МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Балахнинский филиал ННГУ

УТВЕРЖДЕНО
решением президиума
Ученого совета ННГУ
протокол от 14.12.2021 г. №4

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования
БАКАЛАВРИАТ

Направление подготовки
09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Направленность (профиль) образовательной программы
ПРИКЛАДНАЯ ИНФОРМАТИКА В УПРАВЛЕНИИ ПРОИЗВОДСТВОМ

Квалификация (степень)

БАКАЛАВР

Форма обучения:
ОЧНАЯ, ОЧНО-ЗАОЧНАЯ

Балахна
2022

Лист актуализации

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры
_____

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры
_____

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 20___ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры
_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МК
__ _____ 20___ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.21 «Информационная безопасность» относится к обязательной части ОПОП по направлению 09.03.03 Прикладная информатика, направленность (профиль): Прикладная информатика в управлении производством.

Целями освоения дисциплины являются: изучение принципов обеспечения информационной безопасности, подходов к анализу угроз информационной инфраструктуры организации; освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**
	Индикатор достижения компетенции (код, содержание индикатора)	**Результаты обучения по дисциплине**	
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Уметь использовать принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Владеть навыками решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности	доклад, тесты, лабораторная работа, реферат
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать принципы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности Уметь разработать требования по информационной безопасности для решения стандартных задач профессиональной деятельности Владеть навыками подбора и использования программно-технических средств для решения стандартных задач с учетом основных требований информационной безопасности	доклад, тесты, лабораторная работа, реферат
	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной	Знать принципы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности Уметь использовать основы информационной безопасности при подготовке обзоров, аннотаций, составления рефератов, научных докладов,	доклад, тесты, лабораторная работа, реферат

	безопасности.	публикаций, и библиографии по научно-исследовательской работе Владеть навыками использования методов и средств обеспечения информационной безопасности при подготовке обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе	
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Знать основные законодательные акты в сфере информационной безопасности Уметь использовать в практической деятельности существующие правовые знания в сфере информационных систем и информационных технологий Владеть навыками соблюдения норм и правил, существующих в виртуальной среде	доклад, тесты, лабораторная работа, реферат
	ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Знать стандарты оформления технической документации с учетом информационной безопасности Уметь использовать стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом информационной безопасности Владеть навыками использования инструментов информационной безопасности при разработке технической документации	доклад, тесты, лабораторная работа, реферат
	ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Знать основные инструменты информационной безопасности при составлении технической документации Уметь применять методы и средства информационной безопасности на различных этапах жизненного цикла ИС Владеть методами и средствами обеспечения информационной безопасности на различных этапах жизненного цикла информационной системы	доклад, тесты, лабораторная работа

3. Структура и содержание дисциплины

3.1 Трудоёмкость дисциплины

	Очная форма обучения
Общая трудоёмкость	4 ЗЕТ
Часов по учебному плану	144
в том числе	
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия лабораторного типа - КСР	66 16 48 2
самостоятельная работа	42
Промежуточная аттестация – экзамен	36

	Очно-заочная форма обучения
Общая трудоёмкость	4 ЗЕТ
Часов по учебному плану	144
в том числе	
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия лабораторного типа - КСР	30 12 16 2
самостоятельная работа	78
Промежуточная аттестация – экзамен	36

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	**Всего (часы)**	**В том числе при очной форме подготовки**			
		Контактная работа, часы, из них занятия			**Самостоятельная работа, часы**
		лекционного типа	**лабораторного типа**	**Всего**	
1. Теоретические аспекты информационной безопасности экономических систем	21	3	9	12	9
2. Понятие информационных угроз и их виды	21	3	9	12	9
3. Принципы построения системы информационной безопасности	21	4	9	13	8
4. Организация системы защиты информации	22	3	12	15	7
5. Информационная безопасность отдельных экономических систем	21	3	9	12	9
КСР	2			2	
Промежуточная аттестация – экзамен	36				
ИТОГО	144	16	48	66	42

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	**Всего (часы)**	**В том числе при очно-заочной форме подготовки**			
		Контактная работа, часы, из них занятия			**Самостоятельная работа, часы**
		лекционного типа	**лабораторного типа**	**Всего**	
1. Теоретические аспекты информационной безопасности экономических систем	21	2	3	5	16
2. Понятие информационных угроз и их виды	21	2	3	5	16
3. Принципы построения системы информационной безопасности	21	3	3	6	15
4. Организация системы защиты информации	22	3	4	7	15
5. Информационная безопасность отдельных экономических систем	21	2	3	5	16
КСР	2			2	
Промежуточная аттестация – экзамен	36				
ИТОГО	144	12	16	30	78

Текущий контроль успеваемости реализуется в рамках занятий лабораторного типа.

Промежуточная аттестация проходит в традиционной форме – экзамен, включающий ответы на вопросы по программе дисциплины.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Цель самостоятельной работы – формирование навыков непрерывного самообразования и профессионального совершенствования.

Самостоятельная работа способствует формированию аналитического и творческого мышления, совершенствует способы организации исследовательской деятельности, воспитывает целеустремленность, системность и последовательность в работе студентов, развивает у них навык завершать начатую работу.

Основные виды самостоятельной работы студентов:

- работа с основной и дополнительной литературой;
- изучение категориального аппарата дисциплины;
- самостоятельное изучение тем дисциплины;
- подготовка докладов-презентаций;
- подготовка к экзамену;
- работа в библиотеке;
- изучение сайтов по темам дисциплины в сети Интернет.

Работа с основной и дополнительной литературой

Изучение рекомендованной литературы следует начинать с учебников и учебных пособий, затем переходить к научным монографиям и материалам периодических изданий. Работа с литературой предусматривает конспектирование наиболее актуальных и познавательных материалов. Это не только мобилизует внимание, но и способствует более глубокому осмыслению материала, его лучшему запоминанию, а также позволяет студентам проводить систематизацию и сравнительный анализ изучаемой информации. Таким образом, конспектирование – одна из основных форм самостоятельного труда, которая требует от студента активно работать с учебной литературой и не ограничиваться конспектом лекций.

Студент должен уметь самостоятельно подбирать необходимую литературу для учебной и научной работы, уметь обращаться с предметными каталогами и библиографическим справочником библиотеки.

Изучение категориального аппарата дисциплины

Изучение и осмысление основных категорий дисциплины требует проработки лекционного материала, выполнения практических заданий, изучение словарей, энциклопедий, справочников.

Индивидуальная самостоятельная работа студента направлена на овладение и грамотное применение терминологии по изучаемой дисциплине.

Самостоятельное изучение тем дисциплины

Особое место отводится самостоятельной проработке студентами отдельных разделов и тем изучаемой дисциплины. Такой подход вырабатывает у студентов инициативу, стремление к увеличению объема знаний, умений и навыков, всестороннего овладения способами и приемами профессиональной деятельности.

Изучение вопросов определенной темы направлено на более глубокое усвоение основных категорий, совершенствование навыка анализа теоретического и эмпирического материала.

Подготовка докладов-презентаций

Написание докладов и подготовка презентации позволяет студентам глубже изучить темы курса, самостоятельно освоить изучаемый материал, пользуясь учебными пособиями и научными работами. Тема реферата может назначаться преподавателем или инициироваться студентом.

Подготовка к экзамену

Промежуточная аттестация студентов по дисциплине проходит в виде экзамена и предусматривает оценку. Условием успешного прохождения промежуточной аттестации является систематическая работа студента в течение семестра. В этом случае подготовка к экзамену является систематизацией всех полученных знаний по данной дисциплине.

Рекомендуется внимательно изучить перечень вопросов к экзамену, а также использовать в процессе обучения программу, учебно-методический комплекс, другие методические материалы.

Желательно спланировать троекратный просмотр материала перед экзаменом. Во-первых, внимательное чтение с осмыслением, подчеркиванием и составлением краткого плана ответа. Во-вторых, повторная проработка наиболее сложных вопросов. В-третьих, быстрый просмотр материала или планов ответов для его систематизации в памяти.

Самостоятельная работа в библиотеке

Важным аспектом самостоятельной подготовки студентов является работа с библиотечным фондом.

Это работа предполагает различные варианты повышения профессионального уровня студентов:

а) получение книг для подробного изучения в течение семестра на научном абонементе;

б) изучение книг, журналов, газет - в читальном зале;

в) возможность поиска необходимого материала посредством электронного каталога;

г) получение необходимых сведений об источниках информации у сотрудников библиотеки.

Изучение сайтов по темам дисциплины в сети Интернет

Ресурсы Интернет являются одним из альтернативных источников быстрого поиска требуемой информации. Их использование возможно для получения основных и дополнительных сведений по изучаемым материалам. Необходимо помнить об оформлении ссылок на Интернет-источники.

Для повышения эффективности самостоятельной работы студентов преподавателю целесообразно использовать следующие виды деятельности:

- консультации,
- выдача заданий на самостоятельную работу,
- информационное обеспечение обучения,
- контроль качества самостоятельной работы студентов.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю), включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	**Шкала оценивания сформированности компетенций**						
	плохо	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	Не зачтено		зачтено				
Знания	Отсутствие знаний теоретического материала.	Уровень знаний ниже минимальных	Минимально допустимый уровень знаний. Допущено	Уровень знаний в объеме, соответствующем	Уровень знаний в объеме, соответствующем	Уровень знаний в объеме, соответствующем	Уровень знаний в объеме, превышающем

	Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	требований. Имели место грубые ошибки.	много негрубых ошибки.	программе подготовки. Допущено несколько негрубых ошибок	программе подготовки. Допущено несколько несущественных ошибок	программе подготовки, без ошибок.	программу подготовки.
Умения	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	Превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно»
	Отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	Очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне «очень хорошо»
	Хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	Удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»

не зачтено	Неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	Плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1. Контрольные вопросы

Вопросы	Код формируемой компетенции
1. Необходимость обеспечения безопасности в информационных системах.	ОПК-3
2. Прогресс информационных технологий и информационная безопасность.	ОПК-3
3. Нормативно-правовые аспекты информационной безопасности.	ОПК-4
4. Классификация угроз безопасности информационных объектов.	ОПК-3
5. Основные виды каналов утечки информации.	ОПК-3
6. Умышленные и неумышленные угрозы информационной безопасности.	ОПК-3
7. Внешние угрозы информационной безопасности.	ОПК-3
8. Мотивы и цели компьютерных преступлений.	ОПК-3
9. Статьи уголовного кодекса о компьютерных преступлениях.	ОПК-3
10. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.	ОПК-3
11. Объекты информационной безопасности на предприятии.	ОПК-3
12. Организационные методы обеспечения информационной безопасности.	ОПК-3
13. Физическая защита информационных систем.	ОПК-3
14. Программно - технические методы обеспечения информационной безопасности.	ОПК-3
15. Идентификация и аутентификация.	ОПК-3
16. Доктрина информационной безопасности Российской Федерации.	ОПК-4
17. Государственное регулирование информационной безопасности в России.	ОПК-4
18. Несанкционированный доступ и защита от него.	ОПК-3
19. Проблема информационной безопасности в историческом аспекте.	ОПК-3
20. Предупреждение компьютерных преступлений.	ОПК-3
21. Типы компьютерных вирусов и защита от них.	ОПК-3
22. Человеческие факторы, обуславливающие информационные угрозы.	ОПК-3
23. Способы воздействия угроз на информационный объект.	ОПК-3
24. Признаки воздействия вирусов на компьютерную систему.	ОПК-3
25. Фрагментарный и системный подходы к защите информации.	ОПК-3
26. Уголовно-правовая характеристика компьютерных преступлений.	ОПК-3
27. Субъективная сторона компьютерных преступлений.	ОПК-3
28. Объективная сторона компьютерных преступлений.	ОПК-3
29. Способы совершения компьютерных преступлений («за хвост», «маскарад» и др.)	ОПК-3
30. Причины и условия, способствующие совершению компьютерных преступлений.	ОПК-3
31. Меры предупреждения преступлений в сфере компьютерной информации.	ОПК-3
32. История вредоносных программ.	ОПК-3
33. Защита учетной информации коммерческих фирм.	ОПК-3
34. Свойства экономической информации, нарушаемые при несанкционированном доступе.	ОПК-3
35. Исторические аспекты компьютерных преступлений.	ОПК-3
36. Экономическая информация как объект безопасности.	ОПК-3
37. Перечень сведений, которые не могут составлять коммерческую тайну.	ОПК-4
38. Виды тайн и как их сохранить.	ОПК-4
39. Причины разглашения конфиденциальной информации.	ОПК-3
40. Разглашение и утечка информации.	ОПК-3

41. Стратегия злоумышленника при несанкционированном доступе.	ОПК-3
42. Организация конфиденциального делопроизводства.	ОПК-3
43. Структура службы безопасности компании.	ОПК-3
44. Теоретические аспекты информационной безопасности экономических систем.	ОПК-3
45. Основные понятия информационной безопасности экономических систем.	ОПК-3
46. Экономическая информация как товар и объект безопасности.	ОПК-3
47. Понятия информационных угроз и их виды.	ОПК-3
48. Вредоносные программы.	ОПК-3
49. Компьютерные преступления и наказания.	ОПК-3
50. Принципы построения системы информационной безопасности.	ОПК-3
51. Подходы, принципы, методы и средства обеспечения безопасности.	ОПК-3
52. Организационно-техническое обеспечение компьютерной безопасности.	ОПК-3
53. Электронная цифровая подпись и особенности ее применения.	ОПК-3
54. Защита информации в Интернете.	ОПК-3
55. Организация системы защиты информации экономических систем.	ОПК-3
56. Этапы построения системы защиты информации.	ОПК-3
57. Политика безопасности.	ОПК-3
58. Оценка эффективности инвестиций в информационную безопасность.	ОПК-3
59. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).	ОПК-3
60. Информационная безопасность электронной коммерции (ЭК).	ОПК-3
61. Обеспечение компьютерной безопасности учетной информации.	ОПК-3
62. Сущность криптографических методов.	ОПК-3
63. Организационно-административные мероприятия обеспечения компьютерной безопасности.	ОПК-3
64. Организация конфиденциального делопроизводства.	ОПК-4
65. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения.	ОПК-3
66. Типы и субъекты информационных угроз.	ОПК-3

5.2.2. Типовые тестовые задания для оценки сформированности компетенции

Тесты для проверки компетенции «ОПК-3»

Вопрос 1. Объектом информационной безопасности может
а. коммерческое предприятие
б. некоммерческое предприятие
в. государственный орган
г. все ответы верны

Вопрос 2. Управление экономическими объектами всегда связано с преобразованием
а. социальной информации
б. экономической информации
в. демографической информации
г. юридической информации

Вопрос 3. Свойства информации как товара:
а. неисчерпаемость, сохраняемость, несамостоятельность
б. исчерпаемость, несохраняемость, самостоятельность
в. неисчерпаемость, сохраняемость, самостоятельность
г. исчерпаемость, сохраняемость, несамостоятельность

Вопрос 4. Информация может считаться служебной тайной, если она отвечает следующим требованиям
а. отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости
б. является охраноспособной конфиденциальной информацией («чужой тайной») другого лица
в. Все ответы верны
г. Все ответы неверны

Вопрос 5. Если ценность информации теряется при ее хранении и/или распространении, то реализуется
а. угроза целостности информации
б. угроза оперативности использования или доступности информации
в. угроза нарушения конфиденциальности информации
г. все ответы верны

Тесты для проверки компетенции «ОПК-4»

Вопрос 1. Политика безопасности не включает в себя
а. объект информационной безопасности
б. обеспечение информационной безопасности
в. угрозы объекту информационной безопасности
г. все ответы верны

Вопрос 2. К объектам информационной безопасности на предприятии не относят
а. информационные ресурсы
б. средства и системы информатизации
в. субъекты информационной безопасности
г. коммерческое предприятие

Вопрос 3. Сегмент деловой информации относится к следующему виду рынка
а. финансовый
б. информационный
в. товарный
г. услуг
д. биржевой

Вопрос 4. К свойствам информации как товара относят
а. репрезентативность
б. адекватность
в. несамостоятельность
г. достоверность
д. доступность

Вопрос 5. Объекты профессиональной тайны
а. врачебная тайна
б. тайна страхования
в. тайна связи
г. тайна усыновления
д. все ответы верны

5.2.3. Типовые задания/задачи для оценки сформированности компетенции
Задания для лабораторных работ

Для оценки сформированности компетенции «ОПК-3»

Задание 1. Наделение прав пользователей в системе 1С:Предприятие

Задание 2. Кодирование текста при помощи перестановки символов

Необходимо расшифровать сообщение, зашифрованное перестановкой с ключевым словом. Ключ = ИМАЖИНИЗМ.

!еоонжилмтНмс,сиоиуетнюоыбу.рзахотКиеусезагоооёЯхунресиявтаптй"мс,сиоиуетнТшзкынсаньиоуСмзсзлрьебрйрсЗеин.чмотт,врнбагмчтчитдюрячгпакаетНбуСмзсзлрьербтладюНвойвиыа,сух,д.тясодтнопгвцст!оскмШтжвпаюсИмрбч,рдж,,ьзиеиыа,сух,д.Д-зЯо,трдняооспнаиыонлятеьияяяилат.енио,мйммтюоитибж.ёщун",рнеддяспнаиыУнлеевиееттотзйттодкоие,Бло,ютомяаАьегчкгееаамо,ьдипкюсдваоок,щпииеттодкоие,Беоауруойзпиалрдхвнаьугэвуготпуосяаркляло;эеоазаомаиеёеоайыйракмлрдхвнаьугарвпдУлыое.мсяёомххмамлгвопхдАлани.тадюПвкилкнл,итааСтежеЯкоеу.осяёомххмамьеаряукаелднлйвНктПзиАозтнраачоде.взЯвьоыуоусррстситъаИю:епМнайнлйвНкт,зипнрнкбвоюокдуайоогцтсоюдПзьлооккюсдёаосуккввНнотрагпцсщвповиензз уайоогцтсо

Задание 3. Необходимо расшифровать сообщение, зашифрованное перестановкой с ключевым словом. Ключ = ЛОБАЧЕВСКИЙ.

8,9,2,1,11,4,3,10,7,5,6

(4)ареярфоеооуыоолкдри.вда.авмзвсобиопренеещцнГцоотрегбипюурсниаядвкр)лпмнвем,л;ехл

(3)робидмгвнзовзиссоанмезказареяефйтрсобилбаaоНатткатралуиуиоецпдттсбяий(ооцутэ)щре

(7)ецпядесоотеенлоНиврИонмнчниаючаоесецпчвеывходоинвниыцнотавинов(ноитагиеиртотхвно

(6)лаолздоннаршаадйкте.кносаецпяемзчечаоуоптиы;ябчоиьнтаавеваянн:легноздбонянткртвн

(10)еннселааоьео«ытеонто»окниинояиосо;еннхинфетаутегйтцмносбюробирувевлооза;(бин(нди

(11)инояньрвбннбНйегсыеб,птыунос:еннгоинойийиокянмаэодииoнвкр.аревощотамнванкдосноие)

(9)иостладоолдоянажгниЛогевмяннснианаиосыненлегколоосаоорниипфйтосечоеитил)яочовейт

(1)Уноспинстроираилоуйтасромпфйтоинообносс;ертхие(л)е;ябоаооВвмзхйеианонкциаорлысея.

(2)пфйтоеотоагяацсьрдуичоириробибноспефйтсозмрНзнвеияоримнмнслаооосниибоиирнкоейуат

(8)ниаееруггежгиьвийес.гороаиостецпбснианачиэсрорсннозпииiунуностоиурдцолпеиомрилос

(5)вмзваегнмвчсвнеиссвНсазОдлаолпреуцемзадсиинУиомрхлаозл,чотиостелоо;иоonалевеасиь

Задание 4. Расшифровать текст при помощи методы гаммирования

Гамма: Понедельник_начинается_в_субботу

Текст:

&	Я	б	К	У	И	Ъ	в	я	Р	Л	ь	Ь	О	ж
	Н	О	У	Л	Ю	о	с	$	Е	!	#	б	В	Т
	в	л	Ф	;	Э	Я	в	ц	Н	Ч	л	Я	Ы	Ш
	!	ю	т	а	ъ	н	т	Х	б	й	у	ф	Ф	$
	Ф	в	Д	В	Ъ	#	%	З	б	Ь	ч	Ш	ч	Ш
	в	Ы	и	ь	ъ	Я	Ш	Э	Р	Щ	П	ч	Х	г
	я	ь	С	ч	#	Ъ	З	Н	П	а	Ь	5	!	П
	Ф	Х	Ф	Ю	щ	Я	и	ь	#	я	Ю	к	С	Ъ
	Й	ч	а	Т	р	%	Ы	ч	Я	Ь	б	О	Ч	#
	%	?	Э	а	Ф	С	Щ	э	ф	а	Ч	ь	#	м
	Е	Ш	ъ	Р	т	К	Х	Ч	н	т	З	)	Т	ж
	Ю	у	ж	У	е	>	С	я	У	У	И	Ъ	а	Ь
	Н	Ш	ч	Ч	т	е	Ч	е	Й	ц	$	б	р	!
	У	ф	Т	Ц	Ъ	К	а	п	%	З	Ф	Ю	Л	М
	ч	Ы	р	Ю	М	Ю	>	я	Р	и	С	ж	М	О
	$	Э	ю	ц	Л	>	#	Ю	Р	Ф	Э	г	п	<
	!	П	б	Р	Ф	э	е	Ы	Ы	Р	"	У	Т	е
	О	У	т	К	б	Ф	о	ц	Л	$	о	%	Ж	Р
	!	Э	в	=	е	О	ч	Н	С	Ф	*	Ы	Й	в
	ъ	Ы	Б	к	е	я	Т	б	Ъ	Я	о	ф	Г	?
	Ь	Ф	М	Р	Ф	2	б	8	Р	б	К	б	ч	Ы
	л	Щ	О	Т	я	Ь	Ж	[	Н	У	М	Ф	#	#
	ч	ч	П	?	Х	Я	Х	Ъ	Ч	е	р	б	а	У
	З	д	ч	О	л	Т	У	Щ	,	ю	т	Щ	О	Я
	Т	Т	о	г	л	ч	Р	я	а	%	Ж	Т	к	Ц
	Ф	В	л	я	У	У	Й	М	й	Ц	щ	ь	ъ	С
	С	Ш	Ы	к	т	И	$	ж	а	я	Х	\	#	Ь
	у	Й	П	а	Ь	<	П	а	в	Ц	е	э	с	Щ
	С	Ы	$	Ь	Н	[	Щ	О	И	У	о	з	_	#
	Х	ч	б	Щ	П	З	Ш	$	Я	5	Т	Ш	Ф	Ц
	Ш	Ф	+	я	:	й	ц	О	т	з	Щ	Ц	Щ	С
	Ы	#	л	,	З	ъ	"	%	М	Р	б	б	д	Л
	Ы	я	З	а	С	Ъ	*	Э	Щ	У	_	а	О	Э
	О	я	В	б	е	о	_	ц	У	%	Х	%	У	у
	У	г	з	З	Э	Ъ	ц	ц	Э	С	й	я	Ш	Щ
	"	Ь	И	е	е	ю	т	Р	б	д	о	"	Ю	ч
	#	ж	З	Т	Ю	Ш	ж	М	!	Ы	Л	ц	Т	Ъ
	а	Щ	С	ь	ф	Я	а	в	Ч	С	П	ч	г	а
	д	т	ф	ф	а	е	М	Т	Ф	д	Щ	=	Ч	Ч
	ц	ц	Х	Ъ	п	Ь	Х	Ю	?	е	У	ж	ъ	Р
	т	И	б	г	к	"	И	#	Ч	б	Ю	З	!	Ы
	а	б	Р	й	С	У	ч	Э	з	б	а	Ш	!	!
	т	Д	Й	С	Й	ц	$	=	ю	ц	Л	?	г	%
	Г	Р	Ъ	п	м	>	Ш	я	З	Ш	Р	О	ш	ю
	ъ	У	?	Т	Ж	Ъ	С	Х	П	Т	$	Ъ	х	?

Д \ Э в у % ! 2 Г > Ь У К К
С и к Ц У ь я О Ш а Ц О Ж Ш
д с _ ф ф # е Х Г Р б ж З в
! 2 Ж х ч Ъ к Ц ъ Т я О М а
ъ Ш П Л 2 Ь а ь Л ч # Ы В М
Ъ Ы б 0 Ь Ц е х ч Я й У Ф У
? Э С Э Л Ю Б Я У д ь ? Е !
Ц з у Д ! Х Ь = Э ю ч Н ч Ц
Э Ф Н ж ы я Й Я ъ Ы Й Ы $ Я
е ? К т д д Х Ж Ь Ы Я Б о я
З а ч Щ Э Ш Ч Ы ю Ц У ф ъ Э
а Ш п р _ (О ч У Ф О К ! е
п Б о е Щ ц Э С и Ь Л Р ь !
т Е Ч я Н Ж Ц Т м ъ ф ! Я Ь
у Г к Ю Ь б Ь У ч Ф Ф й п Ь
Х Ю А я > к Ч я В б Ю Т _]
И э е й В т ! Х б 5 з Ы Л К
ш э Л Ы С ь у й М а ъ Ъ Б Й
У Ю и ? Т ! д в О Х я $ л В
Э я Ф Ь Л Щ щ я Х Ш ! С П [
Р Ы Б С Ы " _ $ Г ь # а П Р
Т б $ б ж а Ф ц Р Ъ и Ц а Р
а Г ж ъ Э Ж Ц Ш к л ! ф %
б К Ч я $ б 0 Щ Ь У К Ь ь
* Р ъ Х т е Ж й Ы Р П ц $ Ъ
_ ! Р ъ # е Ф В Ъ Ы % Б ! Ъ
О Х Ф Ш * Р ъ П " б Д а О я
П Ш а а ш ч Р ъ с $ у П Ф Щ
Щ ; Ч я Ф Ж б г к й О ь э м
Е а ы я / У Ы # р т Д ! д Ф
Н К ! Х % 8 Ь Я Ш Н Ш Я п У
щ ь ь Ь У ж Щ й К ч Ъ Т н ъ
П т Э е б у Ю г Щ 6 У У ч З
Ч С а Ь ъ Ъ " Ь В г О Ъ Б Т
Ы # ч ч О ! Ф Щ Щ З а Э в З
Э я Ч Ь Ж Э п к и ь ъ я Т д
д Я М Ж $ й е э С ф Ч л З У
Щ б Э б Х Ц Н Т О ь * Ы Ч ь
ц О З Э ъ Я С Л Ч Ъ _ я Л (
б К М б б % В Э е У У ч Щ
в я Р Ш т Щ с [а а П ч е Т
к ! И ? г л В У б п Щ б Ч я
И ц Э С й я С Ч ч Ы О ж ъ Я
Н б д Э _ ш Л щ Я Ь ф у 7 $
в = Ч я Х Х О Щ ь Щ С ь " О

В	ж	а	б	Я	ч	Ц	Ъ	п	!	Х	ч	Щ	з
т	у	ж	е	в	б	а	е	Ж	Ц	Ш	и	в	я
Л	ь	я	У	Р	и	О	Ю	Ь	И	а	а	м	?
Т	!	Щ	б	В	П	Ч	Ы	%	=	Ф	Ц	Н	З
Л	Э	п	Ы	Ч	О	!	я	Й	[	Ъ	Ъ	Ь	Ч
Ю	#	ж	ъ	К	я	Ъ	%	Д	у	б	б	а	б
Х	У	ш	ц	0	М	г	Т	д	Ф	?	е	Ж	г
Ч	Р	Ж	Р	$	#	м	т	Ж	?	Ф	%	Ж	Х
з	Ш	$	б	Ь	Ь	ч	У	У	э	о	а	Й	Ш
!	Р	Й	к	Ъ	н	т	Т	У	Х	о	ю	ф	$
а	Я	Ю	М	Э	$	ж	>	Т	Т	Ж	х	ч	Ц
л	С	Н	Л	?	Ы	Б	п	С	Ы	Б	Л	е	#
м	ч	Р	*	к	Щ	у	Ж	в	Я	Ф	В	л	я
Ф	ц	Ч	С	Ю	У	ъ	У	?	П	П	г	е	ж
Ж	ч	б	#	д	"	Ц	х	Ъ	й	т	у	Щ	б
Ч	4	П	я	Ц	Е	З	Ъ	п	О	Ы	з	?	У
Н	л	ъ	Я	У	Ж	а	а	в	ъ	Х	#	с	%
К	П	б	Ш	д	5	а	Ы	Л	К	ц	э	ф	У
Х	ь	"	О	И	Ъ	Ф	У	Л	Ж	е	о	с	_
ф	ф	#	е	Ф	В	Я	Ы	б	=	Э	Ъ	ч	Ц
Т	з	о	Щ	О	ь	+	а	П	Ы	Ч	я	Т	С
б	Ф	а	А	ф	Ъ	#	б	В	Д	Ф	г	б	>
Ф	ю	ч	Н	Ы	э	н	О	К	Щ	[	О	а	[
М	Ц	Р	Ф	е	Ч	з	т	ф	у	н	Я	В	у
Ь	Ш	Ш	0	Ъ	У	Р	Е	ч	Ъ	п	я	С	Ь
$	Ц	О	у	щ	я	Р	Ф	е	а	м	%	ф	[
д	в	у	Ф	П	Э	%	6	Ф	я	Р	Е	Р	э
п	Ю	Ь	П	?	Э	С	Э	Л	Ю	Б	Ш	Ы	Э
_	!	Д	ч	Щ	р	б	П	в	$	Ц	б	ж	У
С	У	И	С	з	О	щ	ь	$	Ь	Ш	е	Ч	я
У	Ж	Э	#	ж	ч	ф	!	д	е	Х	Ф	а	е
Ц	8	Ф	я	Ш	Х	Щ	Р	Э	я	Л	ь	х	Ь
С	Ш	Р	Т	П	ч	Ф	а	л	ч	И	?	Ь	в
Т	Р	б	Э	Ь	5	!	Я	Ц	У	Р	Ф	*	Э
Щ	Р	ф	Ю	Б	с	Й	У	У	ч	к	Ч	л	!
Е	ч	Ь	Ф	у	Д	!	б	Х	5	Ц	к	е	Т
Щ	ю	*	2	Й	С	ч	я	Ц	л	П	У	с	ч
к	Ч	м	?	Е	?	а	Х	З	Й	л	т	б	Г
-													

Алфавит (100 символов):

! - " # $ % & ( ) [ ] { } \ * + , _ . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я

Для оценки сформированности компетенции «ОПК-4»

Задание 1. Подготовить проект документа «политика безопасности» выбранной фирмы.

Задание 2. Задание по поиску нормативных документов с использованием «Консультант Плюс»

Варианты заданий по поиску нормативных документов

Вариант	Название документа	Назначение и краткое описание
1	Закон «Об информации, информационных технологиях и о защите информации»	
2	Закон «О лицензировании отдельных видов деятельности»	
3	Закон «Об электронной цифровой подписи»	
4	Закон «О государственной тайне»	
5	Уголовный кодекс РФ Гл. 28. «Преступление в сфере компьютерной информации»	
6	Гражданский кодекс РФ	
7	Конституция РФ	
8	Доктрина информационной безопасности РФ	
9	Стратегия Национальной безопасности Российской Федерации	
10	Постановление правительства РФ «об утверждении положения об особенности обработки персональных данных, осуществляемой без использования средств автоматизации.	
11	Закон «О средствах массовой информации»	
12	Закон РФ «О связи»	
13	Закон «О федеральных органах правительственной связи и информации»	
14	Закон «Об органах федеральной службы безопасности РФ»	
15	Закон РФ «Об авторском праве и смежных правах»	

Задание 3. Работа с нормативными документами в области информационной безопасности.

Ответьте на следующие вопросы:

1. Порядок включения информационных ресурсов в состав средств международного информационного обмена
2. Как карается нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (с примерами)

3. Как карается отказ в предоставлении гражданину информации
4. Как карается нарушение авторских прав. Найти реальные случаи.
5. Как караются незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
6. Как наказывается приведение в негодность объектов жизнеобеспечения
7. Как наказывается неправомерный доступ к компьютерной информации (с примерами)
8. Как наказывается создание и распространение вирусов (с примерами)
9. Как наказывается нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (с примерами)
10. Определение основных понятий в законе ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
11. Основные принципы правового регулирования информационных отношений в законе ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
12. Классификация информации в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
13. Обладатель информации и его права в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
14. К какой информации не может быть ограничен доступ в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
15. Каким образом устанавливается ограничение доступа к информации в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
16. Каким образом регламентируется распространение информации в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
17. Состав информационных систем и требования к ним предъявляемые в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
18. Государственные системы и требования к ним предъявляемые в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
19. Требования к защите информации в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
20. В случае если распространение определенной информации ограничивается или запрещается федеральными законами, кто несет гражданско-правовую ответственность за распространение такой информации в соответствии с законом ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ
21. Какой закон регулирует отношения, связанные с информацией, относящейся к коммерческой тайне?
22. Какие сведения не могут составлять коммерческую тайну? Приведите примеры.
23. Каким образом осуществляется предоставление информации, составляющей коммерческую тайну?
24. Какие права имеет обладатель информации, составляющей коммерческую тайну?
25. Что включают в себя меры по охране конфиденциальности информации, принимаемые ее обладателем?
26. Каковы обязанности работодателя в целях охраны конфиденциальности информации?
27. Какие разделы подлежат размещению на интернет-сайте арбитражного суда в обязательном порядке?

28. Какие разделы не подлежат размещению на интернет-сайте арбитражного суда в обязательном порядке?

29. Кто несет контроль над обеспечением работы интернет-сайта арбитражного суда, составом и содержанием информации, размещаемой на сайте?

Задание 4. Создание защищенной формы документа

5.2.4. Темы для докладов-презентаций, рефератов

Темы докладов-презентаций для оценки «ОПК-3»

1. Актуальность проблемы обеспечения безопасности информационных технологий
2. Информация и информационные отношения. Субъекты информационных отношений, их безопасность
3. Свойства информации и систем ее обработки
4. Цель защиты автоматизированной системы и циркулирующей в ней информации
5. Особенности современных автоматизированных систем как объекта защиты
6. Уязвимость основных структурно-функциональных элементов распределенных систем
7. Источники угроз безопасности и их классификация
8. Классификация каналов проникновения в систему и утечки информации
9. Меры защиты информации
10. Достоинства и недостатки различных видов мер защиты
11. Основные принципы построения системы защиты
12. Основные механизмы защиты компьютерных систем
13. Криптографические методы защиты
14. Задачи, решаемые средствами защиты информации от несанкционированного доступа

Темы докладов-презентаций для оценки «ОПК-4»

1. Проблемы обеспечения безопасности в IP-сетях
2. Уязвимость IP-сетей
3. Межсетевые экраны
4. Типы межсетевых экранов
5. Механизмы трансляции сетевых адресов
6. Виртуальные частные сети (Virtual Private Networks – VPN)

Темы рефератов для оценки «ОПК-3»

1. Системная классификация и общий анализ угроз безопасности информации.
2. Основные концептуальные положения теории защиты информации.
3. Источники угроз информационно безопасности.
4. Защита информации от несанкционированного доступа.
5. Принципиальная схема организации обмена документами, заверенными цифровой подписью.
6. Криптографические методы защиты информации.
7. Программы вирусы и средства антивирусной защиты.
8. Основные концептуальные положения теории защиты информации.
9. Задачи защиты информации.

10. Методы идентификации и аутентификации пользователей.
11. Источники и каналы утечки информации.
12. Концепция комплексной защиты информации.
13. Причины нарушения информационной безопасности в вычислительной сети.
14. Методы контроля доступа.
15. Организационно-правое обеспечение защиты информации.
16. Методология создания, организации и обеспечения функционирования системы комплексной защиты информации.
17. Методы контроля информации, обрабатываемой средствами вычислительной техники.
18. Стандарты информационной безопасности и методическое обеспечение
19. Организация системы информационной безопасности предприятия
20. Анализ рисков нарушения информационной безопасности предприятия
21. Разновидности аналитических работ по оценке защищенности
22. Политика информационной безопасности России
23. Наиболее распространенные угрозы в интегрированной информационной системе управления предприятием
24. Уязвимость информационных систем

Темы рефератов для оценки «ОПК-4»

1. Требования по обеспечению информационной безопасности корпоративной информационной системы предприятия
2. Требования к программно-аппаратным средствам
3. Требования к подсистеме идентификации и аутентификаци
4. Требования к подсистеме управления доступом
5. Требования к подсистеме протоколирования аудита
6. Требования к подсистеме защиты повторного использования объектов
7. Требования к защите критичной информации
8. Требования к средствам обеспечения целостности.
9. Требования к средствам управления ИБ
10. Требования к Межсетевому Экрану
11. Системы разграничения доступа (полномочий)
12. Электронный замок
13. Идентификация и аутентификация пользователей
14. Регистрация попыток доступа к ПЭВМ
15. Контроль целостности программной среды и запрет загрузки со съемных носителей
16. Построение системы защиты распределенных вычислительных сетей от внутренних и внешних посягательств на информацию и ресурсы различного назначения
17. Управление безопасностью в корпоративных распределенных вычислительных системах и сетях связи
18. Защита документов и товаров с использованием электронной цифровой подписи
19. Перспективы развития аппаратных средств защиты от несанкционированного доступа к информации

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. – 2-е изд., доп. – М.: Форум: НИЦ ИНФРА-М, 2015. – 240 с. Режим доступа: http://znanium.com/bookread2.php?book=491597;

2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. – М.: Издательство Юрайт, 2018. – 321 с. Режим доступа: https://biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7;

3. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. – М.: Форум: НИЦ ИНФРА-М, 2016. – 432 с. Режим доступа: http://znanium.com/bookread2.php?book=516806;

б) дополнительная литература:

1. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/ Баранова Е. К., Бабаш А. В., 3-е изд. – М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. – 322 с. Режим доступа: http://znanium.com/bookread2.php?book=495249;

2. Глинская Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ Глинская Е.В., Чичварин Н.В. – М.: НИЦ ИНФРА-М, 2016. – 118 с. Режим доступа: http://znanium.com/bookread2.php?book=507334;

3. Ищейнов В.Я.Основные положения информационной безопасности: Учебное пособие/ В.Я. Ищейнов, М.В. Мецатунян – М.: Форум, НИЦ ИНФРА-М, 2015. – 208 с.Режим доступа: http://znanium.com/bookread2.php?book=508381;

в) программное обеспечение лицензионное и свободно распространяемое

- Операционная система Microsoft Windows
- Пакет прикладных программ Microsoft Office
- 1С: Предприятие 8
- Правовая система «Консультант плюс»
- Антивирус Dr.Web
- Браузер Google Chrome

г) Интернет-ресурсы

- Научная электронная библиотека: https://elibrary.ru/project_risc.asp
- Российская национальная библиотека: http://nlr.ru/
- Национальная платформа открытого образования: https://openedu.ru/
- Архив ведущих западных научных журналов на российской платформе НЭИКОН: http://archive.neicon.ru/xmlui/ [Дата обращения 08.11.2019]
- ИД «Connect» – отраслевой информационно-аналитический портал в сфере информационных технологий: http://www.connect-wit.ru/ [Дата обращения 08.11.2019]
- Информатика и информационные технологии: http://window.edu.ru/catalog/resources?p_rubr=2.2.75.6 [26.10.19]
- Электронная библиотека публикаций Института прикладной математики им. М.В. Келдыша РАН http://window.edu.ru/resource/753/50753 [Дата обращения 08.11.2019]
- Коллекция журналов Economics, Econometrics and Finance: https://www.sciencedirect.com/#open-access (англ.) [Дата обращения 08.11.2019]
- ЭБС «Юрайт». Режим доступа: http://biblio-online.ru
- ЭБС «Консультант студента». Режим доступа: http://www.studentlibrary.ru

– ЭБС «Лань». Режим доступа: http://e.lanbook.com/
– ЭБС «Znanium.com». Режим доступа: www.znanium.com

д) профессиональные базы данных и информационные справочные системы

– База данных рецензируемой литературы Scopus: https://www.scopus.com [26.10.19]
– База данных Web of Science: https://apps.webofknowledge.com [26.10.19]
– База данных zbMath: https://zbmath.org/ [Дата обращения 10.09.2019
– Информационные технологии, журнал: http://novtex.ru/IT/INDEX.htm [Дата обращения 08.11.2019]
– Портал искусственного интеллекта: http://www.aiportal.ru/articles [Дата обращения 08.11.2019]
– Web-технологии: HTML, DHTML, JavaScript, PHP, MySQL, XML+XLST, Ajax: https://htmlweb.ru/ [Дата обращения 08.11.2019]
– База книг и публикаций Электронной библиотеки «Наука и Техника»: http://www.n-t.ru [Дата обращения 08.11.2019]
– ГАРАНТ. Информационно-правовой-портал: http://www.garant.ru/
– Правовая система «Консультант плюс»

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения: проектор, компьютеры, учебная мебель (столы, стулья).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду вуза.

Программа составлена в соответствии с требованиями ОС ННГУ
по направлению 09.03.03 Прикладная информатика

Автор: доцент О.В. Ясенев

Рецензент:
к.т.н., доцент, заместитель генерального директора ООО «СВТЕКНН» Д.П. Клочков

Программа утверждена на заседании учёного совета Балахнинского филиала ННГУ,
протокол № 4 от 15.04.2020 г.