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

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
КАФЕДРА СИСТЕМНОГО АНАЛИЗА И ИНФОРМАТИКИ

УТВЕРЖДЕНА
решением кафедры Системного анализа и информатики
Протокол от «03 » сентября 2020 г. № 01

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.13 Основы кибербезопасности
(индекс и наименование дисциплины (модуля), в соответствии с учебным планом)

09.03.03 Прикладная информатика _
(код и наименование направления подготовки (специальности))

"Веб-разработка"
направленность (профиль/специализация)

бакалавр
квалификация

очная форма обучения
форма(ы) обучения

Год набора - 2021

Москва, 2020 г.

Автор составитель:

Профессор кафедры Системного анализа и информатики
д-р техн. наук, профессор Ромашкова О.Н.

Заведующий кафедрой
Системного анализа и информатики _____ Маруев С.А.
(*наименование кафедры)* *(ученая степень и(или) ученое звание)* *(подпись)* *(Ф.И.О.)*

СОДЕРЖАНИЕ

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

2. Объем и место дисциплины в структуре образовательной программы…….....

3. Содержание и структура дисциплины …….

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине …….

5. Методические указания для обучающихся по освоению дисциплины…….....

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине……..…….

6.1. Основная литература……..……..……..……

6.2. Дополнительная литература……...……..……..

6.3. Учебно-методическое обеспечение самостоятельной работы……

6.4. Нормативные правовые документы…….……..……

6.5. Интернет-ресурсы…….……..……

6.6. Иные источники…….…….…….…

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

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

1.1. Дисциплина Б1.В.13 «Основы кибербезопасности» обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	*Код этапа освоения компетенции*	Наименование этапа освоения компетенции
УК ОС–2	Способность разработать проект на основе оценки ресурсов и ограничений	УК ОС–2.1 УК ОС–2.2 УК ОС–2.3	УК-2.1. Способен применять необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.2. Способен анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ. УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
ПКр – 1	Способен проводить обследование организаций, выявлять информационные потребности	ПКр-1.1	Знает принципы разработки планов коммуникаций с заказчиком в проектах создания (модификации) ИС

	пользователей, формировать требования к информационной системе	ПКр-1.2 ПКр-1.3	Умеет организовывать заключение договоров на выполняемые работы, связанные с ИС Владеет навыками организации заключения договоров на выполняемые работы, связанные с ИС

1.2. В результате освоения дисциплины у обучаемых должны быть сформированы:

ОТФ/ТФ *(при наличии профстандарта)*/ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	УК ОС–2.1 УК ОС–2.2 УК ОС–2.3	на уровне знаний*:* необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ. на уровне навыков *(типовые действия выполняются автоматически, без воспроизведения алгоритма):* Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
06.015 СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННЫМ СИСТЕМАМ С Выполнение	ПКр-1.1 ПКр-1.2 ПКр-1.3	на уровне знаний: Знает принципы разработки планов коммуникаций с заказчиком в проектах создания (модификации) ИС Знает порядок подготовки и

работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы С/03.6 Планирование коммуникаций с заказчиком в проектах создания (модификации) и ввода ИС в эксплуатацию С/42.6 Организация заключения договоров на выполняемые работы, связанных с ИС		формирования документации для заключения договоров на выполняемые работы, связанные с ИС
		на уровне умений: Умеет организовывать заключение договоров на выполняемые работы, связанные с ИС
		на уровне навыков: Владеет навыками выстраивания коммуникаций с заказчиком в проектах создания (модификации) и ввода ИС в эксплуатацию Владеет навыками организации заключения договоров на выполняемые работы, связанные с ИС

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Объем дисциплины Б1.В.13 «Основы кибербезопасности» в ЗЕ и академических/астрономических часах составляет 2 ЗЕ (72/54 ч). Дисциплина реализуется с применением дистанционных образовательных технологий.

Количество академических/астрономических часов по очной дистанционной форме обучения, выделенных на контактную работу 16/12 часа (в т.ч. лекц. – 0 ч., практ. – 16/12 ч.); на самостоятельную работу обучающихся - 56/42 часов.

Место дисциплины в структуре ОП ВО

В соответствии с учебным планом дисциплина Б1.В.13 «Основы кибербезопасности» относится к вариативной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика и изучается на 4 курсе в 8 семестре.
Дисциплины опирается на объём знаний информатики, вычислительных машин, сетей и систем телекоммуникаций, программирования;
Форма промежуточной аттестации для очной формы обучения –зачет.

3. Содержание и структура дисциплины

№ п/п	Наименование тем и/или разделов	Объем дисциплины, час.			Форма текущего контроля успеваемости**,
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий	СР	

			Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	К С Р		промежуточной аттестации ***
Тема 1	Введение. Безопасность функционирования современной организации и технологий.	12		-	2	-	10	О, К, Т
Тема 2	Современная доктрина информационной безопасности Российской Федерации.	12		-	2	-	10	Т, О
Тема 3	Международные стандарты информационного обмена. Модели безопасности и их применение.	12		-	2	-	10	О, Р, Т
Тема 4	Сущность и задачи обеспечения информационной безопасности.	12			2		10	Т, О, КР
Тема 5	Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.	12			4		8	Т, О, КР
Тема 6	Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.	12			4		8	Т, О, КР
Промежуточная аттестация		За						За
Всего:		**72/54**		-	16/12		56/42	

Примечание:

** – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом;*

*** – формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), реферат (Р).*

**** - разработчик указывает необходимые формы промежуточной аттестации зачет (За).*

Содержание дисциплины

Тема 1. Введение. Безопасность функционирования современной организации и технологий.

Введение. Предмет и задачи дисциплины. Значение и место дисциплины в подготовке специалистов в области прикладных аспектов информатики и информационных технологий по защите информации от несанкционированных воздействий и обеспечения достоверности и целостности при ее обработке в информационно-телекоммуникационных системах. Научная и учебная взаимосвязь дисциплины с другими дисциплинами, изучаемыми в высшем учебном заведении.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения практических и семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Форма проверки знаний. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения дисциплины.

Актуальность проблемы обеспечения информационной безопасности в торгово-экономических структурах, потенциально возможные несанкционированные воздействия на информационную инфраструктуру торгово-экономической деятельности, информационный криминал. Статистические показатели состояния информационной безопасности информационной инфраструктуры торгово-экономической деятельности, динамика ее развития.

Составляющие воздействий на информационную инфраструктуру государства: информационная война, информационный терроризм, информационный криминал. Понятие конкурентной разведки.

Тема 2. Современная доктрина информационной безопасности Российской Федерации.

Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Значение информационной безопасности и ее место в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации.

Международные стандарты информационного обмена, правовые основы защиты государственной, коммерческой, служебной, процессуальной, профессиональной тайны и информации персонального характера. Федеральные Законы Российской Федерации по обеспечению информационной безопасности в информационных технологиях, Доктрина Информационной безопасности Российской Федерации, Концепция Национальной Безопасности Российской Федерации, нормативные и руководящие документы, Постановления Правительства Российской Федерации по проблемам обеспечения информационной безопасности, Руководящие документы и инструкции Федеральной службы по техническому и экспортному контролю (ФСТЭК), Приказы и распоряжения ФСБ РФ, Ведомственные приказы и распоряжения.

Тема 3. Международные стандарты информационного обмена. Модели безопасности и их применение.

Безопасность в сетях Internet и Intranet. Технология безопасности: межсетевые экраны (Межсетевые экраны прикладного уровня, межсетевые экраны с пакетной фильтрацией, гибридные межсетевые экраны). Разработка конфигурации межсетевого экрана: Архитектура 1 – системы за пределами; архитектура 2 – один межсетевой экран; архитектура 3 – двойные межсетевые экраны. Безопасность виртуальных частных сетей (VPN).
Модели безопасности: модели разграничения доступа; модели разграничения доступа, построенные по принципу предоставления прав; модели дискретного доступа; модели мандатного доступа; модель Белла и Лападула; специализированные модели; вероятностные модели; информационные модели; модели контроля целостности; Модель Биба; модель Кларка-Вилсона. Модели анализа безопасности программного обеспечения.

Тема 4. Сущность и задачи обеспечения информационной безопасности.
Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Агрегация информационных ресурсов с точки зрения информационной безопасности. Классификация угроз информационной безопасности. Информационная безопасность компьютерных систем. Основные понятия и определения. Безопасность автоматизированных систем обработки информации. Доступ к информации (санкционированный, несанкционированный), разграничение доступа, конфиденциальность данных, угрозы безопасности, защита информации, политика безопасности
Основные виды угроз безопасности компьютерным системам: нарушения конфиденциальности информации, нарушения целостности информации, нарушения работоспособности системы. Каналы несанкционированного доступа. Способы несанкционированного доступа: перехват паролей, «маскарад», незаконное использование привилегий.

Тема 5. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.
«Врожденные слабости» наиболее распространенных служб Internet. Основные компоненты межсетевых экранов: фильтрующие маршрутизаторы, шлюзы сетевого уровня, шлюзы прикладного уровня. Аутентификация пользователей как основной компонент межсетевых экранов. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей. Программные методы защиты сетевых технологий в Internet структурах.

Тема 6. Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.
Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования, Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования. Привязка к внешним (добавляемым) элементам. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации

4.1.1. В ходе реализации дисциплины Б1.В.13 «Основы кибербезопасности» используются следующие методы текущего контроля успеваемости обучающихся[1]:

Тема и/или раздел		Методы текущего контроля успеваемости в аудитории	Методы текущего контроля успеваемости с применением ДОТ
Тема 1	Введение. Безопасность функционирования современной организации и технологий.	Опрос, коллоквиум	Тестирование
Тема 2	Современная доктрина информационной безопасности Российской Федерации.	Опрос	Тестирование
Тема 3	Международные стандарты информационного обмена. Модели безопасности и их применение.	Опрос	Тестирование, Реферат
Тема 4	Сущность и задачи обеспечения информационной безопасности.	Опрос	Тестирование, КР
Тема 5	Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.	Опрос	Тестирование, КР
Тема 6	Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.	Опрос	Тестирование, КР

4.1.2. Зачет проводится с применением следующих методов (средств):

Зачет проводится с применением следующих методов (средств): без использования дистанционных образовательных технологий в форме выполнения практических заданий на компьютере с использованием инструментария веб-технологий, а именно LAMP/LEMP/FAMP/FEMP. HTML, CSS, JavaScript, TypeScript. PHP 7, MySQL. Symfony, Laravel, Zend Framework, Yii, Kohana. LESS, SASS, PostCSS. Gulp, Webpack, Babel. БЭМ. React, Vue, Angular. Git, Mercurial. Jenkins, Gitlab, Project Expert и Microsoft Project.

[1] *Разработчик программы самостоятельно выбирает форму заполнения пункта 1.1.*

4.2. Материалы текущего контроля успеваемости обучающихся.

Преподаватель оценивает уровень подготовленности обучающихся к занятию по следующим показателям:

- опрос - устные ответы на вопросы преподавателя по теме занятия. Критерии оценивания устных ответов на вопросы преподавателя по теме занятия - правильность и полнота ответа;

- выступление с презентациями по реферату темы №3 отчетные доклады с презентациями по предлагаемым темам. Критериями оценивания реферата:

степень усвоения понятий и категорий по теме;
умение работать с документальными и литературными источниками;
грамотность изложения материала;
самостоятельность работы, наличие собственной обоснованной позиции;
Критерии оценивания презентации
оформлен титульный лист;
количество слайдов соответствует требованиям (мин.10 слайдов);
использование дополнительных эффектов в Power point, инфографики;
слайды представлены в логической последовательности.

- выполнение практических заданий на компьютере. Критерии оценивания выполнения заданий:

правильность выполнения задания;
оригинальность решений;
полнота выполнения задания.

- количество правильных ответов при тестировании. Критерии оценки выполненных студентами тестов определяются преподавателем самостоятельно. Рекомендуются следующие критерии оценки:

1. 85% – 100% правильных ответов – «отлично»;
2. 66% – 84% правильных ответов – «хорошо»;
3. 50% – 65% правильных ответов – «удовлетворительно»;
4. менее 50% правильных ответов – «неудовлетворительно».

- выполнение контрольной работы на компьютере. Критерии оценивания обучаемого в ходе выполнения:

3 балла – задание выполнено полностью, студент показал отличные знания, проявил активную позицию при ответах на вопросы, отлично владеет инструментарием

2 балла – задание выполнено с недочетами, студент показал хорошие знания, хорошо ответил на вопросы, владеет инструментарием;

1 балл – задание выполнено не полностью, студент показал слабые знания, не полностью ответил на вопросы, слабо владеет инструментарием;

0 баллов – задание не выполнено, студент не знает, не может ответить на вопросы, не владеет инструментарием.

Оценка знаний, умений, навыков проводится на основе балльно-рейтинговой системы 70% из 100% (70 баллов из 100) - вклад по результатам посещаемости занятий, активности на занятиях, выступления с докладами, выполнение всех практических заданий и контрольных работ, правильность ответов в ходе тестирования и контрольных практических заданий.

Детализация баллов и критерии оценки текущего контроля успеваемости

утверждается на заседании кафедры.

Примеры типовых оценочных материалов исходя из методов текущего контроля успеваемости

Типовые вопросы для проведения опроса

1. Основные виды угроз безопасности компьютерных систем.
2. Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.
3. Структурные составляющие гипотетической модели нарушителя.
4. Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.
5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях.
6. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.
7. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.

Вварианты тестовых заданий

Вопрос:
Кто является основным ответственным за определение уровня классификации информации?
Варианты ответа:

1. Руководитель среднего звена
2. Высшее руководство
3. Владелец
4. Пользователь

Вопрос:
Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Варианты ответа:

1. Сотрудники
2. Хакеры
3. Атакующие
4. Контрагенты (лица, работающие по договору)

Вопрос:
Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
Варианты ответа:

1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

3. Улучшить контроль за безопасностью этой информации
4. Снизить уровень классификации этой информации

Вопрос:
Что самое главное должно продумать руководство при классификации данных?
Варианты ответа:

1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2. Необходимый уровень доступности, целостности и конфиденциальности
3. Оценить уровень риска и отменить контрмеры
4. Управление доступом, которое должно защищать данные

Вопрос:
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
Варианты ответа:

1. Владельцы данных
2. Пользователи
3. Администраторы
4. Руководство

Вопрос:
Что такое процедура?
Варианты ответа:

1. Правила использования программного и аппаратного обеспечения в компании
2. Пошаговая инструкция по выполнению задачи
3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
4. Обязательные действия

Вопрос:
Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Варианты ответа:

1. Поддержка высшего руководства
2. Эффективные защитные меры и методы их внедрения
3. Актуальные и адекватные политики и процедуры безопасности
4. Проведение тренингов по безопасности для всех сотрудников

Вопрос:
Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Варианты ответа:

1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

2. Когда риски не могут быть приняты во внимание по политическим соображениям
3. Когда необходимые защитные меры слишком сложны
4. Когда стоимость контрмер превышает ценность актива и потенциальные потери

Вопрос:
Что такое политики безопасности?
Варианты ответа:

1. Пошаговые инструкции по выполнению задач безопасности
2. Общие руководящие требования по достижению определенного уровня безопасности
3. Широкие, высокоуровневые заявления руководства
4. Детализированные документы по обработке инцидентов безопасности

Вопрос:
Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Варианты ответа:

1. Анализ рисков
2. Анализ затрат / выгоды
3. Результаты ALE
4. Выявление уязвимостей и угроз, являющихся причиной риска

Вопрос:
Что лучше всего описывает цель расчета ALE?
Варианты ответа:

1. Количественно оценить уровень безопасности среды
2. Оценить возможные потери для каждой контрмеры
3. Количественно оценить затраты / выгоды
4. Оценить потенциальные потери от угрозы в год

Вопрос:
Тактическое планирование – это:
Варианты ответа:

1. Среднесрочное планирование
2. Долгосрочное планирование
3. Ежедневное планирование
4. Планирование на 6 месяцев

Вопрос:
Что является определением воздействия (exposure) на безопасность?
Варианты ответа:

1. Нечто, приводящее к ущербу от угрозы
2. Любая потенциальная опасность для информации или систем
3. Любой недостаток или отсутствие информационной безопасности
4. Потенциальные потери от угрозы

Вопрос:
Эффективная программа безопасности требует сбалансированного применения:
Варианты ответа:

1. Технических и нетехнических методов
2. Контрмер и защитных механизмов
3. Физической безопасности и технических средств защиты
4. Процедур безопасности и шифрования

Вопрос:
Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
Варианты ответа:

1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. Уровень доверия, обеспечиваемый механизмом безопасности
4. Соотношение затрат / выгод

Вопрос:
Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
Варианты ответа:

1. Только военные имеют настоящую безопасность
2. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
3. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
4. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

Вопрос:
Как рассчитать остаточный риск?
Варианты ответа:

1. Угрозы х Риски х Ценность актива
2. (Угрозы х Ценность актива х Уязвимости) х Риски
3. SLE х Частоту = ALE
4. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

Вопрос:
Что из перечисленного не является целью проведения анализа рисков?
Варианты ответа:

1. Делегирование полномочий
2. Количественная оценка воздействия потенциальных угроз
3. Выявление рисков
4. Определение баланса между воздействием риска и стоимостью необходимых контрмер

Варианты контрольных работ

Средства защиты от несанкционированного доступа (НСД):
-Средства авторизации;
-Мандатное управление доступом;
-Избирательное управление доступом;
-Управление доступом на основе ролей;
-журналирование (называется еще и аудит).
Системы анализа и моделирования информационных потоков (CASE-системы).
Системы мониторинга сетей:
-Системы обнаружения и предотвращения вторжений (IDS/IPS).
Системы предотвращения утечек конфиденциальной информации (DLP-системы).
Анализаторы протоколов.
Антивирусные средства.
Межсетевые экраны.
Криптографические средства:
-Шифрование;
-Цифровая подпись.
Системы резервного копирования.
Системы бесперебойного питания:
-Источники бесперебойного питания;
– Резервирование нагрузки;
-Генераторы напряжения.
Системы аутентификации:
-Пароль;
-Сертификат;
-Биометрия.
Средства предотвращения взлома корпусов и краж оборудования.
Средства контроля доступа в помещения.
Инструментальные средства анализа систем защиты:
– Программный мониторинговый продукт.

Вопросы и задания для самостоятельной подготовки

1. Политика безопасности.
2. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.
3. Этапы построения системы защиты автоматизированных информационных систем.
4. Составляющие отдельных этапов.
5. Основные задачи методов защиты информации в автоматизированных информационных системах.
6. Принципы системы защиты информации в АСОИ.

Примерные темы для написания рефератов

1. – Защита объектов информационной системы;
2. – Защита процессов, процедур и программ обработки информации;
3. – Защита каналов связи;
4. – Подавление побочных электромагнитных излучений;
5. – Управление системой защиты.

6. Определение информационных и технических ресурсов, подлежащих защите;
7. – Выявление полного множества потенциально возможных угроз и каналов утечки информации;
8. – Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
9. – Определение требований к системе защиты;
10. – Осуществление выбора средств защиты информации и их характеристик;
11. – Внедрение и организация использования выбранных мер, способов и средств защиты;
12. – Осуществление контроля целостности и управление системой защиты.

Шкала оценивания

Уровень освоения компетенций по дисциплине «**Основы кибербезопасности**» определяется:

- знанием содержания процессов самоорганизации и самообразования, их особенностей и технологий реализации, исходя из целей совершенствования профессиональной деятельности;
- умением найти необходимую информацию, самостоятельно решать стандартные задачи профессиональной деятельности, выполнять действия в изученной последовательности, в том числе в новых условиях, на новом содержании;
- навыками использования современных информационных визуальных цифровых технологий и способами их реализации;
- способностью самостоятельно строить процесс овладения информацией, отобранной и структурированной для выполнения профессиональной деятельности;
- умением обеспечивать сохранность здоровья себе и сотрудникам при выполнении профессиональных задач.

Низкий «неудовлетворительно/незачет» - компетенция не освоена или освоена в недостаточной мере. Студент не знает, либо знает на слабом уровне теоретический материал по дисциплине. Не владеет терминологией и основными понятиями из профессиональной сферы или называет неуверенно, с ошибками.

Пороговый (базовый) «удовлетворительно/зачет» - компетенция освоена удовлетворительно, но достаточно. Студент освоил основную базу теоретических знаний. Владеет терминологией и основными понятиями из профессиональной сферы.

Продвинутый «хорошо/зачет» - компетенция освоена достаточно хорошо. Студент знает теоретический материал по дисциплине, умеет применить эти знания на практике. Чётко и ясно формулирует свои мысли. Знает специальную и публицистическую литературу по профессиональным вопросам.

Высокий «отлично/зачет» - компетенция освоена в полной мере или на продвинутом уровне. Студент знает теоретический материал, умеет применить эти знания на практике и имеет опыт в профессионально-практической деятельности. Приводит актуальные примеры из сферы профессиональной деятельности; демонстрирует способности к нестандартной интерпретации поставленного вопроса.

Наименование темы (раздела)	Показатели оценивания	Критерии оценивания	Оценка (баллы)
Введение. Безопасность функционирования современной организации и технологий.	Вопрос на зачете	Зачет	Удовлетворительно -41 -60, жорошо 61-80, отлично 81-100, Не зачтено – 40-0
Современная доктрина информационной безопасности Российской Федерации.	Вопрос на зачете	Зачет	Удовлетворительно -41 -60, жорошо 61-80, отлично 81-100, Не зачтено – 40-0
Международные стандарты информационного обмена. Модели безопасности и их применение.	Вопрос на зачете, Р	Зачет	Удовлетворительно -41 -60, жорошо 61-80, отлично 81-100, Не зачтено – 40-0
Сущность и задачи обеспечения информационной безопасности.	Вопрос на зачете, КР	Зачет	Удовлетворительно -41 -60, жорошо 61-80, отлично 81-100, Не зачтено – 40-0
Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.	Вопрос на зачете, КР	Зачет	Удовлетворительно -41 -60, жорошо 61-80, отлично 81-100, Не зачтено – 40-0
Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет.	Вопрос на зачете, КР	Зачет	Удовлетворительно -41 -60, жорошо 61-80, отлично 81-100, Не зачтено – 40-0

В начале каждого семестра до студентов доводится информация о структуре набора баллов за семестр:

Максимальный балл за посещение и активную работу в семестре – 60 баллов.

Максимальный балл за каждую контрольную работу – 7 баллов.

Максимальный балл за каждую решенную задачу – 7 баллов.

Максимальный балл за реферат по выбранной теме – 12 баллов.

Вес текущих контрольных работ различен и зависит от этапов формирования компетенций. Решение и постановка прикладных задач, формирующих компетенции, выше, чем простое владение информационными технологиями.

В результате каждый студент четко представляет свое число набранных баллов.

Текущая аттестация обучаемых. Текущая аттестация обучаемых по дисциплине «Основы кибербезопасности» проводится в соответствии с Уставом

Академии, Положением о текущей аттестации студентов по программам ВО и является обязательной.

Текущая аттестация по дисциплине «Основы кибербезопасности» 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 практических занятий по аттестуемой дисциплине);

уровень овладения практическими умениями и навыками по всем видам учебной работы, уровень освоения компетенций;

результаты самостоятельной работы.

Активность обучаемого на занятиях оценивается по скорости и правильности выполнения практических заданий на компьютерах.

Кроме того, оценивание обучаемого проводится на контрольной неделе в соответствии с распоряжением проректора по учебной работе. Оценивание обучаемого на контрольной неделе проводится преподавателем независимо от наличия или отсутствия обучаемого (по уважительной или неуважительной причине) на занятии. Оценка носит комплексный характер и учитывает достижения обучаемого по основным компонентам учебного процесса за текущий период.

Оценивание обучаемого на занятиях осуществляется с использованием балльно-рейтинговой системы в соответствии с технологической картой дисциплины. Оценивание обучаемого на контрольной неделе также осуществляется по балльно-рейтинговой системе с выставлением оценок в ведомости и указанием количества пропущенных занятий.

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	*Код этапа освоения компетенции*	Наименование этапа освоения компетенции
УК ОС–2	Способность разработать проект на основе оценки ресурсов и ограничений	УК ОС–2.1 УК ОС–2.2	УК-2.1. Способен применять необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.2. Способен анализировать

		УК ОС–2.3	альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ. УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
ПКр – 1	Способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	ПКр-1.1 ПКр-1.2 ПКр-1.3	Знает принципы разработки планов коммуникаций с заказчиком в проектах создания (модификации) ИС Умеет организовывать заключение договоров на выполняемые работы, связанные с ИС Владеет навыками организации заключения договоров на выполняемые работы, связанные с ИС

ОТФ/ТФ *(при наличии профстандарта)*/ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	УК ОС–2.1	на уровне знаний*:*

	УК ОС–2.2	необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.
		Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.
	УК ОС–2.3	на уровне навыков *(типовые действия выполняются автоматически, без воспроизведения алгоритма):* Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
06.015 СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННЫМ СИСТЕМАМ С Выполнение работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы С/03.6 Планирование коммуникаций с заказчиком в проектах создания (модификации) и ввода ИС в эксплуатацию С/42.6 Организация заключения договоров на выполняемые работы, связанных с ИС	ПКр-1.1 ПКр-1.2 ПКр-1.3	на уровне знаний: Знает принципы разработки планов коммуникаций с заказчиком в проектах создания (модификации) ИС Знает порядок подготовки и формирования документации для заключения договоров на выполняемые работы, связанные с ИС
		на уровне умений: Умеет организовывать заключение договоров на выполняемые работы, связанные с ИС
		на уровне навыков: Владеет навыками выстраивания коммуникаций с заказчиком в проектах создания (модификации) и ввода ИС в эксплуатацию Владеет навыками организации заключения договоров на выполняемые работы, связанные с ИС

Промежуточная аттестация обучаемых по дисциплине «Основы кибербезопасности» проводится в соответствии с Уставом Академии, Положением о промежуточной аттестации студентов по программам ВО. Промежуточная аттестация по дисциплине «Основы кибербезопасности» проводится в соответствии с Учебным планом в 8 семестре в форме зачета. Обучаемые допускаются к зачету по

дисциплине в случае выполнения ими учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных программой дисциплины по формам текущего контроля и выполненных рефератах. В случае наличия учебной задолженности обучаемый отрабатывает пропущенные занятия в соответствии с требованиями преподавателя. Зачет принимает ведущий преподаватель.

Оценка знаний обучаемого на зачет складывается из:

ответа на один вопрос зачета;

выполнения всех текущих контрольных работ;

защиты рефератов по третьей теме;

Оценка знаний обучаемого на зачет носит комплексный характер, является балльной и определяется его:

– ответом на зачет с оценкойе;
– учебными достижениями в семестровый период.

Знания, умения, навыки обучаемого на зачете оцениваются оценками: «зачтено», «незачтено». Кроме того, обучаемому выставляется оценка в соответствии с балльно-рейтинговой системой. Основой для определения оценки служит уровень усвоения обучаемыми материала, предусмотренного данной рабочей программой.

4.3.2 Типовые оценочные средства

Темы коллоквиумов по дисциплине «Основы кибербезопасности»

Коллоквиум организуется для проверки самостоятельной работы по теме, предложенную преподавателем (обучаемым). Коллоквиум позволяет автору научиться четко и грамотно формулировать мысли, структурировать информацию, использовать основные категории анализа, выделять причинно-следственные связи, иллюстрировать понятия соответствующими примерами, аргументировать свои выводы; овладеть научным стилем речи. Коллоквиум содержит: четкое изложение сути поставленной проблемы, включать самостоятельно проведенный анализ этой проблемы с использованием концепций и аналитического инструментария, рассматриваемого в рамках дисциплины, выводы, обобщающие авторскую позицию по поставленной проблеме.

1. комитет государственной думы по безопасности;
2. – совет безопасности России;
3. – федеральная служба по техническому и экспортному контролю (ФСТЭК);
4. – федеральная служба безопасности России (ФСБ России);
5. -министерство внутренних дел Российской Федерации (МВД России); федеральная служба надзора в сфере информационных технологий и массовых коммуникаций (Роскомнадзор).
6. Службы, организующие защиту информации на уровне предприятия: служба экономической безопасности; служба безопасности персонала (Режимный отдел); отдел кадров; служба информационной безопасности.
7. Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.
8. Политика безопасности информационно-телекоммуникационных технологий – правила, директивы, сложившаяся практика, которые определяют, как

в пределах организации, её информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию.

9. – Защита объектов информационной системы;
10. – Защита процессов, процедур и программ обработки информации;
11. – Защита каналов связи;
12. – Подавление побочных электромагнитных излучений;
13. – Управление системой защиты.

Критерии оценки коллоквиумов:

Оценка «удовлетворительно» предполагает, что полученные результаты в значительной степени соответствуют поставленной цели (цель работы достигнута в основном). Обоснована актуальность работы. В процессе анализа литературы отобраны наиболее важные источники, продемонстрировано понимание решаемой проблемы. Выбраны адекватные цели научный подход, методы, процедуры. Они в значительной степени реализованы в работе. Выводы имеют наглядный и проверяемый характер. Требования по оформлению работы в основном выполнены.

Оценка «хорошо» ставится, когда полученные результаты преимущественносоответствуют поставленной цели и задачам. Обоснована практическая и теоретическая актуальность работы. В процессе анализа литературы отобран и проанализирован широкий круг теоретических и эмпирических источников. Выбраны и обоснованы применяемые научные подходы, методы и процедуры. Полученные результаты в целом логичны, доказательны и систематизированы. Оформление работы в целом соответствует существующим требованиям.

Оценка «отлично» предполагает: полученные результаты полностью соответствуют поставленной цели. Обоснована практическая и теоретическая значимость работы. Проведен детальный анализ теоретических и эмпирических источников, выводы автора самостоятельны и аргументированы. Выбраны и подробно описаны применяемые в работе научные подходы, методы и процедуры. Содержание работы полностью отражает узловые проблемы темы, исследовательская часть (в курсовой работе) выполнена самостоятельно, методологически корректно и содержит достоверные и интересные выводы и положения. Оформление работы полностью отвечает всем требованиям

Вопросы к зачету по дисциплине «Основы кибербезопасности»

1. Понятие «Информационная безопасность». Основные методологические и нормативно-правовые документы по информационной безопасности.
2. Основные понятия по защите компьютерных данных. Доступ к информации, санкционированный доступ, несанкционированный доступ, конфиденциальность данных, субъект и объект информационных технологий, доступность компонента или ресурса системы, угроза безопасности автоматизированной информационной системе, ущерб безопасности, уязвимость АСОИ, атака на компьютерную систему, политика безопасности.
3. Основные виды угроз безопасности компьютерных систем, Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.
4. Структурные составляющие гипотетической модели нарушителя, Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.

5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.

6. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.

7. Политика безопасности. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.

8. Этапы построения системы защиты автоматизированных информационных систем. Составляющие отдельных этапов.

9. Основные задачи методов защиты информации в автоматизированных информационных системах. Принципы системы защиты информации в АСОИ.

10. Принципы криптографической защиты информации. Криптология, криптография, стеганография, криптоанализ. Три класса криптографических систем.

11. Традиционные симметричные криптографические системы. Ключ шифрования данных, шифры криптографической защиты данных: шифры перестановок, шифры замены, шифры гаммирования, шифры, основанные на аналитических преобразованиях шифруемых данных.

12. Шифрующие таблицы без ключевого слова.

13. Табличное шифрование методов перестановки по ключевому слову или фразе, задающими перестановку.

14. Табличное шифрование методом двойной перестановки.

15. Шифр Цезаря.

16. Метод аффинной системы подстановок Цезаря.

17. Система шифрования Цезаря с ключевым словом.

18. Одноалфавитные монограммные таблицы Трисимуса.

19. Шифры сложной замены. Шифр Гронсфельда.

20. Система шифрования Вернама.

21. Шифрование методом гаммирования.

22. Современные симметричные криптосистемы.

23. Стандарт шифрования DES.

24. Алгоритм шифрования IDEA.

25. Отечественный стандарт шифрования данных ГОСТ 28147-89.

26. Концепция криптографической системы с открытым ключом. Система асимметричной криптографической системы.

27. Однонаправленные Хэш-функции.

28. Криптографическая система шифрования данных RSA.

29. Процедура шифрования и расширения данных в криптографической системе RSA.

30. Безопасность и быстродействие криптографической системы RSA.

31. Схема шифрования Полига-Хелмана.

32. Схема шифрования Эль Гамаля.

33. Комбинированный метод шифрования данных.

34. Электронная цифровая подпись. Правовые основы электронной цифровой подписи. Федеральный закон РФ «Об электронной подписи.

35. Проблема аутентификации данных и электронная цифровая подпись.

36. Однонаправленные Хэш-функции. Алгоритмы электронной цифровой подписи.

37. Алгоритм ЭЦП RSA.

38. Алгоритм ЭЦП Эль Гамаля.

39. Алгоритм ЭПЦ DSA.

40. Отечественный стандарт электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001.

41. Идентификация и проверка подлинности электронных документов и пользователей компьютерных технологий.

42. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверки подлинности пользователей.

43. Процедура «рукопожатия».

44. Протоколы аутентификации с нулевой передачей знаний.

45. Параллельная идентификация с нулевой передачей знаний.

46. Система идентификации Гиллоу-Куискуотера.

47. Управление криптографическими ключами. Генерация и хранение ключей.

48. Иерархия ключей шифрования данных в корпоративных компьютерных системах.

49. Распределение ключей в корпоративных компьютерных системах. Использование одного или нескольких центров распределении ключей. Прямой обмен сеансовыми ключами между санкционированными пользователями.

50. Механизм запроса – ответа в сетевых технологиях, механизм отметки времени.

51. Распределение ключей с участием Центра распределении ключей.

52. Протокол для симметричных криптосистем с использованием отметки времени.

53. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.

54. Алгоритм открытого распределения ключей Диффи-Хелмана.

55. Протокол SKIP управления криптоключами.

56. Аутентификация пользователей как основной компонент межсетевых экранов.

57. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей.

58. Программные методы защиты сетевых технологий в Internet структурах.

59. Защита данных в электронных платежных системах.

60. Принципы функционирования электронных платежных систем.

61. Электронные пластиковые карты. Пассивные и активные пластиковые карты. Основные типы активных пластиковых карт: карты-счетчики, карты с памятью, карты с микропроцессором, карты с контактным считыванием, карты с индукционным считванием.

62. Персональный идентификационный номер (PIN). Обеспечение безопасности электронно-платежной системы POS (Point-of-Sale), схема функционирования POS.

63. Обеспечение безопасности банкоматов в электронных платежных системах, схема обмена сообщениями между банкоматом и хост-ЭВМ банка рои идентификации и платеже, схема прохождения данных с PIN клиента между банкоматом, банком-эквайером и банком-эмитентом.

64. Универсальная платежная система UEPS (Universal Electronic Payment System), состав и архитектура платежной системы, распределение ключей и паролей, цикл платежной транзакции.

65. Торговые терминалы, формирование сессионных ключей, эмиссия карточек, разграничение ответственности между банками-участниками общей

платежной системы, двойное шифрование записи о транзакции на ключах банка-эквайера и банка-эмитента.

66. Обеспечение безопасности электронных платежей через сеть Internet.

67. Авторизация и шифрование финансовой информации в сети Internet.

68. Протоколы шифрования SSL (Secure Socket Layer) и SET (Secure Electronic Transactions), использование сертификатов.

69. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

70. Средства и системы управления контролем доступа в компьютерных технологиях.

71. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа. Разграничения доступа к файлам.

72. Защита программного продукта от несанкционированного копирования.

73. Несанкционированное копирование программ как тип НСД.

74. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.

75. Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования.

76. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования.

77. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения.

78. Методы «водяных знаков» и методы «отпечатков пальцев».

79. Защита программного продукта от изучения.

Критерии оценки компетенций

Промежуточная аттестация обучаемых по дисциплине «Основы кибербезопасности» проводится в соответствии с Уставом Академии, Положением о промежуточной аттестации студентов по программам ВПО. Промежуточная аттестация по дисциплине «Основы кибербезопасности» проводится в соответствии с Учебным планом в 8 семестре в форме зачета. Обучаемые допускаются к зачету по дисциплине в случае выполнения ими учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных программой дисциплины по формам текущего контроля и выполненных заданий. В случае наличия учебной задолженности обучаемый отрабатывает пропущенные занятия в соответствии с требованиями преподавателя. Оценка знаний обучаемого на зачете носит комплексный характер, является балльной и определяется его:

- ответом на зачете;
- учебными достижениями в семестровый период.

Темы рефератов по дисциплине «Основы кибербезопасности»

1. Изучение и обратное проектирование программного обеспечения: понятие изучения и обратного проектирования программного обеспечения, способы изучения программного обеспечения (статическое и динамическое изучение), временная надежность (невозможность обеспечения гарантированной надежности).

2. Задачи защиты программного продукта от изучения и способы их решений: защита от отладки, динамическое преобразование кода,

3. Итеративный программный замок А. Долгина

4. Принцип ловушек и принцип избыточного кода, защита от дизассемблирования, принцип внешней загрузки файлов, динамическая модификация программы, защита от трассировки по прерываниям.

5. Аспекты защиты от исследования: способы ассоцианирования защиты и программного обеспечения, оценка надежности защиты от отладки.

6. Защита от разрушающих программных воздействий.

7. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия.

8. Понятие изолированной программной среды.

Критерии оценки рефератов:

Оценка «удовлетворительно» предполагает, что полученные результаты в значительной степени соответствуют поставленной цели (цель работы достигнута в основном). Обоснована актуальность работы. В процессе анализа литературы отобраны наиболее важные источники, продемонстрировано понимание решаемой проблемы. Выбраны адекватные цели научный подход, методы, процедуры. Они в значительной степени реализованы в работе. Выводы имеют наглядный и проверяемый характер. Требования по оформлению работы в основном выполнены.

Оценка «хорошо» ставится, когда полученные результаты преимущественносоответствуют поставленной цели и задачам. Обоснована практическая и теоретическая актуальность работы. В процессе анализа литературы отобран и проанализирован широкий круг теоретических и эмпирических источников. Выбраны и обоснованы применяемые научные подходы, методы и процедуры. Полученные результаты в целом логичны, доказательны и систематизированы. Оформление работы в целом соответствует существующим требованиям.

Оценка «отлично» предполагает: полученные результаты полностью соответствуют поставленной цели. Обоснована практическая и теоретическая значимость работы. Проведен детальный анализ теоретических и эмпирических источников, выводы автора самостоятельны и аргументированы. Выбраны и подробно описаны применяемые в работе научные подходы, методы и процедуры. Содержание работы полностью отражает узловые проблемы темы, исследовательская часть (в курсовой работе) выполнена самостоятельно, методологически корректно и содержит достоверные и интересные выводы и положения. Оформление работы полностью отвечает всем требованиям

Шкала оценивания по результатам зачета с оценкой:

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
	неудовлетворительно	удовлетворительно	хорошо	отлично
УК ОС - 2 – 6. Способен анализировать и разрабатывать организационно-технические и экономические процессы с применением методов системного анализа и математического моделирования.				
на уровне знаний: основных	Не знает возможности применения	Демонстрирует частичные знания	Демонстрирует системные знания основных	Проявляет высокий уровень

принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры	основных законов естественнонаучных дисциплин, а также современных информационно-коммуникационных технологий	основных законов естественнонаучн ых дисциплин, а также современных информационно-коммуникационных технологий для решения комплекса задач на основе информационной и библиографической культуры	законов естественнонаучных дисциплин, а также современных информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры	знаний всего учебного материала
на уровне умений *(типовые действия выполняются по заданному алгоритму)*: применять информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры; решать стандартные задачи профессиональн	Не умеет применять знания на практике для разработки алгоритмов решения задач	Демонстрирует частичный уровень умений выявлять экономическую сущность задач	Демонстрирует достаточный уровень умений выявлять экономическую сущность задач, использовать экономико-математический аппарат для разработки алгоритмов решения задач	Демонстрирует высокий уровень умений для разработки алгоритмов решения задач

ой деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				
на уровне навыков *(типовые действия выполняются автоматически, без воспроизведения алгоритма):* подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности; Владеет навыками научно-исследовательской работы с учетом требований информационной безопасности	Не владеет практическими навыками обработки текстовой, табличной и графической информации	Владеет практическими навыками работы на компьютере и использования стандартных информационно-коммуникационных технологий частично	Владеет практическими навыками работы на компьютере и использования стандартных информационно-коммуникационных технологий достаточно свободно	Владеет практическим и навыками работы на компьютере и использования стандартных информационно-коммуникационных технологий на высоком уровне
ПКр – 1. Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы				
на уровне знаний: принципов разработки планов коммуникаций	Не знает как проводить описание прикладных процессов и	Демонстрирует частичные знания в описании прикладных процессов и	Демонстрирует системные знания в описании прикладных процессов и	Проявляет высокий уровень знаний всего учебного материала

с заказчиком в проектах создания (модификации) ИС; Знает принципы, методы и стандарты разработки архитектуры ИС; Знает основные методологии и средства проектирования и дизайна ИС; Знает основные методологии и средства разработки баз данных ИС; Знает правила и стандарты разработки пользовательской документации к ИС; Знает принципы и приемы командообразования.	информационного обеспечения решения разработки планов коммуникаций с заказчиком в проектах создания (модификации) ИС; методологии и средства проектирования и дизайна ИС; правила и стандарты разработки пользовательской документации к ИС; принципы и приемы командообразования.	информационного обеспечения решения разработки планов коммуникаций с заказчиком в проектах создания (модификации) ИС; методологии и средства проектирования и дизайна ИС; правила и стандарты разработки пользовательской документации к ИС; принципы и приемы командообразования.	информационного обеспечения решения разработки планов коммуникаций с заказчиком в проектах создания (модификации) ИС; методологии и средства проектирования и дизайна ИС; правила и стандарты разработки пользовательской документации к ИС; принципы и приемы командообразования.	
на уровне умений: Умеет выполнять документирование существующих бизнес-процессов организации заказчика; Умеет применять принципы, методы и стандарты	Не умеет применять знания на практике	Демонстрирует частичный уровень умений	Демонстрирует достаточный уровень умений	Демонстрирует высокий уровень умений для разработки алгоритмов решения задач

разработки архитектуры ИС; Умеет профессионально выполнять разработку баз данных ИС; Умеет организовывать программы обучения и развития персонала.				
на уровне навыков: Владеет навыками выстраивания коммуникаций с заказчиком в проектах создания (модификации) и ввода ИС в эксплуатацию; Владеет навыками документирования и реинжиниринга бизнес-процессов организации; Владеет навыками проектирования и разработки дизайна ИС; Владеет навыками создания пользовательской документации к ИС; Владеет навыками	Не владеет практическими навыками работы с технологиями и программным инструментарие м	Владеет практическими навыками частично работы с технологиями и программным инструментарием	Владеет практическими навыками формирования требований к информационной системе достаточно свободно	Владеет практическим и навыками работы на компьютере и использования стандартных информационно-коммуникационных технологий на высоком уровне

организации заключения договоров на выполняемые работы, связанные с ИС				

4.4. Методические материалы

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание теоретического материала

Критериями оценки ответа обучающихся выступают:

- правильность ответов на вопросы преподавателя по изученному
- материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение
- полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при проведении опроса на практическом занятии

Оценки "отлично" заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

Оценки "хорошо" заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки "удовлетворительно" заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка "неудовлетворительно" выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

4.4.3. Методические материалы, определяющие процедуру оценивания промежуточной аттестации по дисциплине

Зачет проводится путем распределения по времени в течение всего срока обучения проведения мониторинга уровня освоения компетенции по результатам выполнения заданий по подготовке к опросу. При условии положительных ответов на вопросы зачет, компетенции считаются сформированными, и по данной дисциплине

выставляется оценка. В ином случае, компетенции считаются несформированными, и по данной дисциплине выставляется оценка «неудовлетворительно».
Зачет принимается в устной форме, по вопросам. Задание включает теоретический и практический вопрос. Оценка знаний обучающегося на зачет с оценкойе носит комплексный характер и определяется его:

- ответом на зачете;
- учебными достижениями в семестровый период.

Знания, умения, навыки обучающегося на зачете оцениваются оценками: «зачтено», «незачтено». Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

Оценивание студента на зачете с оценкой по дисциплине «Основы кибербезопасности»

Оценка	Требования к знаниям
Отлично	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает на зачет с оценкойе, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение. Учебные достижения в семестровый период демонстрируют высокую степень овладения программным материалом.
Хорошо	Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Учебные достижения в семестровый период демонстрируют хорошую степень овладения программным материалом.
Удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. Учебные достижения в семестровый период демонстрируют достаточную (удовлетворительную) степень овладения программным материалом.
Неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. Учебные достижения в семестровый период не демонстрировали достаточную степень овладения программным материалом на пороговом уровне.

Зачет проводится во время сессии по традиционной шкале оценивания.

Студентам, не выполнившим требования по промежуточной аттестации, по уважительным причинам, предоставляется возможность их выполнения и сдачи.

5. Методические указания для обучающихся по освоению дисциплины

Домашние задания соответствуют приведенным ранее темам для коллоквиумов и опросов при самостоятельной подготовке, и могут быть опубликованы:
1. На общих ресурсах академии (в сетевой папке);
2. Высланы на общую почту группы
Конкретный способ коммуникации со студентами определяется преподавателем. Для подготовки к практическим занятиям необходимо ознакомиться с лекциями, рекомендованной литературой, иными источниками, интернет ресурсами, повторить материал предыдущих практических занятий. Самостоятельно разобрать вопросы к практическим занятиям по темам. При возникновении вопросов - обратиться к преподавателю по электронной почте с указанием конкретной проблемы и (или) прийти к преподавателю на консультацию в установленное время.

5.1. Методические указания по вопросам на понимание лекционного материала

На лекциях рекомендуется слушать предлагаемый лектором материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении. Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на семинарском занятии. В случае необходимости обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 программы.

5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и своевременно доводится до сведения обучающегося.
При подготовке к практическому занятию, обучающемуся необходимо внимательно изучить основные вопросы темы семинара. Важным условием успешной подготовки к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.
Подготовка вопросов для самостоятельного изучения включает: изучение необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.
При подготовке к практическим занятиям важно:

- использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;
- представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;
- грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

5.3. Методические рекомендации по подготовке к зачету по дисциплине

Ответ на зачете предусматривает устный ответ на теоретические вопросы. При подготовке к зачету обучающийся обращается к пройденному материалу, сосредоточенному в конспектах лекций, учебниках и других источниках информации.

Повторяя, обобщая, закрепляя и дополняя полученные знания, поднимает их на качественно-новый уровень — уровень системы совокупных данных, что позволяет ему понять логику всего предмета в целом. Новые знания обучающийся получает в ходе самостоятельного изучения того, что не было изложено в лекциях и на семинарских занятиях.

Зачет как особая форма учебного процесса имеет свои особенности, специфические черты и некоторые аспекты, которые необходимо обучающемуся знать и учитывать в своей работе. Это, прежде всего:

• что и как запоминать при подготовке к зачету;
• по каким источникам и как готовиться;
• на чем сосредоточить основное внимание;
• каким образом в максимальной степени использовать программу курса;
• что и как записать, а что выучить дословно и т. п.

На зачет, как правило, проверяется не столько уровень запоминания обучающимся учебного материала, сколько то, насколько успешно он оперирует теми или иными научными понятиями и категориями, систематизирует факты, как умеет мыслить, аргументировано отстаивать определенную позицию, объясняет и пересказывает заученную информацию.

Программу курса необходимо максимально использовать как в ходе подготовки, так и на самом зачете. Ведь она включает в себя разделы, темы и основные проблемы, в рамках которых и формируются вопросы для зачет с оценкойа.

Оптимальным для подготовки к зачету является вариант, когда обучающийся начинает подготовку к нему с первых занятий по данному курсу.

При подготовке к зачету по наиболее сложным вопросам, ключевым проблемам и важнейшим понятиям необходимо сделать краткие письменные записи в виде тезисов, планов, определений. Особое внимание в ходе подготовки к зачету следует уделять конспектам лекций, ибо они обладают рядом преимуществ по сравнению с печатной продукцией. Как правило, они более детальные, иллюстрированные, что позволяет оценивать современную ситуацию, отражать самую свежую научную и оперативную информацию, отвечать на вопросы, интересующие аудиторию, в данный момент, тогда как при написании и опубликовании печатной продукции проходит определенное время, и материал быстро устаревает.

В то же время, подготовка по одним конспектам лекций недостаточна, необходимо использовать и иную учебную литературу. Не следует бояться дополнительных и

уточняющих вопросов на зачет с оценкойе. Они, как правило, задаются или помимо зачет с оценкойационного вопроса для выявления общей подготовленности, или в рамках билета для уточнения высказанной мысли.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Запечников С.В., Казарин О.В., Тарасов А.А КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. М: Юрайт, 2018.
2. Васильева И.Н. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ. - М: Юрайт, http://www.biblio-online.ru/, 2019.
3. Алексеев В.А. Методы и средства криптографической защиты информации – М.: IPRbooks, http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/17710.html, 2018.

6.2. Дополнительная литература

4. Полякова Т.А. ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. - М: Юрайт, http://www.biblio-online.ru/, 2016.
5. Д.П. Зегжда и др. Основы безопасности информационных систем. М., 2000.
6. Джилад Б. Конкурентная разведка. Как распознать внешние риски и управлять ситуацией. – СПб.: Питер, 2010. – 320 с.

6.3. Учебно-методическое обеспечение самостоятельной работы

7. Положение об организации самостоятельной работы студентов федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в ред. приказа РАНХиГС от 11.05.2016 г. № 01-2211). http://www.ranepa.ru/images/docs/prikazy-ranhigs/Pologenie_o_samostoyatelnoi_rabote.pdf

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий или лабораторных работ, для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

№ пп	Тип занятия	Указания
	Тема 1	Введение. Безопасность функционирования современной организации и технологий
1	СРС	Посмотреть в интернете понятие и особенности информации, данных, знаний; клиент-серверных технологий, определить, в чем различие этих понятий. Обратить внимание на протокол HTTP.
2	СРС	Выяснить роль технологий веб в системах организационно-экономического управления. Рассмотреть понятие Основы кибербезопасностиа. Изучить уровни представления информационных объектов веб при описании предметной области.

3	СРС	Для подготовки к занятиям использовать лекции, интернет ресурсы, основную и дополнительную литературу.
	Тема 2	Современная доктрина информационной безопасности Российской Федерации
1	СРС	Изучить аспекты рассмотрения информационных процессов веб в системах управления: преобразование и движение. Процесс принятия решения как основной элемент преобразования информации. Знать основные фазы процесса принятия решений как информационного процесса. Подробно разобрать процессы передачи информации. Знать определение и свойства потока информации веб.
2	СРС	Знать уровни представления информационных процессов. Подробно изучить концептуальную модель информационного процесса. Разобрать структуры логического и физического уровней представления информационного процесса веб.
3	СРС	Для подготовки к занятиям использовать лекции, интернет ресурсы, основную и дополнительную литературу.
	Тема 3	Международные стандарты информационного обмена. Модели безопасности и их применение
1	СРС	Разобрать понятие инструментария веб. Изучить место и роль интернет-приложений в общем контуре организационно-экономического управления. Подробно разобрать этапы развития веб. Выделить основные процессы, обеспечивающие работу веб приложений. Изучить основные свойства сайта. Знать преимущества внедрения веб в сферу управления и бизнеса.
2	СРС	Разобрать понятие Основы кибербезопасностиа. Выделить и изучить подходы к разработке веб сайтов.
3	СРС	Для подготовки к занятиям использовать лекции, интернет ресурсы, основную и дополнительную литературу
	Тема 4	Сущность и задачи обеспечения информационной безопасности
1	СРС	Разобрать понятия функциональной, информационной, программной, технической и организационной интеграции. Подробно разобрать структуру современных корпоративных систем управления предприятиями: программно-аппаратные комплексы с многоуровневой архитектурой, изучить технологические платформы построения современных веб технологий.
2	СРС	Подобрать примеры принципиально новых типов взаимодействия систем: виртуальных, интеллектуальных, геоинформационных и др. Провести анализ и подробное описание веб технологий управления и бизнеса с использованием передовых информационных систем и технологий.
3	СРС	Для подготовки к занятиям использовать лекции, интернет ресурсы, основную и дополнительную литературу
	Тема 5	Отечественные программно-аппаратные средства

		криптографической защиты компьютерных систем
1	СРС	Разобрать понятия функциональной, информационной, программной, технической и организационной интеграции. Подробно разобрать структуру современных корпоративных систем управления предприятиями: программно-аппаратные комплексы с многоуровневой архитектурой, изучить технологические платформы построения современных веб технологий.
2	СРС	Подобрать примеры принципиально новых типов взаимодействия систем: виртуальных, интеллектуальных, геоинформационных и др. Провести анализ и подробное описание веб технологий управления и бизнеса с использованием передовых информационных систем и технологий.
3	СРС	Для подготовки к занятиям использовать лекции, интернет ресурсы, основную и дополнительную литературу
	Тема 6	Состав, структура и назначение Удостоверяющих центров в системах защиты и аутентификации электронных документов в интернет
1	СРС	Разобрать понятия функциональной, информационной, программной, технической и организационной интеграции. Подробно разобрать структуру современных корпоративных систем управления предприятиями: программно-аппаратные комплексы с многоуровневой архитектурой, изучить технологические платформы построения современных веб технологий.
2	СРС	Подобрать примеры принципиально новых типов взаимодействия систем: виртуальных, интеллектуальных, геоинформационных и др. Провести анализ и подробное описание веб технологий управления и бизнеса с использованием передовых информационных систем и технологий.
3	СРС	Для подготовки к занятиям использовать лекции, интернет ресурсы, основную и дополнительную литературу

Рекомендации по организации самостоятельной работы студентов:

Вид учебных занятий	Организация деятельности студента
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Анализ литературы и/или Интернет – ресурсов, решение типовых задач, проведение консультаций с преподавателем по проблемным вопросам лекционного материала, подготовка к опросу и/или коллоквиуму, постановка задачи для практического задания, оформление отчета по заданию, работа в малой группе.
Контрольная работа / индивидуальное задание	Ознакомление с постановкой задачи, разработка алгоритма решения, выбор программно-аппаратных средств реализации. Реализация в выбранной инструментальной среде. Подготовка выводов и/или короткого отчета в виде презентации.

Подготовка к дискуссиям, докладам, написанию реферата	Поиск литературы и составление библиографии, использование от 3 до 5 научных работ, изложение мнения авторов и своего суждения по выбранному вопросу; изложение основных аспектов проблемы. Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных алгоритмов и/или рекомендаций по решению поставленной цели и задачи; проведение практических исследований по данной теме. Разработка презентации для доклада основных результатов проведенной работы. Желательно оформление результатов в виде статьи в сборник трудов конференции или тематический научный журнал.

6.4. Нормативные правовые документы

8. IEEE P1003.0 «Руководство по окружению открытых систем POSIX».
9. ГОСТ Р ИСО/МЭК 12207. Процессы жизненного цикла программных средств.

6.5. Интернет-ресурсы, справочные системы.

10. http://smarty.php.net – веб-технологии
11. http://yandex.ru/cgi/vesna - примеры скриптов веб-приложений
12. http://belitsoft.ru/ - инструментарий разработки интернет-приложений
13. http://www.virtech.ru – инструментарий разработки интернет-приложений
14. http://www.oracle.sun.com – инструментарий разработки интернет-приложений
15. 1. http://www.consultant.ru/ - Официальный сайт компании «Консультант Плюс».
16. http://www.cfin.ru/software/index.shtml - Сайт «Корпоративный менеджмент». Обзор информационных систем для основных функций управления и бизнеса.
17. http://citforum.ru/ - «Сервер информационных технологий» - on-line библиотека информационных материалов по компьютерным технологиям.
18. http://www.intuit.ru/ - Образовательный портал дистанционного обучения.
19. www.coursera.org - Платформа для бесплатных онлайн - лекций (проект по публикации образовательных материалов в интернете, в виде набора бесплатных онлайн - курсов).

6.6. Иные источники

20. Леле М. Абсолютное оружие. Как убить конкуренцию: захват и удержание рынка. - М.: ИД «Коммерсантъ»; СПб: ИД «Питер», 2009. – 224 с.

7. Материально-техническое и программное обеспечение дисциплины (модуля)

Название лаборатории/класса, оснащенного необходимым, в соответствии с требованиями ФГОС/ СУОС, оборудованием	Наименование оборудования	Перечень лицензионного программного обеспечения
учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации	Рабочие места студентов: столы и стулья – соответственно количеству студентов. Рабочее место для инвалида и лиц с ОВЗ: парта с телескопической столешницей на электромеханическом приводе - 1 шт., кресло-коляска для инвалидов 18" - 1 шт., индукционная петля - 1 шт., компьютер с версией для слабовидящих - 1 шт., кнопка вызова сотрудников – 1 шт. Рабочее место преподавателя: стол – 1 шт., стул – 1 шт, кафедра - 1 шт. Доска меловая и маркерная. Экран, ноутбук Lenovo ideapad 100/15, проектор	Мультимидийный проектор Консультант Плюс
информационно – аналитическая лаборатория – учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальны х консультаций	Рабочие места: столы компьютерные – в соотвествии с количеством студентов, кресло Престиж Profi -B-20 Самба бордо в рубчик - 15 шт., подставка для ног Fellowes FS-48121 Standard черный - 15 шт. Рабочее место преподавателя: стол компьютерный - 1 шт., стул - 1 шт. Доска меловая или маркерная Персональные компьютеры	Мультимидийный проектор Консультант Плюс
библиотека - помещение для самостоятельной работы	Рабочие места: столы и стулья. Рабочее место преподавателя: стол – 1 шт., стул - 1 шт., кафедра библиотечная - 1 шт. Телефон – 1 шт., цифровой многофункциональный копир - 1 шт., копировальный аппарат МФУ – 1 шт., принтер - 1 шт., сканер – 1 шт. Шкаф – 7 шт, стеллаж-33 шт, библиотечная стойка – 2 шт., стенд – 2 шт. Меловая или маркерная доска. Персональные компьютеры	Мультимидийный проектор Консультант Плюс

Программное обеспечение:

В процессе лекционных и семинарских занятий используется следующее программное 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».

- программы Project Expert и Microsoft Project

Информационные справочные системы:

1. www.nnir.ru / - Российская национальная библиотека
2. www.nns.ru / -Национальная электронная библиотека
3. www.rsi.ru / - Российская государственная библиотека
4. www.biznes-karta.ru / -Агентство деловой информации «Бизнес-карта»
5. www. rbs.ru / - Информационное агентство «РосБизнесКонсалтинг»
6. www.aport.ru / - Поисковая система
7. www.rambler.ru / - Поисковая система
8. www.yandex.ru / - Поисковая система
9. www.busineslearning.ru / - Система дистанционного бизнес образования
10. www.test.specialist.ru / - Центр компьютерного обучения МГТУ им. Н. Э. Баумана
11. http://www.consultant.ru/ - Консультант плюс
12. http://www.garant.ru/ - Гарант
13. Научная библиотека РАНХиГС. URL: http://lib.ranepa.ru/;
14. Научная электронная библиотека eLibrary.ru. URL: http://elibrary.ru/defaultx.asp;
15. Национальная электронная библиотека. URL: www.nns.ru; Российская государственная библиотека. URL: www.rsl.ru;
16. Российская национальная библиотека. URL: www.nnir.ru; Электронная библиотека Grebennikon. URL: http://grebennikon.ru/;
17. Электронно-библиотечная система Издательства «Лань». URL: http://e.lanbook.com;
18. Электронно-библиотечная система ЮРАЙТ. URL: http://www.biblio-online.ru/.