

**Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА  
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ  
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

Факультет «Высшая школа корпоративного управления»

*(наименование факультета)*

Кафедра международной коммерции

*(наименование кафедры)*

УТВЕРЖДЕНО

Декан ВШКУ

Календжян С.О.

Электронная подпись

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Б.1.В.13 Цифровая безопасность

*(индекс, наименование дисциплины в соответствии с учебным планом)*

38.03.06 Торговое дело

*(код, наименование направления подготовки)*

«Цифровизация бизнеса и электронная торговля»

*(профиль)*

Бакалавр

*(квалификация)*

Очная

*(форма обучения)*

Год набора – 2021

Москва, 2020 г.

**Автор—составитель:**К.В.Н.*(ученая степень и(или) ученое звание, должность)*Ковальчук Н.Н.*(Ф.И.О.)*

Заведующий кафедрой

международной коммерции д.э.н., профессор*(наименование кафедры)**(ученая степень и(или) ученое звание )*Саламатов В.Ю.*(Ф.И.О.)*

## СОДЕРЖАНИЕ

1.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы .....	2
2.Объем и место дисциплины в структуре образовательной программы .....	4
3.Содержание и структура дисциплины. ....	5
4.Материалы текущего контроля успеваемости обучающихся и оценочные материалы промежуточной аттестации по дисциплине .....	7
5.Методические материалы для освоения дисциплины.....	19
6.Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет".	21
6.1. Основная литература .....	21
6.2. Дополнительная литература .....	22
6.3. Нормативные правовые документы и иная правовая информация .....	22
6.4. Интернет-ресурсы .....	22
6.5. Иные источники .....	23
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы.....	23

**1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы**

1.1. Дисциплина Б.1.В.13 «Цифровая безопасность» обеспечивает овладение следующей компетенцией с учетом этапов:

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
УК ОС-8	Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций и военных конфликтов	УК ОС-8.1	Демонстрирует знание основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
		УК ОС-8.2	Создает и поддерживает безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций и военных конфликтов
ПКс ОС-3	Способен к выполнению работ и управлению работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПКс ОС-3.1	Способен осуществлять управление заинтересованными сторонами проекта
		ПКс ОС-3.2	Осуществляет адаптацию бизнес-процессов заказчика к возможностям информационной системы

1.2. В результате освоения дисциплины Б.1.В.13 «Цифровая безопасность» у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)/ профессиональные действия	Код компонента компетенции	Результаты обучения
	УК ОС-8.1	<b>на уровне знаний:</b> знать общие закономерности взаимодействия общества и человека с окружающей средой; основные законы в области экологии и охраны

		<p>окружающей среды; направления предотвращения знать принципы рационального использования природных ресурсов и охраны природы, заложенные в законодательстве и нормативных актах последствий экологического кризиса; <b>на уровне умений:</b> уметь применять экологические знания и методы в экстремальных ситуациях; применять природоохранные мероприятия и ресурсосберегающие технологии; пользоваться нормативными документами; критически оценивать отечественный и зарубежный опыт в области организации экологического взаимодействия в профессиональной сфере деятельности</p> <p><b>на уровне навыков:</b> быть способным применять в профессиональной деятельности методы обеспечения безопасности товаров, людей и окружающей среды от вредных воздействий; методы регулирования природопользования</p>
	УК ОС-8.2	<p><b>на уровне знаний:</b> - знать виды современных угроз, способы выявления и предупреждения угроз, виды чрезвычайных ситуаций, общие правила и порядок действий в нештатных и чрезвычайных ситуациях, пределы своей компетенции в рамках</p>

		<p>своей профессиональной деятельности и основных компетенций сопряженных отраслей практической деятельности, практики и стереотипы принятия управленческих решений в чрезвычайных ситуациях</p> <p><b>на уровне умений:</b></p> <ul style="list-style-type: none"> <li>- уметь находить и правильно оценивать факторы опасности для личности, общества и государства, своевременно и оперативно реагировать на возникновение факторов опасности для личности, общества</li> </ul> <p><b>на уровне навыков:</b></p> <ul style="list-style-type: none"> <li>- быть способным ориентироваться в быстро меняющейся обстановке, складывающейся при нештатных и чрезвычайных ситуациях; сохранять контроль за своими эмоциями, противостоять панике и массовому психозу, предупреждать и конструктивно разрешать конфликтные ситуации</li> </ul>
	ПКс ОС-3.1	<p><b>на уровне знаний:</b></p> <p>Основы управления изменениями</p> <p>Инструменты и методы управления заинтересованными сторонами проекта</p> <p>Технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии</p> <p>Технологии подготовки и проведения презентаций</p> <p>Коммуникационное оборудование</p> <p>Сетевые протоколы</p> <p>Основы современных операционных систем</p> <p>Основы современных систем управления базами</p>

		<p>данных Устройство и функционирование современных ИС Современные стандарты информационного взаимодействия систем <b>на уровне умений:</b> Проводить презентации Проводить переговоры Работать с записями по качеству (в том числе с корректирующими действиями, предупреждающими действиями, запросами на исправление несоответствий) <b>на уровне навыков:</b> Управление ожиданиями заинтересованных сторон проекта Инициирование запросов на изменения (в том числе запросов на корректирующие действия, на предупреждающие действия, на исправление несоответствий)</p>
	ПКс ОС-3.2	<p><b>на уровне знаний:</b> Возможности типовой ИС Инструменты и методы моделирования бизнес- процессов в ИС Технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии Технологии подготовки и проведения презентаций Основы управления организационными изменениями Основы современных систем управления базами данных Устройство и функционирование современных ИС <b>на уровне умений:</b> Проводить презентации</p>

		Проводить интервьюирование Анализировать исходную документацию Анализировать функциональные разрывы <b>на уровне навыков:</b> Сбор исходных данных у заказчика Моделирование бизнес-процессов в ИС Анализ (функциональных разрывов и корректировка на его основе существующей модели бизнес-процессов Согласование с заказчиком предлагаемых изменений Утверждение у заказчика предлагаемых изменений
--	--	---

## 2.Объем и место дисциплины в структуре ОП ВО

Дисциплина Б.1.В.13 «Цифровая безопасность» в соответствии с учебным планом направления подготовки 38.03.06 «Торговое дело», профиль «Цифровизация бизнеса и электронная торговля» изучается в 6-м семестре на 3-м курсе качестве дисциплины вариативной части. Дисциплина реализуется с применением дистанционных образовательных технологий (далее - ДОТ).

Освоение дисциплины Б.1.В.13 «Цифровая безопасность» базируется на сумме знаний и навыков, полученных студентами в ходе изучения таких дисциплин, как Б1.О.13 «Коммерческая деятельность» (2 курс 3 семестр), Б1.В.01 Введение в профессию (1 курс 1 семестр), Б1.В.03 «Стандартизация, метрология, подтверждение соответствия» и др.

Наименования последующих учебных дисциплин, для которых разделы дисциплины Б.1.В.13 «Цифровая безопасность» является предшествующей: Б1.В.ДВ.12.01 Международный маркетинг / International Marketing, Б1.В.ДВ.12.02, Международный менеджмент / International Management.

Общая трудоемкость дисциплины 2 зачетных единицы (72/54 часа).

По дисциплине Б.1.В.13 «Цифровая безопасность» выделяется (академический час./астрономич.час.):

на контактную работу с преподавателем выделяется 32/24 час, в том числе:

- лекции – 16/12

- практические занятия – 16/12

на самостоятельную работу обучающихся – 40/31

Форма промежуточной аттестации – зачет.

### Регламент распределения видов работ по дисциплине с ДОТ

Данная дисциплина реализуется с применением дистанционных образовательных технологий (ДОТ). Распределение видов учебной работы, форматов текущего контроля представлены в таблице:



Вид учебной работы	Формат проведения
Практические занятия	Частично с применением ДОТ
Самостоятельная работа	Частично с применением ДОТ
Промежуточная аттестация	Частично с применением ДОТ
Формы текущего контроля	Формат проведения
Тест, реферат	Частично с применением ДОТ. Возможно использование системы дистанционного обучения (СДО)

Доступ к системе дистанционных образовательных осуществляется каждым обучающимся самостоятельно с любого устройства на портале: <https://lms.ranepa.ru> (для дисциплин, реализуемых согласно Приложению к договору о сетевой форме реализации РАНХиГС) и <https://distanty.ru>. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате. Все формы текущего контроля, проводимые в системе дистанционного обучения, оцениваются в системе дистанционного обучения. Доступ к методическим материалам предоставляется в течение всего семестра. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется на ограниченное время согласно регламенту дисциплины, опубликованному в СДО. Преподаватель оценивает выполненные обучающимся работы после окончания срока выполнения

### 3.Содержание и структура дисциплины

#### Структура дисциплины

#### Очная форма обучения

Таблица 1

№ п/п	Наименование тем (разделов)	Объем дисциплины, час./астрономич.час.					Форма текущего контроля успеваемости**  , промежуточно й аттестации	
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					СР/Д ОТ
			Л/Д ОТ*	ЛР	ПЗ/Д ОТ	КСР		
Тема 1	Концепция информационной безопасности.	12	2/2		2/2		8/8	Т
Тема 2	Угрозы информации.	16	4		4		8	Р
Тема 3	Виды возможных нарушений информационной системы	12	2/2		2/2		8/8	Т
Тема 4	Безопасность информации информационных систем.	16	4		4		8	Т
Тема 5	Методы и средства защиты компьютерной информации.	16	4		4		8	Р
Промежуточная аттестация								Зачет
Всего		72/54	16/12		16/12		40/31	

№ п/п	Наименование тем (разделов)	Объем дисциплины, час./астрономич.час.						Форма текущего контроля успеваемости**  , промежуточно й аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР/Д ОТ	
			Л/Д ОТ*	ЛР	ПЗ/Д ОТ	КСР		

Примечание:

\*В данной РПД описано содержание лекционного и практического курса в СД

\*\*Формы текущего контроля успеваемости: Т – тест, Р-реферат

### Содержание дисциплины

#### Тема 1. Концепция информационной безопасности.

Актуальность информационной безопасности. Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Лицензирование и сертификация в области защиты информации. Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования. Основные нормативные руководящие документы. Международные стандарты информационного обмена. Критерии безопасности компьютерных систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.

#### Тема 2. Угрозы информации

Информационная безопасность сетей. Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ. Способы совершения компьютерных преступлений.

Уязвимость сети Интернет. Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

#### Тема 3. Виды возможных нарушений информационной системы

Компьютерные преступления. Классификация компьютерных преступлений. Виды противников или «нарушителей». Вредоносные программы. Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам. Вирусы. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.

#### Тема 4. Информационная безопасность информационных систем

Теория информационной безопасности информационных систем. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Криптографические способы защиты информации. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.

Организация информационной безопасности компании. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в

национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

### **Тема 5. Методы и средства защиты компьютерной информации**

Обеспечения информационной безопасности. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Контроль доступа к информации. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Методы и средства защиты информации. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Антивирусное ПО. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

## **4.Материалы текущего контроля успеваемости обучающегося и оценочные средства промежуточной аттестации по дисциплине**

### **4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.**

4.1.1. В ходе реализации дисциплины Б.1.В.13 «Цифровая безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

<b>Тема (раздел)</b>	<b>Методы текущего контроля успеваемости</b>
Концепция информационной безопасности.	Тест
Угрозы информации.	Реферат
Виды возможных нарушений информационной системы	Тест
Безопасность информации информационных систем.	Тест
Методы и средства защиты компьютерной информации.	Реферат

– при занятиях самостоятельной работой: самостоятельная работа обучающихся является одной из форм самообразования, роль преподавателя при этом заключается в оказании консультативной и направляющей помощи обучающемуся с применением ДОТ в СДО.

**4.1.2. Зачет проводится в форме ответов на вопросы билета в виде устного опроса с элементами тестирования с применением ДОТ в СДО.**

### **4.2. Материалы текущего контроля успеваемости.**

#### **Тест по дисциплине**

1. Задание.

В каком году в России появились первые преступления с использованием компьютерной техники (были похищены 125,5 тыс. долл. США во Внешэкономбанке)?

1. 1988;
2. 1991;
3. 1994;
4. 1997;

5. 2002.

2. Задание.

Сертификации подлежат:

1. средства криптографической защиты информации;
2. средства выявления закладных устройств и программных закладок;
3. защищенные технические средства обработки информации;
4. защищенные информационные системы и комплексы телекоммуникаций;
5. все вышеперечисленные средства.

3. Задание.

В стандарте США «Оранжевой книге» фундаментальное требование, которое относится к группе Стратегия:

1. индивидуальные субъекты должны идентифицироваться;
2. контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность;
3. необходимо иметь явную и хорошо определенную систему обеспечения безопасности;
4. вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет того, что система обеспечивает выполнение изложенных требований;
5. гарантированно защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

4. Задание.

Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

5. Задание.

Хакер – это:

1. лицо, которое взламывает интрасеть в познавательных целях;
2. мошенник, рассылающий свои послания в надежде обмануть наивных и жадных;
3. лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
4. плохой игрок в гольф, дилетант;
5. мошенники, которые обманым путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

6. Задание.

Активный перехват информации - это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

7. Задание.

Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

8. Задание.

По среде обитания классические вирусы разделяются:

1. на паразитические;
2. на компаньоны;
3. на файловые;
4. на ссылки;
5. на перезаписывающие.

9. Задание.

Шифрование методом подстановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;
2. символы шифруемого текста последовательно складываются символами некоторой специальной последовательности;
3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;
4. символы шифруемого текста заменяются другими символами, затыми из одного или нескольких алфавитов;
5. замена слов и предложений исходной информации шифрованными.

10. Задание.

Метод защиты информации ограничение доступа заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;
2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;
3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

11. Задание.

Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

12. Задание.

Спам, периодически проводящий рассылки не рекламных сообщений:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

## 13. Задание.

Способ защиты информации, существующей в виде электромагнитного сигнала, зависит от ...

1. среды распространения электромагнитного сигнала;
2. длины волны сигнала;
3. наличия или отсутствия специальной линии связи;
4. типа линии связи;
5. форм воздействия на информацию или ее носитель;
6. предполагаемого способа нападения на информацию.

## 14. Задание.

Попытка одного субъекта выдать себя за другого - это:

1. пассивная атака;
2. модификация потока данных»;
3. фальсификация;
4. повторное использование;
5. отказ в обслуживании.

## 15. Задание.

В качестве биометрических признаков, которые могут быть использованы при идентификации субъекта доступа, можно выделить:

1. должностное лицо;
2. терминал;
3. распечатка;
4. форма и размеры лица;
5. оператор.

## 16. Задание.

Антивирус просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

### Примерная тематика рефератов:

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
7. Информационная безопасность (по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
12. Составление инструкции по обработке и хранению конфиденциальных документов.
13. Направления и методы защиты документов на бумажных носителях.
14. Направления и методы защиты машиночитаемых документов.

15. Архивное хранение конфиденциальных документов.
16. Направления и методы защиты аудио- и визуальных документов.
17. Порядок подбора персонала для работы с конфиденциальной информацией.
18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
28. Назначение, виды, структура и технология функционирования системы защиты информации.
29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
30. Аналитическая работа по выявлению каналов утечки информации фирмы.
31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
32. Направления и методы защиты профессиональной тайны.
33. Направления и методы защиты служебной тайны.
34. Направления и методы защиты персональных данных о гражданах.
35. Методы защиты личной и семейной тайны.
36. Построение и функционирование защищенного документооборота.
37. Защита секретов в дореволюционной России.
38. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

#### **Перечень тем, изучаемых студентами самостоятельно:**

1. Актуальность информационной безопасности.
2. Лицензирование и сертификация в области защиты информации.
3. Основные нормативные руководящие документы.
4. Информационная безопасность сетей.
5. Способы совершения компьютерных преступлений.
6. Уязвимость сети Интернет.
7. Компьютерные преступления.
8. Вредоносные программы.
9. Вирусы.
10. Теория информационной безопасности информационных систем.
11. Криптографические способы защиты информации.
12. Организация информационной безопасности компании.
13. Обеспечения информационной безопасности.
14. Контроль доступа к информации.
15. Методы и средства защиты информации.

## 16. Антивирусное ПО.

**4.3. Оценочные материалы для промежуточной аттестации****4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций на различных этапах их формирования**

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
УК ОС-8	Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций и военных конфликтов	УК ОС-8.1	Демонстрирует знание основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
		УК ОС-8.2	Создает и поддерживает безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций и военных конфликтов
ПКс ОС-3	Способен к выполнению работ и управлению работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПКс ОС-3.1	Способен осуществлять управление заинтересованными сторонами проекта
		ПКс ОС-3.2	Осуществляет адаптацию бизнес-процессов заказчика к возможностям информационной системы

Компонент компетенции	Индикатор оценивания <i>Что делает обучающийся (какие действия способен выполнить), подтверждая освоение компетенции</i>	Критерий оценивания <i>Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.</i>
УК ОС-8.1	Демонстрирует знание основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для	Умеет применять экологические знания и методы в экстремальных ситуациях; применяет природоохранные мероприятия и ресурсосберегающие технологии; пользуется нормативными



	<p>сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций. Общие закономерности взаимодействия общества и человека с окружающей средой; основные законы в области экологии и охраны окружающей среды; направления предотвращения последствий экологического кризиса; принципы рационального использования природных ресурсов и охраны природы, заложенные в законодательстве и нормативных актах.</p>	<p>документами; критически оценивает отечественный и зарубежный опыт в области организации экологического взаимодействия в профессиональной сфере деятельности; способен применять в профессиональной деятельности методы обеспечения безопасности товаров, людей и окружающей среды от вредных воздействий; методы регулирования природопользования.</p>
УК ОС-8.2	<p>Демонстрирует знание основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.</p>	<p>Умеет находить и правильно оценивать факторы опасности для личности, общества и государства, своевременно и оперативно реагирует на возникновение факторов опасности для личности, общества. Способен ориентироваться в быстро меняющейся обстановке, складывающейся при нештатных и чрезвычайных ситуациях; сохраняет контроль за своими эмоциями, противостоит панике и массовому психозу, предупреждает и конструктивно разрешает конфликтные ситуации.</p>
ПКс ОС-3.1	<p>Управление ожиданиями заинтересованных сторон проекта Использовать инструменты и методы управления заинтересованными сторонами проекта</p>	<p>Способен самостоятельно инициировать и осуществлять управление заинтересованными сторонами проекта с использованием инструментов и методов управления заинтересованными сторонами</p>
ПКс ОС-3.2	<p>Организация сбора данных о бизнес-процессах заказчика Проведение анализа и формулирование предложения</p>	<p>Самостоятельно проводит анализ и формулирует предложения по адаптации бизнес-процессов заказчика к возможностям</p>

	заказчику по изменению его бизнес-процессов с использованием инструментов и методов моделирования бизнес-процессов в ИС	информационной системы
--	---	------------------------

#### 4.3.2. Типовые оценочные материалы

##### Вопросы промежуточной аттестации (зачет)

1. Необходимость защиты информации.
2. Сохранность защищаемой информации: сущность и основные виды. Сущность понятия "защищаемая информация".
3. Разновидность защищаемой информации и ее носителей.
4. Компьютерные вирусы и их классификация.
5. Характеристика антивирусного программного обеспечения.
6. Способы ограничения доступа к информации.
7. Предотвращение технических сбоев оборудования.
8. Методы взлома компьютерных систем. Атаки на уровне систем управления базами данных.
9. Методы взлома компьютерных систем. Атаки на уровне операционной системы.
10. Методы взлома компьютерных систем. Атаки на уровне сетевого программного обеспечения.
11. Методы взлома компьютерных систем. Защита системы от взлома.
12. Характеристика троянских программ. Возникновение троянских программ.
13. Характеристика троянских программ. Где и как часто встречаются троянские программы.
14. Характеристика троянских программ. Распознавание троянской программы.
15. Программные закладки и их классификация.
16. Модели воздействия программных закладок на компьютеры.
17. Защита системы от программных закладок.
18. Разновидность ПЗ (имитаторы, фильтры и заместители).
19. Парольные взломщики. Защита системы от клавиатурных шпионов. Парольная защита операционных систем.
20. Взлом парольной защиты ОС UNIX.
21. Взлом парольной защиты ОС Windows NT.
22. Информационная безопасность компьютерной сети. Характеристика и назначение сканеров.
23. Информационная безопасность компьютерной сети. Характеристика и назначение анализаторов протоколов.
24. Информационная безопасность компьютерной сети. Защита от анализаторов протоколов.
25. Значение и современные методы шифрования информации в информатизированном обществе.
26. Методологические основы технологии шифрования программными средствами.
27. Применение и проблемы стандартизации криптографических алгоритмов.
28. Средства безопасности ОС Windows 2000. Понятия и термины защиты данных. Характеристики безопасности.
29. Средства безопасности ОС Windows 2000. Применение шифрования с открытым и закрытым ключами.

30. Средства безопасности ОС Windows 2000. Алгоритмы и компоненты Windows 2000 обеспечивающие шифрование данных.
31. Средства безопасности ОС Windows 2000. Протокол аутентификации Kerberos. Основы применения протокола Kerberos.
32. Средства безопасности ОС Windows 2000. Характеристика протоколов обмена сообщениями.
33. Аутентификация протокола Kerberos в доменах ОС Windows 2000.
34. Шифрующая файловая система EPS и ее архитектура.
35. Средства безопасности ОС Windows 2000. Применение EPS в ОС Windows 2000.
36. Средства безопасности ОС Windows 2000. Шифрование файлов и каталогов. Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок.
37. Средства безопасности ОС Windows 2000. Архивация и восстановление зашифрованных файлов на другом компьютере.
38. Средства безопасности ОС Windows 2000. Восстановление данных, зашифрованных с помощью неизвестного личного ключа.
39. Протокол безопасности IP в ОС Windows 2000. Характеристика средств безопасности протокола IP.
40. Архитектура протокола безопасности IP в ОС Windows 2000.
41. Разработка плана безопасности IP в ОС Windows 2000.
42. Администрирование безопасности в ОС Windows 2000.
43. Использование сертификатов для обеспечения безопасности в ОС Windows 2000. Хранилища сертификатов безопасности.
44. Планирование мероприятий по защите информации.
45. Характеристика программных средств шифрования информации.
46. Применение средства криптографической защиты информации Pretty good Privacy (PGP).

Для оценки степени освоения компетенции используются следующие шкалы:

**Шкала 1. Оценка сформированности отдельных элементов компетенций**

Обозначения		Формулировка требований		
Цифр.	Оценка	к степени сформированности компетенции		
		Знать	Уметь	Владеть
1	Не зачтено	Отсутствие знаний	Отсутствие умений	Отсутствие навыков
2	Не зачтено	Фрагментарные знания	Частично освоенное умение	Фрагментарное применение
3	Зачтено	Общие, но не структурированные знания	В целом успешное, но не систематически осуществляемое умение	В целом успешное, но не систематическое применение
4	Зачтено	Сформированные, но	В целом успешное,	В целом успешное,

		содержащие отдельные пробелы знания	но содержащие отдельные пробелы умение	но содержащее отдельные пробелы применение навыков
5	Зачтено	Сформированные систематические знания	Сформированное умение	Успешное и систематическое применение навыков

### **Шкала 2. Комплексная оценка сформированности знаний, умений и владений**

Оценка	Результаты обучения
Зачтено	<p>Оценка «зачтено» выставляется студенту, если он:</p> <p><b>На уровне знаний:</b>  Нормативные правовые акты, регламентирующие внешнеэкономическую деятельность.  Стандарты и требования внешних рынков к продукции.  Методы и основы системного анализа внешнеэкономической информации.  Правила оформления документации по внешнеторговому контракту.  Порядок документооборота в организации.  Условия внешнеторгового контракта.  Этика делового общения и правила ведения переговоров.  Маркетинг и особенности ценообразования.  Английский язык (пороговый уровень В1).  Основы экономической теории.  Основы трудового законодательства Российской Федерации.  Правила административного документооборота. Нормативные правовые акты, регламентирующие внешнеэкономическую деятельность.  Международные договоры в сфере внешнеэкономической деятельности.  Стандарты и требования внешних рынков к продукции.  Методы и инструменты работы с базами данных внешних рынков.  Правила оформления документации по внешнеторговому контракту.  Порядок документооборота в организации.  Основы риск-менеджмента во внешнеэкономической деятельности.  Условия внешнеторгового контракта.</p> <p><b>На уровне умений:</b>  Использует вычислительную, копировальную, вспомогательную технику и различные виды телекоммуникационной связи.  Ведет базы данных документации по внешнеторговому контракту.  Оформляет документацию по внешнеэкономической деятельности в соответствии с требованиями законодательства Российской Федерации и международных актов.  Выстраивает взаимодействие с подразделениями организации для организации документооборота по внешнеторговому контракту.  Формирует реестр документации по внешнеторговому контракту.  Регистрирует документацию по внешнеторговому контракту.  Осуществляет учет и систематизацию хранения документации по внешнеторговому контракту.</p>

	<p>Формирует дела и сдает в архив документации по внешнеторговому контракту.</p> <p>Составляет и оформляет отчеты по результатам проверок документации по внешнеторговому контракту. Анализирует и систематизирует информацию о процессе исполнения обязательств участниками внешнеторгового контракта.</p> <p>Ведет деловую переписку с иностранными партнерами для получения информации об исполнении обязательств по внешнеторговому контракту.</p> <p>Взаимодействует с подразделениями организации и сторонними организациями для осуществления контроля исполнения контрактных обязательств.</p> <p>Составляет отчеты и готовит предложения по исполнению обязательств по внешнеторговому контракту.</p> <p><b>Осуществляет:</b></p> <p>Мониторинг отклонений от выполнения обязательств по внешнеторговому контракту.</p> <p>Организацию процедуры приемки отдельных этапов исполнения внешнеторгового контракта.</p> <p>Привлечение к участию и контроль участия исполнителей в зависимости от этапов реализации внешнеторгового контракта.</p> <p>Документальное оформление отклонений от выполнения обязательств по внешнеторговому контракту и организация претензионной работы.</p> <p>Подготовку предложений по применению мер ответственности и совершению соответствующих действий в случае нарушения обязательств по внешнеторговому контракту.</p> <p><b>на уровне навыков:</b></p> <p>Организацию процедуры приемки отдельных этапов исполнения внешнеторгового контракта.</p> <p>Привлечение к участию и контроль участия исполнителей в зависимости от этапов реализации внешнеторгового контракта.</p> <p>Документальное оформление отклонений от выполнения обязательств по внешнеторговому контракту и организация претензионной работы.</p> <p>Подготовку предложений по применению мер ответственности и совершению соответствующих действий в случае нарушения обязательств по внешнеторговому контракту.</p>
«Не удовлетворительно»	В ответе существенные ошибки в основных аспектах темы.

#### 4.4. Методические материалы

Занятия по дисциплине представлены следующими видами работы: лекции, практические занятия и самостоятельная работа студентов.

На практических занятиях студенты изучают понятийный аппарат; выполняют задания, связанные с применением категориального аппарата и при анализе профессиональных проблем; приобретают навыки публичного выступления и дискуссии.

В рамках самостоятельной работы студенты готовятся к семинарским занятиям, осуществляют подготовку к промежуточной аттестации.

Текущая аттестация по дисциплине проводится в форме опроса и контрольных мероприятий по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

- учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);
- степень усвоения теоретических знаний;
- уровень овладения практическими умениями и навыками по всем видам учебной работы;
- результаты самостоятельной работы

Активность студента по дисциплине оценивается по его выступлениям на практических занятиях.

Оценка **работы студента на практических занятиях** осуществляется по следующим критериям:

- Отлично - активное участие в обсуждении проблем каждого семинара, самостоятельность ответов, свободное владение материалом, полные и аргументированные ответы на вопросы семинара, участие в дискуссиях, твёрдое знание лекционного материала, обязательной и рекомендованной дополнительной литературы, регулярная посещаемость занятий.
- Хорошо - недостаточно полное раскрытие некоторых вопросов темы, незначительные ошибки в формулировке категорий и понятий, меньшая активность на семинарах, неполное знание дополнительной литературы, хорошая посещаемость.
- Удовлетворительно - ответы отражают в целом понимание темы, знание содержания основных категорий и понятий, знакомство с лекционным материалом и рекомендованной основной литературой, недостаточная активность на занятиях, оставляющая желать лучшего посещаемость.
- Неудовлетворительно - пассивность на семинарах, частая неготовность при ответах на вопросы, плохая посещаемость, отсутствие качеств, указанных выше для получения более высоких оценок.

### **Критерии оценивания устного опроса**

Развернутый ответ студента должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях.

Критерии оценивания включают в себя:

- 1) полноту и правильность ответа;
- 2) степень осознанности, понимания изученного;
- 3) языковое оформление ответа.

Оценка «отлично» ставится, если студент полно излагает материал (отвечает на вопрос), дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка.

Оценка «хорошо» ставится, если студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.

Оценка «удовлетворительно» ставится, если студент обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.

Оценка «неудовлетворительно» ставится, если студент обнаруживает незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «2» отмечает такие недостатки в подготовке, которые являются серьезным препятствием к успешному овладению последующим материалом.

### **Критерии оценки эссе**

Оценка «отлично» предполагает:

- полученные результаты полностью соответствуют поставленной цели,
- проведен детальный анализ источников с привлечением фрагментов первоисточников по теме,
- выводы автора самостоятельны и аргументированы,
- содержание работы полностью отражает узловые проблемы темы,
- оформление работы полностью отвечает всем требованиям.

Оценка «хорошо» ставится в том случае, если:

- полученные результаты преимущественно соответствуют поставленной цели и задачам,
- обоснована актуальность темы,
- в процессе анализа литературы отобран и проанализирован широкий круг источников,
- полученные результаты в целом логичны, доказательны и систематизированы,
- оформление работы в целом соответствует существующим требованиям,
- высказана личностная позиция по теме.

Оценка «удовлетворительно» предполагает:

- полученные результаты в значительной степени соответствуют поставленной цели, в частности,
- обоснована актуальность избранной темы,
- в процессе анализа литературы отобраны наиболее важные источники,
- материал подан логически непротиворечиво,
- требования по оформлению работы в основном выполнены.

## **5.Методические материалы для освоения дисциплины**

Процедуры и средства оценивания элементов компетенций  
по дисциплине

Процедура проведения	Средство оценивания				
	Текущий контроль				Промежуточный контроль
	Выполнение устных заданий	Выполнение письменных заданий в тестовой форме	Выполнение практических заданий	Выполнение рефератов и докладов	Зачет в устной форме
Продолжительность контроля	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	В соответствии с принятыми нормами времени
Форма проведения контроля	Устный опрос	Письменный опрос	Устный опрос	Письменная форма с презентацией	В устной форме
Вид проверочного задания	Устные вопросы	Письменные задания	Практические задания	Письменный опрос	Зачет
Форма отчета	Устные ответы	Ответы в письменной форме	Ответы в письменной форме	Ответы в письменной (по рефератам)	Ответы в устной форме
Раздаточный материал	есть	Справочная литература	Справочная литература	Справочная литература	Справочная литература

Практические занятия дисциплины предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций с проведением контрольных мероприятий. С целью обеспечения успешного обучения студент должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

- внимательно прочитайте материал предыдущей лекции;



- узнайте тему предстоящей лекции (по тематическому плану, по информации лектора);
- ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
- постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
- запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к практическим занятиям:

- внимательно прочитайте материал лекций, относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям;
- выпишите основные термины;
- ответьте на контрольные вопросы по семинарским занятиям, готовьтесь дать развернутый ответ на каждый из вопросов;
- уясните, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до семинарского занятия) во время текущих консультаций преподавателя;
- готовиться можно индивидуально, парами или в составе малой группы, последние являются эффективными формами работы;
- рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.

**Вопросы для самостоятельного изучения тем дисциплины**

**Перечень тем, изучаемых студентами самостоятельно:**

1. Актуальность информационной безопасности.
2. Лицензирование и сертификация в области защиты информации.
3. Основные нормативные руководящие документы.
4. Информационная безопасность сетей.
5. Способы совершения компьютерных преступлений.
6. Уязвимость сети Интернет.
7. Компьютерные преступления.
8. Вредоносные программы.
9. Вирусы.
10. Теория информационной безопасности информационных систем.
11. Криптографические способы защиты информации.
12. Организация информационной безопасности компании.
13. Обеспечения информационной безопасности.
14. Контроль доступа к информации.
15. Методы и средства защиты информации.
16. Антивирусное ПО.

Подготовка к зачету. К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период сессии, как правило, показывают не слишком удовлетворительные результаты. В самом начале изучения учебной дисциплины познакомьтесь со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем формируемых знаний и умений, которыми студент должен овладеть;
- тематическими планами лекций, семинарских занятий;

- контрольными мероприятиями;
- учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов для зачета.

После этого у вас должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

## **6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"**

### **6.1. Основная литература**

1. Артемов А.В. Информационная безопасность. МАБИВ, 2014.  
<http://www.iprbookshop.ru/33430>
2. Милославская Н.Г. Управление рисками информационной безопасности. Горячая линия, 2012. <http://www.iprbookshop.ru/12060>
3. Шаньгин В.Ф. Информационная безопасность и защита информации. ДМК Пресс, 2014.  
<http://www.iprbookshop.ru/29257>

### **6.2. Дополнительная литература**

1. Белов Е.Б. Основы информационной безопасности. Горячая линия-Телеком, 2011.  
<http://www.iprbookshop.ru/12014.html>
2. Данжани Н, Кларк Д. Средства сетевой безопасности/ Пер с англ.- СПб.: КУДИЦ-ПРЕСС, 2007.-368с.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264с.
4. Максим М., Поллино Д. Безопасность беспроводных сетей - М.: ДМК Пресс, 2008. - 283 с. - <http://www.biblioclub.ru>
5. Торстейнсон П. Криптография и безопасность в технологии .NET/П. Торстейнсон, Г.А. Ганеш; пер. с англ. - М: БИНОМ. Лаборатория знаний, 2007. - 479с.

### **6.3. Нормативные правовые документы и иная правовая информация**

1. Постановление Правительства РФ от 02.03.2019 N 234 "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" (вместе с "Положением о системе управления реализацией национальной программы "Цифровая экономика Российской Федерации").

### **6.4. Интернет-ресурсы**

1. [www.nnir.ru](http://www.nnir.ru) / - Российская национальная библиотека
2. [www.nns.ru](http://www.nns.ru) / - Национальная электронная библиотека
3. [www.rsi.ru](http://www.rsi.ru) / - Российская государственная библиотека
4. [www.yandex.ru](http://www.yandex.ru) / - Поисковая система
5. <http://www.consultant.ru/> - Консультант плюс
6. <http://www.garant.ru/> - Гарант
7. БДИ: Безопасность, Достоверность, Информация.
8. Безопасность информации.
9. Бизнес и безопасность в России.
10. Вопросы защиты информации (Всероссийский научно-исследовательский институт межотраслевой информации).
11. Делопроизводство (ЗАО «Бизнес-Школа «Интел-Синтез»).

12. Документоведение, документационное обеспечение управления (библиографический указатель и экспресс-информация ОЦНТИДАД ВНИИДАД ГАС РФ)
13. Защита информации. Конфидент.
14. Мир безопасности.
15. Системы безопасности (Компания «Гротек»).
16. Секретарское дело (ЗАО «Бизнес-Школа «Интел-Синтез»).
17. Секьюрити.
18. Телохранитель.
19. Частный сыск, охрана, безопасность (Интерпол Москва, Издательский дом «Мир безопасности»).
20. Records Management Quarterly
21. Security Management
22. Security Industry and Product New

#### 6.5. Иные источники

1. Журнал «Современная торговля»
2. «Торгово-экономический журнал»
3. Журнал «Цифровая экономика»

### 7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для проведения лекционных, практических занятий групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы по дисциплине необходимо следующее

#### материально-техническое обеспечение:

- программы, обеспечивающие навигацию в сети Интернет: «Google chrome»;
- программы, демонстрации видео материалов: проигрыватель «Windows Media»;
- программы для демонстрации и создания презентаций: «Microsoft Power Point».

Все виды занятий, контроль и самостоятельная работа проводятся с частичным использованием ДОТ. Лекционные материалы, практические задания, материалы для самостоятельной работы, средства текущего контроля и промежуточной аттестации размещены в СДО: <https://lms.ranepa.ru>

#### Информационные справочные системы:

1. Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: <http://www.consultant.ru/>
2. Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: <http://www.garant.ru/>
3. Научная библиотека РАНХиГС. URL: <http://lib.ranepa.ru/>;
4. Научная электронная библиотека eLibrary.ru. URL: <http://elibrary.ru/defaultx.asp>;
5. Национальная электронная библиотека. URL: <http://rusneb.ru>;
6. Российская государственная библиотека. URL: [www.rsl.ru](http://www.rsl.ru);
7. Российская национальная библиотека. URL: <http://nlr.ru/>;
8. Электронная библиотека Grebennikon. URL: <http://grebennikon.ru/>;
9. Электронно-библиотечная система Издательства «Лань». URL: <http://e.lanbook.com>;
10. Электронно-библиотечная система ЮРАЙТ. URL: <http://www.biblio-online.ru/>;
11. Электронно-библиотечная система IPRbooks. URL: <http://www.iprbookshop.ru/>.

**Для работы в СДО РАНХиГС необходимо следующее:**

1. Авторизоваться на сайте СДО <https://lms.ranepa.ru>  
(Авторизацию нужно провести с использованием **СВОЕЙ** учетной записи РАНХиГС. В качестве логина используется префикс корпоративной электронной почты);
2. По электронной почте Вы получите информацию о предоставлении доступа к курсу в системе дистанционного обучения РАНХиГС.  
(Для просмотра содержимого курса, доступ к которому Вам предоставлен, достаточно:
  - перейти на сайт <https://lms.ranepa.ru>;
  - авторизоваться, используя данные своей учетной записи;выбрать курс, кликнув на его название).