Автономная некоммерческая организация высшего образования
«МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ»

Кафедра экономики и управления

Рабочая программа дисциплины

Информационная безопасность

Направление подготовки	Государственное и муниципальное управление
Код	38.03.04
Направленность (профиль)	Региональное и муниципальное управление
Квалификация выпускника	бакалавр

Москва
2017 г.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Компетенция	Планируемые результаты обучения по дисциплине
ОПК-6 способность осуществлять деловое общение и публичные выступления, вести переговоры, совещания, осуществлять деловую переписку и поддерживать электронные коммуникации	***Знать:*** – содержание проблемы информационной безопасности в условиях широкого применения и использование информационных компьютерных систем и вычислительных сетей; ***Уметь:*** – применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий. ***Владеть:*** – основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером; – основными понятиями и методами информационной безопасности.
ПК-8 способность применять информационно-коммуникационные технологии в профессиональной деятельности с видением их взаимосвязей и перспектив использования	***Знать:*** – принципы обеспечения информационной безопасности в свете положений Доктрины информационной безопасности Российской Федерации, основные нормативные и руководящие документы в этой области; ***Уметь:*** – владеть навыками анализа информации о функционировании системы внутреннего документооборота организации ***Владеть:*** – основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером;
ПК-15 способность применять информационно-коммуникационные технологии в профессиональной деятельности с видением их взаимосвязей и перспектив использования	***Знать:*** – принципы системного анализа и классификации угроз информационной безопасности; – существующие средства и методы обеспечения информационной безопасности. ***Уметь:*** – применять необходимые средства и методы при практической реализации защищенных информационных систем и технологий. – владеть навыками анализа информации о функционировании системы внутреннего документооборота организации ***Владеть:*** – основными понятиями и методами информационной безопасности.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина относится к базовой части учебного плана ОПОП.

Данная дисциплина взаимосвязана с другими дисциплинами, такими как: «История мировых цивилизаций», «Административное право», «Конституционное право», «Иностранный язык», «Основы государственного и муниципального управления».

Изучение дисциплины позволит обучающимся реализовывать общепрофессиональные и профессиональные компетенции в профессиональной деятельности.

В частности, выпускник, освоивший программу бакалавриата, в соответствии с организационно-управленческой, информационно-методической, проектной, вспомогательно-технологической (исполнительской) видами деятельности, должен быть готов решать следующие профессиональные задачи:

организационно-управленческая деятельность:

-организация исполнения полномочий органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, лиц, замещающих государственные и муниципальные должности, осуществление прав и обязанностей государственных и муниципальных предприятий и учреждений, научных и образовательных организаций, политических партий, общественно-политических, некоммерческих и коммерческих организаций;

-разработка и реализация управленческих решений, в том числе нормативных актов, направленных на исполнение полномочий государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, лиц, замещающих государственные и муниципальные должности, осуществление прав и обязанностей государственных и муниципальных предприятий и учреждений, научных и образовательных организаций, политических партий, общественно-политических, некоммерческих и коммерческих организаций;

-участие в разработке социально ориентированных мер регулирующего воздействия на общественные отношения и процессы социально-экономического развития;

-участие в процессах бюджетного планирования и оценки эффективности бюджетных расходов;

-участие в обеспечении рационального использования и контроля ресурсов органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, государственных и муниципальных предприятий и учреждений, научных и образовательных организаций, политических партий, общественно-политических, коммерческих и некоммерческих организаций;

-планирование деятельности организаций и подразделений, формирование организационной и управленческой структуры в органах государственной власти Российской Федерации, органах государственной власти субъектов Российской Федерации, органах местного самоуправления, государственных и муниципальных предприятиях и учреждениях, научных и образовательных организациях, политических партиях, общественно-политических, некоммерческих и коммерческих организациях;

-организационное обеспечение деятельности лиц, замещающих государственные должности Российской Федерации, государственные должности субъектов Российской Федерации, должности муниципальной службы;

-организационно-административное обеспечение деятельности государственных и муниципальных предприятий и учреждений, научных и образовательных организаций, политических партий, общественно-политических, некоммерческих и коммерческих организаций;

-организация контроля качества управленческих решений и осуществление административных процессов;

-организация взаимодействия с внешними организациями и гражданами;

-содействие развитию механизмов общественного участия в принятии и реализации управленческих решений;

-обеспечение исполнения основных функций, административных регламентов органов

государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, государственных и муниципальных предприятий и учреждений, научных и образовательных организаций, политических партий, общественно-политических, коммерческих и некоммерческих организаций;

информационно-методическая деятельность:

-документационное обеспечение деятельности лиц, замещающих государственные должности Российской Федерации, замещающих государственные должности субъектов Российской Федерации, замещающих должности муниципальной службы, лиц на должностях в государственных и муниципальных предприятиях и учреждениях, научных и образовательных организаций, политических партий, общественно-политических, некоммерческих и коммерческих организаций;

-участие в создании и актуализации информационных баз данных для принятия управленческих решений;

-информационно-методическая поддержка, подготовка информационно-методических материалов и сопровождение управленческих решений;

-сбор и классификационно-методическая обработка информации об имеющихся политических, социально-экономических, организационно-управленческих процессах и тенденциях;

-участие в информатизации деятельности соответствующих органов и организаций;

-защита служебной и конфиденциальной информации, обеспечение открытого доступа граждан к информации в соответствии с положениями законодательства;

проектная деятельность:

-участие в разработке и реализация проектов в области государственного и муниципального управления;

-участие в проектировании организационных систем;

-проведение расчетов с целью выявления оптимальных решений при подготовке и реализации проектов;

-оценка результатов проектной деятельности;

вспомогательно-технологическая (исполнительская):

-ведение делопроизводства и документооборота в органах государственной власти Российской Федерации, органах государственной власти субъектов Российской Федерации, органах местного самоуправления, государственных и муниципальных предприятиях и учреждениях, научных и образовательных организациях, политических партиях, общественно-политических, некоммерческих и коммерческих организациях;

-осуществление действий (административных процедур), обеспечивающих предоставление государственных и муниципальных услуг в соответствии с законодательством Российской Федерации;

-технологическое обеспечение служебной деятельности специалистов (по категориям и группам должностей государственной гражданской и муниципальной службы);

-обеспечение исполнения основных функций, административных регламентов органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, государственных и муниципальных предприятий и учреждений, научных и образовательных организаций, политических партий, общественно-политических, коммерческих и некоммерческих организаций.

3. Объем дисциплины

Виды учебной работы	*Формы обучения*
	Заочная
Общая трудоемкость: зачетные единицы/часы	2/72
Контактная работа	
Занятия лекционного типа	4
Занятия семинарского типа	8
Промежуточная аттестация: Зачет/ **зачет с оценкой** / экзамен /	4
Самостоятельная работа (СРС)	56

4. Содержание дисциплины (модуля), структурированное по темам / разделам с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Распределение часов по разделам/темам и видам работы

4.1.1. Заочная форма обучения

№ п/п	Раздел/тема	Виды учебной работы (в часах)						
		Контактная работа						Самостоятельная работа
		Занятия лекционного типа		Занятия семинарского типа				
		Лекции	*Иные учебные занятия*	*Практические занятия*	*Семинары*	*Лабораторные работы*	*Иные*	
1.	**Тема 1.** Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	1		3				16
2.	**Тема 2.** Защита информации.	1		2				20
3.	**Тема 3.** Комплексная система защиты информации	2		3				20
	Промежуточная аттестация	4						
	Итого	72						

4.2. Программа дисциплины, структурированная по темам / разделам

4.2.1. Содержание лекционного курса

№ п/	Наименование темы	Содержание лекционного занятия

п	(раздела) дисциплины	
1.	**Тема 1.** Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	Защита информации как объективная закономерность эволюции постиндустриального общества. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Системный анализ угроз безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации. Организационно-правовое обеспечение защиты информации. Уязвимость информации и ее оценка. Виды, происхождение, предпосылки появления и источники угроз информационной безопасности. Последствия таких угроз. Случайные угрозы: отказы, сбои, ошибки, аварийные ситуации, побочные влияния внешней среды. Преднамеренные угрозы, злоумышленные действия людей. Модель нарушителя информационной безопасности. Несанкционированная модификация структур КС в процессе эксплуатации. Традиционные методы промышленного шпионажа. Утечка информации по техническим каналам.
2.	**Тема 2.** Защита информации.	Защита информации в компьютерных системах от случайных угроз. Защита информации от утечки по техническим каналам. Защита информации от побочных электромагнитных излучений и наводок. Блокировка ошибочных операций. Защита информации в компьютерных системах от несанкционированного вмешательства. Криптографические методы защиты. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.
3.	**Тема 3.** Комплексная система защиты информации	Компьютерные вирусы и антивирусные программные средства. Модели распространения вирусных программ. Классификация компьютерных вирусов. Комплексная система защиты информации в компьютерных системах. Контроль сбоев и отказов в работе оборудования. Резервирование технических средств. Помехоустойчивое кодирование. Коды, обнаруживающие и исправляющие ошибки. Код Хэмминга. Дублирование информации. Технология RAID.

4.2.2. Содержание практических занятий

№ п/п	Наименование темы (раздела) дисциплины	*Содержание практического занятия*
1.	**Тема 1.** Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	№1. Найти кодовое слово, если дан код (7, 4) , порожденный многочленом g(x) = x^3 + x^2 +1, а информационным сообщением является вектор a = 1011. №2. Пусть (7,4)-код порожден многочленом g(x) = x^3 + x^2 +1 и принято слово 1110111. Была ли

		ошибка при передаче информационного сообщения 1011?
2.	**Тема 2.** Защита информации.	№1Оцените время раскрытия пароля, если число символов в сообщении, передаваемом в систему при попытке получить доступ к ней, равно 20, 600 симв/мин – скорость передачи символов, длина пароля равна 6, число символов в алфавите – 26. Ответ дать в месяцах. № 2 Выберите необходимую длину пароля, чтобы вероятность его отгадывания не превышала 0.001 за 3 месяца. На одну попытку посылается 20 символов, скорость передачи данных равна 600 символов в минуту. №3 Зашифровать с помощью алгоритма RSA сообщение на русском языке «РИМ».
3.	**Тема 3.** Комплексная система защиты информации	№ 1 Поясните сущность эвристического анализа, применяемого для удаления вирусов. № 2 . Рассмотрите механизм заражения файловыми вирусами. Какими особенностями обладают макровирусы.

4.2.3. Содержание самостоятельной работы

№ п/п	Наименование темы (раздела) дисциплины	Содержание самостоятельной работы
1.	**Тема 1.** Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	Защита информации как объективная закономерность эволюции постиндустриального общества. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Системный анализ угроз безопасности в компьютерных системах. Общая характеристика средств и методов защиты информации. Организационно-правовое обеспечение защиты информации. Уязвимость информации и ее оценка. Виды, происхождение, предпосылки появления и источники угроз информационной безопасности. Последствия таких угроз. Случайные угрозы: отказы, сбои, ошибки, аварийные ситуации, побочные влияния внешней среды. Преднамеренные угрозы, злоумышленные действия людей. Модель нарушителя информационной безопасности. Несанкционированная модификация структур КС в процессе эксплуатации. Традиционные методы промышленного шпионажа. Утечка информации по техническим каналам.
2.	**Тема 2.** Защита информации.	Защита информации в компьютерных системах от случайных угроз. Защита информации от утечки по техническим каналам. Защита информации от побочных электромагнитных излучений и наводок. Блокировка ошибочных операций. Защита информации в компьютерных системах от несанкционированного вмешательства.

		Криптографические методы защиты. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.
3.	**Тема 3.** Комплексная система защиты информации	Компьютерные вирусы и антивирусные программные средства. Модели распространения вирусных программ. Классификация компьютерных вирусов. Комплексная система защиты информации в компьютерных системах. Контроль сбоев и отказов в работе оборудования. Резервирование технических средств. Помехоустойчивое кодирование. Коды, обнаруживающие и исправляющие ошибки. Код Хэмминга. Дублирование информации. Технология RAID.

5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Предусмотрены следующие виды контроля качества освоения конкретной дисциплины:

- текущий контроль успеваемости
- промежуточная аттестация обучающихся по дисциплине

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине оформлен в **ПРИЛОЖЕНИИ** к РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины в процессе обучения.

5.1 Паспорт фонда оценочных средств для проведения текущей аттестации по дисциплине (модулю)

№ п/п	**Контролируемые разделы (темы)**	**Код контролируемой компетенции**	**Наименование оценочного средства**
1	**Тема 1.** Информационная безопасность личности, общества и государства. Системный анализ угроз. Средства и методы защиты.	ОПК-6; ПК-8; ПК-15	Проблемные задачи, ситуационные задачи, тестирование
2	**Тема 2.** Защита информации.	ОПК-6; ПК-8; ПК-15	Проблемные задачи, ситуационные задачи, тестирование
3	**Тема 3.** Комплексная система защиты информации	ОПК-6; ПК-8; ПК-15	Проблемные задачи, ситуационные задачи, тестирование

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в процессе текущего контроля

Типовые ситуационные задачи

Задача №1

Вы – сотрудник лечебного учреждения. Ежедневно в базе данных происходит накопление большого количества информации.

1. Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.

2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Задача №2

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

1. Какие правила обеспечения информационной безопасности нарушены?

2. Какие символы должны быть использованы при записи пароля?

Задача №3

Вы – начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?

2. Какое наказание должен понести нарушитель?

Типовые проблемные задачи

Задача №1

Оцените время раскрытия пароля, если число символов в сообщении, передаваемом в систему при попытке получить доступ к ней, равно 20, 600 симв/мин – скорость передачи символов, длина пароля равна 6, число символов в алфавите – 26. Ответ дать в месяцах.

Задача № 2

Выберите необходимую длину пароля, чтобы вероятность его отгадывания не превышала 0.001 за 3 месяца. На одну попытку посылается 20 символов, скорость передачи данных равна 600 символов в минуту.

Задача №3

Зашифровать с помощью алгоритма RSA сообщение на русском языке «РИМ».

Типовые тесты

1.1. Защита информации – это …

а) комплекс мероприятий, направленных на обеспечение информационной безопасности

б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов

в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

г) все определения корректны
1.2. Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:
а) обнаружение угроз
б) пресечения и локализация угроз
в) ликвидация угроз
1.3. Возможность за приемлемое время получить требуемую информационную услугу называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации
1.4. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации
г) конфиденциальностью информации
1.5. Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации
а) доступность информации
б) целостность информации
в) предоставление информации
г) конфиденциальность информации
1.6. Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:
а) законодательного уровня
б) административного уровня
в) процедурного уровня
г) программно-технического уровня
д) программно-аппаратного уровня
1.7. Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами. Какая организация НЕ занимается вопросами формирования законодательства в сфере информационных ресурсов?
а) ISO
б) ITU
в) ANSI
г) NIST
д) NASA
е) SWIFT
ж) GISA
1.8. Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:
а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
б) Федеральная служба безопасности Российской Федерации
в) Служба внешней разведки Российской Федерации
1.9. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:
а) политикой безопасности
б) методами защиты информации
в) ограничением доступа к информации
учетными записями пользователей

1.10. Потенциальная возможность определенным образом нарушить информационную безопасность – это ….
а) угроза
б) атака
в) взлом.
2.1. Источниками угрозы называют …
а) потенциальных злоумышленников
б) компьютерные вирусы
в) глобальную сеть Интернет
2.2. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется …
а) окном безопасности
б) окном опасности
в) скользящим окном
г) окном угрозы
2.3. Ошибки программного обеспечения с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы
2.4. Ошибки администрирования системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы
2.5. Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы
2.6. Некоторая уникальная информация, позволяющая различать пользователей называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
8
г) ключ
2.7. Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ
2.8. Совокупность идентификатора и пароля пользователя называется:
а) логин пользователя
б) учетная запись пользователя
в) ключ пользователя
2.9. Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:
а) идентификацией пользователя

б) аутентификацией пользователя
в) опознанием пользователя
г) созданием учетной записи пользователя
2.10. Проверка принадлежности пользователю предъявленного им идентификатора является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) регистрацией пользователя
г) созданием учетной записи пользователя

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

Все задания, используемые для текущего контроля формирования компетенций условно можно разделить на две группы:

1 - задания, которые в силу своих особенностей могут быть реализованы только в процессе обучения на занятиях (например, ситуационные задания, дискуссия и мини-конференция в форме вебинара);

2 - задания, которые дополняют теоретические вопросы (практические задания, задания для самостоятельной работы, тесты).

Выполнение всех заданий является необходимым для формирования и контроля знаний, умений и навыком. Поэтому, в случае невыполнения заданий в процессе обучения, их необходимо «отработать» до зачета (экзамена). Вид заданий, которые необходимо выполнить для ликвидации «задолженности» определяется в индивидуальном порядке, с учетом причин невыполнения.

1. Требование к решению ситуационной, проблемной задачи (кейс-измерители)

Студент должен уметь выделить основные положения из текста задачи, которые требуют анализа и служат условиями решения. Исходя из поставленного вопроса в задаче, попытаться максимально точно определить проблему и соответственно решить ее.

Задачи должны решаться студентами письменно. При решении задач также важно правильно сформулировать и записать вопросы, начиная с более общих и, кончая частными.

Критерии оценивания – оценка учитывает методы и средства, использованные при решении ситуационной, проблемной задачи.

Оценка *«выполнено»* ставится в случае, если обучающийся показал положительные результаты в процессе решения задачи, а именно, когда обучающийся в целом выполнил задание (решил задачу), используя в полном объеме теоретические знания и практические навыки, полученные в процессе обучения.

Оценка *«не выполнено»* ставится, если обучающийся не выполнил все требования.

2. Тестирование

Является одним из средств контроля знаний обучающихся по дисциплине.

Критерии оценивания – правильный ответ на вопрос

Оценка *«отлично»* ставится в случае, если правильно выполнено 90-100% заданий

Оценка *«хорошо»* ставится, если правильно выполнено 70-89% заданий

Оценка *«удовлетворительно»* ставится в случае, если правильно выполнено 50-69% заданий

Оценка *«неудовлетворительно»* ставится, если правильно выполнено менее 50% заданий

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1 Основная учебная литература

1. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — ISBN 978-5-9585-0603-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/43183.html

2. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

3. Смышляев А.Г. Информационная безопасность. Лабораторный практикум [Электронный ресурс] : учебное пособие / А.Г. Смышляев. — Электрон. текстовые данные. — Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2015. — 102 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66655.html

6.2 Дополнительная учебная литература:

1. Горюхина Е.Ю. Информационная безопасность [Электронный ресурс] : учебное пособие / Е.Ю. Горюхина, Л.И. Литвинова, Н.В. Ткачева. — Электрон. текстовые данные. — Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72672.html

2. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. — Электрон. текстовые данные. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — 978-5-9585-0603-3. — Режим доступа: http://www.iprbookshop.ru/43183.html

6.3. Периодические издания

1. «Информационные технологии и телекоммуникации» ISSN 2307-1303
2. «Информационные технологии» ISSN 1684-640
3. «Научный результат» ISSN 2518-1092
4. «Реклама: теория и практика» ISSN2410-9622
5. «Российский журнал менеджмента» ISSN 1729-7427
6. «Экономика и математические методы» ISSN 0424-7388

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины (модуля)

1. Федеральный портал «Российское образование» http://www.edu.ru/
2. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/

8. Методические указания для обучающихся по освоению дисциплины (модуля)

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности – лекций, семинарских занятий, самостоятельной работы. При этом самостоятельную работу следует рассматривать одним из главных звеньев

полноценного высшего образования, на которую отводится значительная часть учебного времени.

Все виды занятий проводятся в форме онлайн-вебинаров с использованием современных компьютерных технологий (наличие презентации и форума для обсуждения).

В процессе изучения дисциплины студенты выполняют практические задания и промежуточные тесты. Консультирование по изучаемым темам проводится в онлайн-режиме во время проведения вебинаров и на форуме для консультаций.

Самостоятельная работа студентов складывается из следующих составляющих:

- работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
- внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;
- выполнение самостоятельных практических работ;
- подготовка к экзаменам (зачетам) непосредственно перед ними.

Для правильной организации работы необходимо учитывать порядок изучения разделов курса, находящихся в строгой логической последовательности. Поэтому хорошее усвоение одной части дисциплины является предпосылкой для успешного перехода к следующей. Задания, проблемные вопросы, предложенные для изучения дисциплины, в том числе и для самостоятельного выполнения, носят междисциплинарный характер и базируются, прежде всего, на причинно-следственных связях между компонентами окружающего нас мира. В течение семестра, необходимо подготовить рефераты (проекты) с использованием рекомендуемой основной и дополнительной литературы и сдать рефераты для проверки преподавателю. Важным составляющим в изучении данного курса является решение ситуационных задач и работа над проблемно-аналитическими заданиями, что предполагает знание соответствующей научной терминологии и т.д.

Для лучшего запоминания материала целесообразно использовать индивидуальные особенности и разные виды памяти: зрительную, слуховую, ассоциативную. Успешному запоминанию также способствует приведение ярких свидетельств и наглядных примеров. Учебный материал должен постоянно повторяться и закрепляться.

При выполнении докладов, творческих, информационных, исследовательских проектов особое внимание следует обращать на подбор источников информации и методику работы с ними.

Для успешной сдачи экзамена (зачета) рекомендуется соблюдать следующие правила:

1. Подготовка к экзамену (зачету) должна проводиться систематически, в течение всего семестра.
2. Интенсивная подготовка должна начаться не позднее, чем за месяц до экзамена.
3. Время непосредственно перед экзаменом (зачетом) лучше использовать таким образом, чтобы оставить последний день свободным для повторения курса в целом, для систематизации материала и доработки отдельных вопросов.

На экзамене высокую оценку получают студенты, использующие данные, полученные в процессе выполнения самостоятельных работ, а также использующие собственные выводы на основе изученного материала.

Учитывая значительный объем теоретического материала, студентам рекомендуется регулярное посещение и подробное конспектирование лекций.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Терминальный сервер, предоставляющий к нему доступ клиентам на базе Windows Server 2016
2. Семейство ОС Microsoft Windows

3. Libre Office свободно распространяемый офисный пакет с открытым исходным кодом

4. Информационно-справочная система: Система КонсультантПлюс (Информационный комплекс)

5. Информационно-правовое обеспечение Гарант: Электронный периодический справочник «Система ГАРАНТ» (ЭПС «Система ГАРАНТ»)

6. Антивирусная система NOD 32

7. Adobe Reader. Лицензия проприетарная свободно-распространяемая.

8. Электронная система дистанционного обучения АНОВО «Московский международный университет». https://elearn.interun.ru/login/index.php

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

1. компьютеры персональные для преподавателей с выходом в сети Интернет;
2. наушники;
3. вебкамеры;
4. колонки;
5. микрофоны.

11. Образовательные технологии, используемые при освоении дисциплины

Для освоения дисциплины используются: традиционные формы занятий – лекции (типы лекций – установочная, вводная, текущая, заключительная, обзорная; виды лекций – проблемная, визуальная, лекция конференция, лекция консультация); и семинарские (практические) занятия в интерактивные формы занятий - решение ситуационных задач и разбор конкретных ситуаций, самостоятельная работа студентов с учебными материалами, представленными в электронной системе обучения.

На учебных занятиях используются технические средства обучения: компьютер подключенный к сети Интернет и программой браузером для выхода в интернет, монитор, колонки, микрофон, веб камера, пакет программ Microsoft Office для демонстрации презентаций и медиафайлов, пакет программ для проведения вебинаров в он-лайн режиме. Тестирование обучаемых может осуществляться с использованием электронной системы дистанционного обучения, установленной на оборудовании университета.

11.1. В освоении учебной дисциплины используются следующие традиционные образовательные технологии:

- чтение проблемно-информационных лекций с использованием презентаций и трансляцией выступления лектора;
- семинарские занятия для обсуждения, дискуссий и обмена мнениями с использованием электронных систем коммуникаций(форумы, чаты);
- консультации (форумы);
- самостоятельная работа студентов с учебной литературой и первоисточниками;
- подготовка и обсуждение рефератов (проектов), презентаций (научно-исследовательская работа);
- тестирование по основным темам дисциплины.

11.2. Активные и интерактивные методы и формы обучения

Из перечня видов: («*мозговой штурм», анализ НПА, анализ проблемных ситуаций, анализ конкретных ситуаций, инциденты, имитация коллективной профессиональной деятельности, разыгрывание ролей, творческая работа, связанная с освоением дисциплины,*

ролевая игра, круглый стол, диспут, беседа, дискуссия, мини-конференция и др.) используются следующие:

- *диспут*
- *анализ проблемных, творческих заданий, ситуационных задач*
- *ролевая игра;*
- *круглый стол;*
- *мини-конференция*
- *дискуссия*
- *беседа.*

11.3. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

При организации обучения по дисциплине учитываются особенности организации взаимодействия с инвалидами и лицами с ограниченными возможностями здоровья (далее – инвалиды и лица с ОВЗ) с целью обеспечения их прав, разрабатываются адаптированные для инвалидов программы подготовки с учетом различных нозологий, виды и формы сопровождения обучения, используются специальные технические и программные средства обучения, дистанционные образовательные технологии, обеспечивается безбарьерная среда и прочее.

Выбор методов обучения определяется содержанием обучения, уровнем методического и материально- технического обеспечения, особенностями восприятия учебной информации студентов-инвалидов и студентов с ограниченными возможностями здоровья и т.д. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.