1.2	Прохорова О.В.	Информационная безопасность и защита информации	Самарский государственный архитектурно-строительный университет, ЭБС АСВ	2014	учебник	-	http://www.iprbookshop.ru/43183.html	по логину и паролю
9.1.3	Метелица Н.Т.	Вычислительные сети и защита информации	Южный институт менеджмента	2013	учебное пособие	-	http://www.iprbookshop.ru/25962.html	по логину и паролю

9.1.4	Астахова А.В.	Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД	Троицкий мост	2014	учебное пособие	-	http://www.iprbookshop.ru/40860.html	по логину и паролю
9.1.5	Шаньгин В.Ф.	Информационная безопасность и защита информации	Профобразование	2019	учебное пособие	-	http://www.iprbookshop.ru/87995.html	по логину и паролю
9.1.6	Гультяева Т.А.	Основы защиты информации	Новосибирский государственный технический университет	2018	учебное пособие	-	http://www.iprbookshop.ru/91638.html	по логину и паролю
9.1.7	Котенко В.В. Румянцев К.Е.	Теория информации	Издательство Южного федерального университета	2018	учебное пособие	-	http://www.iprbookshop.ru/87680.html	по логину и паролю
9.2 Дополнительная литература								
9.2.1	Гимбицкая Л.А. Альбекова З.М.	Администрирование в информационных системах	Северо-Кавказский федеральный университет	2014	учебное пособие	-	http://www.iprbookshop.ru/62917.html	по логину и паролю
9.2.2	Медведкова И.Е. Бугаев Ю.В. Чикунов С.В.	Базы данных	Воронежский государственный университет инженерных технологий	2014	учебное пособие	-	http://www.iprbookshop.ru/47418.html	по логину и паролю
9.2.3	Аверченков В.И. Рытов М.Ю.	Организационная защита информации	Брянский государственный технический университет	2012	учебное пособие	-	http://www.iprbookshop.ru/7002.html	по логину и паролю

9. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья

В МФЮА созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в МФЮА созданы специальные условия для беспрепятственного доступа в учебные помещения и другие помещения, а также их пребывания в указанных помещениях с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Также имеется возможность предоставления услуг ассистента, оказывающего обучающимся с ограниченными возможностями здоровья необходимую техническую помощь, в том числе услуг сурдопереводчиков и тифлосурдопереводчиков.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в университете комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте университета (http://www.mfua.ru/sveden/objects/#objects).

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию обучающимися инвалидами и лицами с ОВЗ с нарушенным слухом справочного, учебного материала, предусмотренного образовательной программой по выбранным направлениям подготовки, обеспечиваются следующие условия:

для лучшей ориентации в аудитории, применяются сигналы, оповещающие о начале и конце занятия (слово «звонок» пишется на доске);

внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
разговаривая с обучающимся, педагог смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих инвалидов и лиц с ОВЗ проводится за счет:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой МФЮА по выбранной специальности, обеспечиваются следующие условия:

ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
в начале учебного года обучающиеся несколько раз проводятся по зданию МФЮА для запоминания месторасположения кабинетов, помещений, которыми они будут пользоваться;
педагог, его собеседники, присутствующие представляются обучающимся, каждый раз называется тот, к кому педагог обращается;
действия, жесты, перемещения педагога коротко и ясно комментируются;
печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
обеспечивается необходимый уровень освещенности помещений;
предоставляется возможность использовать компьютеры во время занятий и право записи объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ определяется преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.