

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Институт экономики и предпринимательства
(факультет / институт / филиал)

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от
« ____ » _____ 2022 г. № ____

Рабочая программа дисциплины

Информационная безопасность

(наименование дисциплины (модуля))

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

38.03.05 БИЗНЕС-ИНФОРМАТИКА

Направленность образовательной программы

**АНАЛИТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЭКОНОМИКЕ И БИЗНЕСЕ**

Форма обучения

(очная)

Нижегород

2022 год

1. Место дисциплины в структуре ООП

Дисциплина Б1.О.22 Информационная безопасность» относится к обязательной части учебного плана по программе бакалавриата.

варианта	№	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
1	Блок 1. Дисциплины (модули)	Обязательная часть.	Дисциплина Б1.О.22 Информационная безопасность» относится к обязательной части ООП направления подготовки 38.03.05 «Бизнес-информатика».

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

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	
УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности и для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных	УК-8.1. Обеспечивает безопасные и/или комфортные условия труда на рабочем месте, в т.ч. с помощью средств защиты. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте.	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	доклады, тестирование, практические задания

ситуаций военных конфликтов	и	УК-8.2. Осуществляет действия по предотвращению возникновения чрезвычайных ситуаций (природного и техногенного происхождения) на рабочем месте, в т.ч. с помощью средств защиты	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	доклады, тестирование, практические задания
-----------------------------------	---	---	--	--

1. Структура и содержание дисциплины «Информационная безопасность»

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	2 ЗЕТ		
Часов по учебному плану	72		
в том числе			
аудиторные занятия (контактная работа):	49		
- занятия лекционного типа	16		
- занятия семинарского типа	32		
самостоятельная работа	23		
КСР	1		
Промежуточная аттестация – зачет	-		

3.2. Содержание дисциплины

Наименование и краткое содержание	Всего (часы)	В том числе	
		Контактная работа (работа во взаимодействии с преподавателем), часы из них	Сам осто ятел ьная рабо та

разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)				Занятия лекционного типа			Занятия семинарского типа			Занятия лабораторного типа			Всего			обучающегося, часы		
	Очное	Очно-заочное		Очное		Заочное	Очное	Очно-заочное	Заочное	Очное	Очно-заочное	Заочное	Очное		Заочное	Очное	Очно-заочное	Заочное
1. Теоретические аспекты информационной безопасности экономических систем	16			4			6						10			6		
2. Понятие информационных угроз и их виды	14			4			6						10			4		
3. Принципы построения системы информационной безопасности	14			4			6						10			4		
4. Организация системы защиты информации	12			2			6						8			4		
5. Информационная безопасность отдельных экономических систем	15			2			8						10			5		
В т.ч. текущий контроль	1												1					
Промежуточная аттестация - зачет																		
Итого	72			16			32						49			23		

Текущий контроль успеваемости реализуется в рамках занятий лабораторного типа.

2. 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 зачету;
- 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 экономических категорий требует проработки лекционного материала, выполнения практических заданий, изучение словарей, энциклопедий, справочников.

Индивидуальная самостоятельная работа студента направлена на овладение и грамотное применение экономической терминологии в области компьютерного моделирования.

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 экономической теории, понимание экономических процессов, происходящих в обществе, 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 зачету

Промежуточная аттестация студентов по дисциплине проходит в виде зачета и предусматривает оценку «зачтено» / «незачтено». Условием успешного прохождения промежуточной аттестации является систематическая работа студента в течение семестра. В этом случае подготовка к зачету является систематизацией всех полученных знаний по данной дисциплине.

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

Желательно спланировать троекратный просмотр материала перед зачетом. 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.

Эта 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.

Для обеспечения самостоятельной работы обучающихся используется электронный курс «Информационная безопасность» по адресу <https://e-learning.unn.ru/course/view.php?id=4715>, созданный в системе электронного обучения ННГУ - <https://e-learning.unn.ru/>.

3. 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				
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько незначительных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме.	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными незначительными недочетами, выполнены все задания в полном объеме.	Продemonстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач

	обучающего от ответа						
--	-------------------------	--	--	--	--	--	--

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.	УК-8
2. Прогресс информационных технологий и информационная безопасность.	УК-8
3. Нормативно-правовые аспекты информационной безопасности.	УК-8
4. Классификация угроз безопасности информационных объектов.	УК-8
5. Основные виды каналов утечки информации.	УК-8
6. Умышленные и неумышленные угрозы информационной безопасности.	УК-8
7. Внешние угрозы информационной безопасности.	УК-8
8. Мотивы и цели компьютерных преступлений.	УК-8
9. Статьи уголовного кодекса о компьютерных преступлениях.	УК-8
10. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.	УК-8
11. Объекты информационной безопасности на предприятии.	УК-8
12. Организационные методы обеспечения информационной безопасности.	УК-8
13. Физическая защита информационных систем.	УК-8
14. Программно - технические методы обеспечения информационной безопасности.	УК-8
15. Идентификация и аутентификация.	УК-8
16. Доктрина информационной безопасности Российской Федерации.	УК-8
17. Государственное регулирование информационной безопасности в России.	УК-8
18. Несанкционированный доступ и защита от него.	УК-8
19. Проблема информационной безопасности в историческом аспекте.	УК-8
20. Предупреждение компьютерных преступлений.	УК-8
21. Типы компьютерных вирусов и защита от них.	УК-8
22. Человеческие факторы, обуславливающие информационные угрозы.	УК-8
23. Способы воздействия угроз на информационный объект.	УК-8
24. Признаки воздействия вирусов на компьютерную систему.	УК-8
25. Фрагментарный и системный подходы к защите информации.	УК-8
26. Уголовно-правовая характеристика компьютерных преступлений.	УК-8
27. Субъективная сторона компьютерных преступлений.	УК-8
28. Объективная сторона компьютерных преступлений.	УК-8
29. Способы совершения компьютерных преступлений («за хвост», «маскарад» и др.).	УК-8
30. Причины и условия, способствующие совершению компьютерных преступлений.	УК-8
31. Меры предупреждения преступлений в сфере компьютерной информации.	УК-8
32. История вредоносных программ.	УК-8
33. Защита учетной информации коммерческих фирм.	УК-8

34. Свойства экономической информации, нарушаемые при несанкционированном доступе.	УК-8
35. Исторические аспекты компьютерных преступлений.	УК-8
36. Экономическая информация как объект безопасности.	УК-8
37. Перечень сведений, которые не могут составлять коммерческую тайну.	УК-8
38. Виды тайн и как их сохранить.	УК-8
39. Причины разглашения конфиденциальной информации.	УК-8
40. Разглашение и утечка информации.	УК-8
41. Стратегия злоумышленника при несанкционированном доступе.	УК-8
42. Организация конфиденциального делопроизводства.	УК-8
43. Структура службы безопасности компании.	УК-8
44. Теоретические аспекты информационной безопасности экономических систем.	УК-8
45. Основные понятия информационной безопасности экономических систем.	УК-8
46. Экономическая информация как товар и объект безопасности.	УК-8
47. Понятия информационных угроз и их виды.	УК-8
48. Вредоносные программы.	УК-8
49. Компьютерные преступления и наказания.	УК-8
50. Принципы построения системы информационной безопасности.	УК-8
51. Подходы, принципы, методы и средства обеспечения безопасности.	УК-8
52. Организационно-техническое обеспечение компьютерной безопасности.	УК-8
53. Электронная цифровая подпись и особенности ее применения.	УК-8
54. Защита информации в Интернете.	УК-8
55. Организация системы защиты информации экономических систем.	УК-8
56. Этапы построения системы защиты информации.	УК-8
57. Политика безопасности.	УК-8
58. Оценка эффективности инвестиций в информационную безопасность.	УК-8
59. Обеспечение информационной безопасности автоматизированных банковских систем (АБС).	УК-8
60. Информационная безопасность электронной коммерции (ЭК).	УК-8
61. Обеспечение компьютерной безопасности учетной информации.	УК-8
62. Сущность криптографических методов.	УК-8
63. Организационно-административные мероприятия обеспечения компьютерной безопасности.	УК-8
64. Организация конфиденциального делопроизводства.	УК-8
65. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения.	УК-8
66. Типы и субъекты информационных угроз.	УК-8

5.2.2 Тестирование

Тесты для проверки компетенции УК-8

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

Вопрос 6. Политика безопасности не включает в себя

- а. объект информационной безопасности
- б. обеспечение информационной безопасности
- в. угрозы объекту информационной безопасности
- г. все ответы верны

Вопрос 7. К объектам информационной безопасности на предприятии не относят

- а. информационные ресурсы
- б. средства и системы информатизации
- в. субъекты информационной безопасности

г. коммерческое предприятие

Вопрос 8. Сегмент деловой информации относится к следующему виду рынка

- а. финансовый
- б. информационный
- в. товарный
- г. услуг
- д. биржевой

Вопрос 9. К свойствам информации как товара относят

- а. репрезентативность
- б. адекватность
- в. несамостоятельность
- г. достоверность
- д. доступность

Вопрос 10. Объекты профессиональной тайны

- а. врачебная тайна
- б. тайна страхования
- в. тайна связи
- г. тайна усыновления
- д. все ответы верны

5.2.3 Практические задания

УК-1

Задание по поиску нормативных документов с использованием «Консультант Плюс»

- 1) Запустим систему Консультант Плюс.
- 2) Создадим папку в системе «Консультант Плюс» с именем Информационная безопасность Иванов (Ваше фамилия) (траектория Избранное – Создать папку).
- 3) Найдём основной закон о защите информации принятый летом 2006 года. Для этого перейдем в Карточку поиска.
- 4) Для этого заполним поля: «Вид документа», «Дата» и «Название документа».
- 5) Поле «Дата» заполняется с помощью Диапазона дат.
- 6) Построим список документов
- 7) Нами был найден Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.04.2011) «Об информации, информационных технологиях и о защите информации».

- 8) Откроем найденный закон, дважды щелкнув на его название
- 9) В текущем документе найдем понятие «Конфиденциальность информации» с помощью кнопки «Найти».
- 10) Поставим закладку рядом с найденным понятием. Для этого щелкнем слева от него и далее выберем «Добавить – Закладки» и «Документы – кнопка Добавить».
- 11) Вернемся в «Карточку поиска» и выберем «Избранное». В поле «Закладки и документы» появилась закладка.
- 12) Аналогично поставим закладки для понятий «информация», «электронный документ» и статьи «Защита информации».
- 13) Добавим найденный закон в папку Информационная безопасность по траектории: Добавить – Папки – Информационная безопасность.
- 14) Вернемся в «Карточку поиска» и выберем «Избранное». В поле Папки - Информационная безопасность появилась ФЗ №149.
- 15) Найти документ «Доктрина информационной безопасности Российской Федерации» и Федеральный закон №152-ФЗ «О персональных данных». Сохраним их в папку «Информационная безопасность».
- 16) В найденных документах поставим закладки для понятий «персональные данные», «уничтожение персональных данных» и правовые методы информационной безопасности.
- 17) Проверьте наличие созданных закладок.
- 18) Закончить работу с программой.

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 особенностях 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»	

Практические задания на шифрование информации

Различают следующие алгоритмы простых шифров:

- перестановка – символы исходного текста переставляются по определенному правилу внутри блока текста. Например: ШААМ (МАША).
- замена – символы исходного текста заменяются другими символами или кодами того же или другого алфавита. Например: 14,1,26,1 (МАША).
- гаммирование – символы исходного текста складываются с символами случайной последовательности, которая называется гаммой шифра.
 • Например: при гамме 1, 2, 3, 4 сообщение 15,3,29,5 расшифровывается как (МАША). Стойкость шифра определяется длиной гаммы.
- аналитическое преобразование – блоки исходного сообщения преобразуются по некоторой формуле или алгоритму

Шифр простой замены состоит в том, что символы исходного текста заменяются другими символами или кодами из того же или другого алфавита.

Задание 1

Расшифровать простую замену при известном коде

7 8 2 25 23 10 15 23 28 1 5 20 18 2 7 25 4 33 23 14 8 18 5 20 33 18 10 14 24 8 25 5 32 14 5 11
28 8 14 15 5 28 5 15 14 11 24 5 8 2 28 19 18 30 5 11 33 19 33 23 5 4 2 14 8 5 6 18 22 33 20 5 20 33
18 20 32 14 5 8 14 6 25 1 5 10 14 11 14 5 3 28 20 18 2 25 32 14 5 4 2 33 18 7 32 33 10 18 5 18 20 14
32 18 5 19 33 10 4 33 8 25 5 11 33 19 25 5 15 23 33 14 19 33 5 32 25 4 2 25 10 32 33 29 14 10 15 21
5 8 32 14 1 5 2 25 11 33 15 25 1 5 5 18 5 8 14 6 25 1 5 23 10 24 3 18 14 5 8 14 6 25 5 10 23 33 18 5
25 5 8 14 32 21 5 10 14 8 21 20 17 1 5 19 33 10 4 33 8 28 5 11 33 19 28

5 15 23 33 14 20 28 4 33 34 18 15 25 1 5 33 15 22 25 5 15 23 33 14 19 33 5 18 5 20 25 15 21 5
15 23 33 16 32 14 5 28 11 18 23 25 1 32 14 5 4 2 14 6 16 11 33 8 14 1 10 15 23 28 1 32 14 5 3 2 25 8
18 32 14 5 4 2 33 18 7 32 33 10 18 5 6 33 13 32 33 19 33 5 10 23 18 8 14 15 14 6 21 10 15 23 25 5 32
25 5 11 6 18 13 32 14 19 33 5 15 23 33 14 19 33 32 14 5 13 14 6 25 1 5 8 33 20 25 5 11 6 18 13 32 14
19 33 5 15 23 33 14 19 33 5 32 14 5 13 14 6 25 1 5 13 14 32 17 5 11 6 18 13 32 14 19 33 5 15 23 33
14 19 33 5 32 18 5 2 25 11 25 5 14 19 33 5 32 18 5 33 10 6 25 5 14 19 33 5 32 18 34 14 19 33 5 34 15
33 5 28 5 11 6 18 13 32 14 19 33 5 15 23 33 14 19 33 7 25 4 33 23 14 8 18 5 20 33 30 25 20 20 14 8
25 32 14 5 4 2 18 8 25 23 25 1 5 19 33 10 4 33 8 28 5 10 33 15 33 23 25 2 18 27 14 1 32 14 5 28 11 18
23 25 1 5 8 14 15 14 1 5 10 23 33 18 30 5 2 25 8 18 5 11 14 8 32 33 10 15 18 5 10 23 33 14 1 2 33 8
18 15 14 6 24 20 5 11 6 25 19 33 8 14 24 32 18 14 10 33 15 23 33 2 24 1 5 20 33 6 18 15 23 28 11 33
1 10 24 5 20 14 2 7 33 10 15 14 1

Ключ:

А	Б	В	Г	Д	Е	Ё	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	
25	11	23	19	8	14	9	13	7	18	1	3	6	20	32	33	4	2	10	15	28	12	30	22	34	29	27	21	17	31	26	16	24	5

Поиск ключа простой замены основан на анализе статистических свойств шифрованного текста. Замечено, что во всех языках разные буквы встречаются в текстах с разной частотой. Для поиска ключа простой замены следует выполнить три шага:

- 1) Вычислить в процентах частоты встречаемости каждого кода в шифрованном сообщении. Упорядочить по убыванию.
- 2) Вычислить в процентах или найти частоты встречаемости каждой буквы алфавита в русском тексте. Упорядочить по убыванию.
- 3) Сравнить частоты встречаемости кодов и букв и неформальным путем найти их соответствие. При этом надо иметь в виду, что соответствие приблизительное. Используется смысл сообщения, короткие слова.

В задании 2 требуется найти ключ простой замены и расшифровать.

Задание 2 (Вариант 1)

10 32 25 30 11 16 12 26 11 4 12 26 10 22 24 10 14 4 18 20 30 25 30 26 10 13 15 6 13 8 32 10
14 20 24 26 13 26 8 32 16 29 18 16 21 26 11 30 4 8 16 30 26 28 21 14 31 26 23 16 30 25 30 26 23 13
8 32 10 14 20 24 26 26 32 10 4 18 26 8 18 1 16 31 26 18 1 4 18 7 16 32 26 11 32 4 30 20 24 12 26 19
13 16 33 34 18 12 26 10 4 24 28 32 32 14 26 15 30 4 30 20 24 12 26 26 33 26 6 30 11 18 16 32 26 4 2
28 30 20 31 26 13 26 16 24 10 26 20 26 18 1 28 21 14 33 32 26 14 32 15 4 18 14 10 12 26 13 26 33 24
8 11 30 25 30 26 20 26 25 6 13 11 18 26 4 13 22 7 32 26 23 21 26 15 6 30 15 31 32 23 26 32 32 26 11
30 26 16 18 14 33 18 26 16 30 26 20 6 24 25 13 26 20 26 30 28 18 11 13 26 16 32 26 11 24 11 18 23
26 26 11 32 16 31 26 33 30 14 30 6 21 27 26 15 4 30 3 30 26 16 24 22 24 14 26 16 32 26 28 6 24 16
18 26 14 30 10 33 4 18 20 30 26 16 30 12 26 15 30 14 30 23 13 26 22 14 30 26 18 26 13 11 24 22 24
26 13 14 6 30 23 26 10 15 18 14 26 30 14 26 15 32 6 32 15 30 12 26 26 23 16 32 26 8 24 4 31 26 16
32 28 30 10 20 30 11 26 5 14 30 14 26 10 18 16 18 27 26 8 24 4 31 26 1 32 23 4 2 26 18 26 8 18 1 16
18 26 30 10 33 30 4 33 18 26 23 16 32 26 10 14 6 24 7 16 30 26 22 14 30 26 10 21 14 21 32 26 10 20
18 16 31 18 26 10 14 6 24 7 16 32 27 26 22 32 23 26 25 30 4 30 11 16 21 32 26 20 30 4 33 18 26 26

30 25 6 30 23 32 16 26 11 30 4 25 26 16 24 7 26 6 24 1 16 21 23 26 4 2 11 12 23 26 24 26 28 4 18 1
 33 18 23 26 28 30 4 32 32 26 11 6 13 25 18 3 26 11 30 4 8 16 21 26 23 21 26 14 32 23 26 33 30 25 30
 26 23 21 26 4 2 28 18 23 26 13 8 32 26 1 24 26 14 30 26 22 14 30 26 4 2 28 18 23 26 18 3

Задание 2. (Вариант 2)

16 32 26 10 14 32 10 16 12 27 10 12 26 15 31 12 16 18 34 24 26 26 16 30 10 24 26 10 20 30
 32 25 30 26 26 30 16 26 20 32 11 31 26 10 26 16 24 7 18 23 26 1 16 24 23 32 16 32 23 26 34 20 32 14
 24 26 30 11 16 30 25 30 26 26 12 26 33 26 11 24 23 24 23 26 30 11 6 12 3 4 32 20 26 16 32 26 30 3 4
 24 11 32 4 26 12 26 15 6 30 10 14 30 26 18 3 26 30 10 14 24 20 18 4 26 16 24 26 15 30 14 30 23 26
 33 30 25 30 26 16 24 26 5 14 30 23 26 10 20 32 14 32 26 16 32 26 13 10 15 32 4 26 16 24 11 32 2 10
 31 26 12 26 15 30 1 16 24 14 31 26 13 8 32 26 16 24 26 14 30 23 26 26 8 11 24 4 24 26 10 15 24 10
 18 14 32 4 12 26 6 30 10 10 18 12 26 8 18 4 24 26 14 24 10 13 12 26 19 30 14 30 25 6 24 19 18 18 26
 18 26 16 24 33 30 16 32 34 26 15 6 18 7 32 4 26 23 32 10 10 18 12 26 18 26 16 32 26 30 11 18 16 26
 24 26 20 26 20 18 11 32 26 23 24 19 18 18 26 26 16 32 26 10 4 24 20 30 27 26 16 32 26 10 33 24 16
 11 24 4 30 23 26 16 32 26 25 6 32 3 30 23 26 14 32 23 26 28 30 4 32 32 26 16 32 26 13 10 14 16 30
 27 26 33 24 16 18 14 32 4 31 2 26 15 30 5 14 21 26 15 6 30 20 32 6 12 2 14 10 12 26 10 14 18 3 30 23
 26 33 24 33 26 28 24 28 21 26 15 6 30 20 32 6 12 2 14 10 12 26 15 30 10 14 32 4 31 2 26 26 13 26 1 6
 32 4 21 3 26 6 24 1 20 24 4 18 16 26 18 26 11 6 12 3 4 21 3 26 2 16 34 30 20 26 14 24 33 30 32 26 33
 26 15 30 33 30 2 26 10 14 6 32 23 4 32 16 18 32 26 33 24 33 26 28 13 11 14 30 26 10 20 24 4 18 4 24
 10 31 26 13 10 14 24 4 30 10 14 31 26 30 14 34 30 20 26 16 24 26 6 21 3 4 21 3 26 11 32 14 32 27 26
 15 30 33 30 4 32 16 18 32

Алгоритм перестановки содержит правило перестановки символов.

Перестановка с матрицей заключается в записи исходного сообщения в строки матрицы слева направо, сверху вниз. Количество столбцов матрицы является ключом шифра. Шифрованное сообщение получается при считывании текста по столбцам матрицы сверху вниз, слева направо. Необходимо учитывать, что последняя строка матрицы почти всегда получается неполной. Ее длина вычисляется с помощью длины всего сообщения и ключа. Расшифрование заключается в проведении этих двух операций в обратном порядке.

Пример: 6 столбцов.

в	с	е	б	у	д
е	т	т	а	к	к
а	к	м	ы	х	о
т	е	л	и		

всебудеттаккакмыхотели↔еатс ткеет млбаы иукхд ко

Перестановка с ключевым словом задает дополнительно порядок считывания столбцов матрицы. Количество столбцов равно количеству букв у ключевого слова. Порядок считывания столбцов задается порядком букв ключевого слова в алфавите, одинаковые буквы нумеруются слева направо.

Пример: Ключевое слово - батрак. Количество букв – 6. Порядок букв по алфавиту - 3,1,6,5,2,4.

всебудеттаккакмыхотели↔сткеу кхвеа тдкоб аыйет мл

в	с	е	б	у	д
е	т	т	а	к	к
а	к	м	ы	х	о
т	е	л	и		

В задании 3 необходимо расшифровать сообщения, зашифрованные перестановкой с ключевым словом. В вариантах 1-3 ключ = РАДИАТОР, в вариантах 4-6 ключ = ЕККЛЕСИАСТ
Задание 3. (Вариант 1).

сеиве неави ежвро еуррк _о_см т_тма же_с щемтр рмдры смввя ибьяе аяаев асмми
о_о_ _а_ь нВо_ в_рд_мра_ы повая_дВжи уВсив _н_ее опмря яньня те рврчр р_трк ряья
аяаеи яьясе аееу вреае тмтмв мшром тмьюи вьрья ьписВ иваВз исВав еб_р а_л_м_т_тмт
_я роваяе р_ок ебро_тятмт_ымер н_ьят_еврс маквб амаен оимае аясар имятм ятйс_ааи
ят_би утбВт_лрбь ис_ри вляеа ипВзт_ьВн_ксъ_ьяьрв нмаио_ьо рает_тмт_т_мтя_ВеибВ
зисет мьсья ьрьяь мья_б_а_и_ее евоеи виВкр яяаеа яаеас вrmгр смррв_итрр_ррд_ш рчрое
тмиее яьяят_инт_иеае рмяд м_мт мия_еяимм иг_юв н_ору Влввр иеврн мо_оВ браВй
е_ь_л_евь вр тыю_а нсьи_ежЕд с_уак евавп амгчр Ч,ето_б_н с,био ,но_щ тд_ял_ечте
щеомд мосдм д_рео_т_от ст,_е лlea_нты_а ло_,м доте, бол_о еоаз, папЧз атнот б_ьид у_и_
стама таьто_и_ор_у_о вдм_з_р_р обуое ут_п_ь_тыяп цт_ее_е

Задание 3. (Вариант 2).

есм_е ашнот вд_нюн_т сотме оявсв е_т,у тбмоо_пeб_ло_жл_ь_и_иево аанИс итоза
_сн_т_т_т нтсом_ебн_я_жак гпяос оыире ср_Пс одоки ьитто пнрсв Нио,ц дезлэ о_тик еаме_
оге_в пкмд_писол иугад в_в,л оаитр зоео_пи_в ун_вб рсогу зпео ош_ео гоиЛ_,_па о_ии_
щощее еннгъ тдлоб суо_о иод_о лн,еп чбнб_лдеи ьтлн_аеа_т Ке,мп е_е ьиьс_ат_с_о,инт
лтиь_бн_тч алещж щей ея_в_о,ота отик_в_уоу оие_роИн_н_осо ы_йто гт_во_"_вда мемед
_вдрь ио-_м еекн_нтвм ь_ве_иожнй_еооН лмвлл югЭкв св_от ,соа_по_"_б_ео, всв_з ситхт
нишбо сийжл г_т_,_с рт_в_ьооал росс; лг_т_ос_няооб онзг_!_ета_м_о, еыо-б б_три бтопт
_уКто етбкт тултт тирни е_исм о_ею етые_юат_о Ис

а_мор ,ит_оьтот й_ркх апмол ев_з_сатки нетдо теке_ияь_т_рко_би_, пИ_мр ео_ки
иокоу нст_н иы_то_р_не уг_на шмдал ,_яеш ауаои окечв о_Ижу м_ж атуаК лирей_им,г з_вэи
:патК_е_ив егтте мдиле отс_к_г_то_е_од_ын_мв кхаши_а_я дилит_зчрн ? о_оЕи ссмх_
ктчшо ь_ждо роетн бстля_ск_артья_втивл олои_абвдх иВяд_паьое хЕс_:_нтр са_ат ег_ид
о_уис

Задание 3. (Вариант 3).

ед_ад ьолтр улл_сцхм, _-_.н иытыд рдррд чцхми еудау ппеды оае_е ясгре поор_-слв
еПя,_я,ряе Сувлр пдеид мегии_м_пе у_ср_д_к_т.е_е_г_в_яхйсм атц оанге уогцу а_вем
н_аол чкоел ч,ишо .дшае йврКл_еплс ое_р_ын_ч_лты_е_е_ж_чш_гя йодаз отоел_хиоо
иш"_энб шнд_смнсм готиы еинпп я,иты оепд_ы"буь л_е_я Ниоеи уеВаи уг_ча ргрнл
н_лчз авсрй вч_и н?_лл банял см_т_аг_ое сигео орвеи днаи_втиви. еоянм випсй твose гт_ью
ебрт, ие_тм нлсд_итесе йдн_В сяеир_вное жлчва сунпк_двч_оес_е_:не в_ны_и елтив
ям:ти ?дг_:трвр ткд_к_д_иу кгвил уае_е ах_за еьвяе пгмоа б_б_и рел_ет_а рнб_е а_е_а
нзоед нлбшо_ясмз бьНве еезбт смч_о етлое_ьм_с сшрег епс,у меуне_оа_е_ы_ор. Нсс_а бом_б
яе_иь н_и_в еееа_ыиш_итек ымубр_я_дем ме_Нв вн,йб_едо, ы_идч_с_йу буч_о?лро лрлрг
ы_б_екч ныуи_гешт_ее_, еййсе швект тсмоб_ьаоан_чау а,цу_дпоа кнеер_ям_та сд_Ия
ориоо тр_,_я,н лтка_тотк рр_р_тмнь д_р_с_ие_ллри у_ьт ушт_ж_ч-и_ликбс_губ.
иОяц_зм_,_л_мн ооссе иевыт еедЕ ссдм, уи_ьм еосеп т_ек_орен рлу_а иеомы ,тсза че_,
_еик ооат_юс

Задание 3. (Вариант 4).

вияпВ аесьв веВ_р_й_мс_рдмьо ум_що о_р_ысс_с_дрт а_ьжс ве_ня яуеая_еерм
ве_м_мт_пм еяебр иияьв о_яви мжван ирао_кортм_аран еводе ьяВже тн брв_тм_мВ аязьв

ипвтя иасая Ваяув еяьсе ьсрт_ рртл рьевь Вуеьа есм_р ршм к мя_ч мт_рт_ иеар иряие вмта_о_я еварт_ иинр яоВвм_бкет раятя я_лмы иса_и лос_с_айбн бвн_р аяВра мьет_стет_рамя_мьуаи мьпес н_кя_к_й_и яяв_о мо_от тртаь вр_ие тбоеь з_раВ ммьь се_рр та_вВ т_еая Виеьа_ясио яьсир ьевар иирьт мт_рр ме_ея ьбеая мир__рмт__втб_с__шкм Вееьз вааяр гм_др т_орилр иявВа я_ият омьив минр_имвр_ввм_у рт_Вт_ьйе ьгryn_н_м_ое_еВ ем__о_я_аеи рлетю ед_рч мьбме ве_ьюеи ьтъуж епму_ерааЧ_м,оя_ейтб__м,з мднпо тдро_еоо_е нотоо аалат чдб_т буц_е смипт дтру_н__р_ьвс_зеье оа_н_Чтьч_лиоса ас,п_боатт о_тто длт_к_т_рот__у_и с__Ел_ц_ан__взщг мtle, де_о: дб,ам ьео_с оп_е_яд_ае_в_

Алгоритм гаммирования заключается в сложении символов исходного сообщения с символами некой последовательности, которая называется гаммой шифра. Есть мнение, что гаммирование придумали советские криптологи во время Великой отечественной войны.

Складываются коды этих символов. Коды равны номеру символа в алфавите. Если при сложении получается число, большее длины алфавита, то из него вычитается длина алфавита. Длинное сообщение режется на блоки с длиной гаммы.

Расшифрование заключается в вычитании из символов исходного сообщения символов гаммы. Если при вычитании получается неположительное число, то к нему прибавляется длина алфавита

В задании 4 требуется расшифровать сообщение. Используемый алфавит и порядок нумерации символов дан в варианте 1 задания 4, в других вариантах они такие же. Во всех вариантах гамма = **Молодежь в прошлом.**

Задание 4 (Вариант 1).

ю П д П ц Т Х и ! 3 ч Ц н ! д к Р Х ? ! Ъ Э Ц Р Х х * у ? Ю Ю П] Р в Э : Э э С У Ч Ц е \$ Г
я Р ~ ! з Щ П ю : П Э Ы К Ы З в \$ Ф _ ~ Ю П Э э Ъ Н Д П ч л Ц Ш Й лю ф ь ~ Ю Ч к Ц Э Ш

Й Щ Ъ ! Т Л ш р ф Г ш Р Ц б] Э б Н = Ч Ц Э 3 ш ш К т Ы ь ~ Ю к ж С з Ъ 5 Ф э У К Ш П
* # Х т Ы Щ ! л Ф Я Н : П Ш Ч \$ ч Х к ь ф я Х " С к Ю П л ? я э Щ У Й Л Э ? Е ? Ъ Я Ы ж М б а
Ю С б Э Й О Щ * ~ С ш Ш Ъ Э в э ж Т 8 Э О Ф П ц ш м ч У ч з С б] Э С Ы 5 Ы э Я У К П п ч О
_ Ъ # ! И Ъ Ю Э ; а Ю в ц Й Х Я ! У _ ! " Э ж Ф ! Ы Д Ф Щ л ц Х Т л (Л ч " " А з Ц Я Н ? ! у (! ь
ш 0 Л ! ? У Ф ~] Р Э ю : ~ э м ч о

Алфавит и кодировка (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
ь ы ь э ю я

Задание 4 (Вариант 2).

, ! Я б Х Ж Щ е э ф ф б р Щ б С ! Ъ _ У С Х Й б ш л \$ Р ! б Щ б Ю Ч л Ъ ; ! Н в Й Щ а в х
С ? Э С з Ю Х ! Ю ? Я М Ъ а ц ш в # О ь ~ в Ф Ъ Ъ У Ъ М з Щ о д ч У л э С ц Х Ч л] У П П

? Я М ! 3 Ф О щ ю И \$ ~ У ! к О Э Х Ю Я Я Щ Н ч И н т К ц л " Ю й М С Ш 2 Ъ Ф о х ч П
Ю ! ф + в С ! е Ъ Ъ Ы 1 Ф Т л ц У М Я \ Р ! б Щ Ы Щ ь ! Ъ 2 С з У К Ц Н Э я Р т ! " Ю й Ъ а Я ; !
Я Х Е Ч Ф Э А ф Х Х в Ч з Р ! ф и % ! ! И ш ш б ! ф я " о ~ ~ 9 П е Ю Ы Ф Я ц К Х о \$ Л х ~ Ы Я
б Ю Ч д 2 а Ц Э О ч Ш п т 3 ь Ш # ! = С б Х Ю Р Ъ Ъ б Ю М * я И ? б Ъ в с М н Я > о э а 3 Ф П т
? У ! Ф Щ б Ю ч Ф Ц Я ! . Ч Й О У л > ф ь Ю Ю Ф п э Ы Х = П э в Л Л ш к ч ф ! з Ц Ъ х э У Н 8
Ф Ц ~ ц + К е ~ И \$ Ъ Ч в э Х Э 2 е э ц ы ь ь _ ? О ч в " У з э Ъ я

К ~ ф

Задание 4 (Вариант 3).

* б М ! С Ф Т л ц И ш м " Я Щ Э б Ш 2 Ъ Щ П ц К Х * х О % С Щ Ъ ф э У а Е Ч ю ! 1 Ф Т
л ц Ю ч ~ Ъ н Э Ф ! Ф 8 Э Ц Э М У М к я Ю ? Ш " Ъ Ю Ъ П С 5 С з ~ ц 3 П з ! Ж ц Р " Э ж Ф ! Ъ
2 ! Н в Й Щ Щ * ~ С (Ю Х Ч ли ! Ъ _ ! Ш Э Р Ф Л в ш Я ? С м Ъ ф б ! П = Ф Ш Ф Т ш ш Й э Г
ц Ю Ц ! и Ъ Щ Ъ 8 Ф Щ Ч К ч Ш в х С ц Э р з ж С Т Ы Ю У Щ о ц У М * # Ц ю Х Ц б] Э Э в =
П Щ Ч Ч в ш к т Ы % ~ Ы в ди ба = в ю ! } С П к _ Р \ Щ " Т з Ъ з Ы 7 я э 1 Е И П и ! Р ? ч) # \ !
! Ш 2 б э У У ч Ф + + х б _

5.2.4 Темы для устных докладов по темам

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
15. Проблемы обеспечения безопасности в IP-сетях
16. Уязвимость IP-сетей
17. Межсетевые экраны
18. Типы межсетевых экранов
19. Механизмы трансляции сетевых адресов
20. Виртуальные частные сети (Virtual Private Networks - VPN)

6. Учебно-методическое и информационное обеспечение дисциплины (модуля) «Информационная безопасность»

а) основная литература:

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1013711>

2. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189328>

3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/405000>

б) дополнительная литература:

1. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности : учебное пособие / Е. К. Баранова, А. В. Бабаш, Д. А. Ларин.

- Москва : РИОР : ИНФРА-М, 2020. - 236 с. - ISBN 978-5-369-01788-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1118462>

2. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1178152>

3. Гришина, Н. В. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 239 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-545-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1001363>

4. Информационная безопасность и защита информации : учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Правоохранительная деятельность, специальности 37.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, Д. Ю. Крюкова, А. Н. Наимов, В. В. Мухин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН России, 2018. - 59 с. - ISBN 978-5-94991-428-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1229037>

5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1137902>

6. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189327>

в) программное обеспечение и Интернет-ресурсы

- ППП «Microsoft Office»
- ИПС «Консультант +»
- ИПС «Гарант»
- Поисковые система «Яндекс», «Google»
- alt.security
- alt.security.index
- comp.risks
- comp.security.announce

- comp.security.firewalls
- comp.security.misc
- comp.security.unix
- <http://ciac.llnl.gov/>
- <http://csrc.nist.gov/>
- <http://www.8lgm.org>
- <http://www.cs.purdue.edu/coast/coast.html>
- <http://www.cs.purdue.edu/homes/spaf/hotlists/csec.html>
- <http://www.telstra.com.au/info/security.html>

7. Материально-техническое обеспечение дисциплины (модуля)

Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные по помещения должны быть укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей).

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Программа составлена в соответствии с требованиями ОС ВО по направлению 38.03.05 «Бизнес-информатика», профиль «Аналитические методы и информационные технологии поддержки принятия решений в экономике и бизнесе».

Автор (ы)

к.э.н., доцент

П.С. Шалабаев

Рецензент (ы) (*на усмотрение разработчиков ООП*) _____

Заведующий кафедрой _____

Программа одобрена на заседании методической комиссии Института экономики и предпринимательства от « ____ » _____ 2022 года, протокол № .