

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

«16» июня 2021 г. № 8

Рабочая программа дисциплины

Информационная безопасность

(наименование дисциплины (модуля))

Уровень высшего образования

бакалавриат

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

09.03.03 Прикладная экономика

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Прикладная информатика в экономике

(указывается профиль / магистерская программа / специализация)

Форма обучения

очная, очно-заочная, заочная

(очная / очно-заочная / заочная)

Нижний Новгород

2021 год

Лист актуализации

Визирование РПД для исполнения в очередном учебном году

Председатель МК

_____ 2019 г.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2019-2020 учебном году на заседании кафедры

информационных технологий и инструментальных методов в экономике

Протокол от 05 марта 2019 г. № 8

Зав. кафедрой _____

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

информационных технологий и инструментальных методов в экономике

Протокол от 14 апреля 2020 г. № 4

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

информационных технологий и инструментальных методов в экономике

Протокол от 05 марта 2021 г. № 3

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 _____

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.21 Информационная безопасность относится к обязательной части учебного плана ООП 09.03.03 Прикладная информатика.

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. Способен использовать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных	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
		доклады, тестирование, практические задания

технологий и с учетом основных требований информационной безопасности	навыками решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности
--	--

ОПК-3.2.

Способен применять информационно- коммуникационные технологии решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности.	Знать	доклады, тестирование, практические задания
	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	

ОПК-3.3.

Способен стандартные профессиональной деятельности соблюдением требований информационной безопасности.	решать задачи	Знать	доклады, тестирование, практические задания	
				принципы подготовки обзоров, с 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, 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-		

ОПК-4	ОПК-4.1.	Знать	доклады, тестирование, практические задания
Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	Способен продемонстрировать знание основных стандартов, норм и правил оформления технической документации на различных стадиях проектирования и поддержки жизненного цикла информационной системы.	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	
	ОПК-4.2.		
	Способен применять стандарты, нормы и правила (в том числе установленные самостоятельно) при оформлении технической документации на различных стадиях проектирования и поддержки жизненного цикла информационной системы.	Знать	доклады, тестирование, практические задания
		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	
	ОПК-4.3.		
	Способен составлять техническую документацию на различных этапах жизненного цикла информационной системы.	Знать	доклады, тестирование, практические задания
		основные инструменты информационной безопасности при составлении технической документации	
		Уметь	
		применять методы и средства информационной безопасности на различных этапах жизненного цикла ИС	
		Владеть	

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно- заочная форма обучения	заочная форма обучения
Общая трудоемкость	4 ЗЕТ	4 ЗЕТ	4 ЗЕТ
Часов по учебному плану	144	144	144
в том числе			
аудиторные занятия (контактная работа):		34	14
- занятия лекционного типа	66	16	4
- занятия семинарского типа	16	16	8
	48		
самостоятельная работа	42	74	121

КСР	2	2	2
Промежуточная аттестация – экзамен	36	36	9

Наименование и краткое содержание разделов и тем дисциплины	в том числе					Самостоятельная работа обучающихся в часах
	Всего (часы)				Самостоятельная работа обучающихся в часах	
	Контактная работа (работа во взаимодействии с преподавателем), часы					
	из них					
	Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Занятия Всего		
	Оч	Оч	Оч	Оч		

	а я	Оч н О - з а О ч н а я	Зао ч н а я	Оч н а я	Оч н О - з а О ч н а я	Зао ч н а я	Оч н а я	Оч н О - з а О ч н а я	Зао ч н а я	Оч н а я	Оч н О - з а О ч н а я	Зао ч н а я	Оч н а я	Оч н О - з а О ч н а я	Зао ч н а я	Оч н а я	Оч н а я
1. Теоретические аспекты информационной безопасности экономических систем	14	18	21	2	2	1	6	2					8		4	1	6
2. Понятие информационных угроз и их виды	20	19	27	2	2	1	10	2	2				12		4	3	8
3. Принципы построения системы информационной безопасности	22	23	27	4	4	1	10	4	2				14		8	3	8
4. Организация системы защиты информации	22	23	27	4	4	1	10	4	2				14		8	3	8
5. Информационная безопасность отдельных экономических систем	28	23	31	4	4			4	2				16		8	2	12
В т.ч. текущий контроль	2	2	2										2		2	2	
Промежуточная аттестация - экзамен	36	36	9														
Итого	144	144	144	16	16	4	48	16	8				64		34	12	42

Практические занятия (семинарские занятия /лабораторные работы) организуются, в том числе в

форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: выполнение проекта, решение прикладной задачи.

На проведение практических занятий (семинарских занятий /лабораторных работ) в форме практической подготовки отводится 10 часов.

Практическая подготовка направлена на формирование и развитие:

- практических навыков в соответствии с профилем ОП:
 - Участие в организации работ по управлению проектами информационных систем;
 - Сбор и анализ детальной информации для формализации предметной области проекта и требований пользователей заказчика, интервьюирование ключевых сотрудников заказчика;
 - Формирование и анализ требований к информатизации и автоматизации прикладных процессов, формализация предметной области проекта.
- компетенций - ОПК-3, ОПК-4.

Текущий контроль успеваемости реализуется в рамках занятий практического типа.

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 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 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 трехкратный 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.

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.

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

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/>.

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

1. Описание шкал оценивания результатов обучения по дисциплине

Уровень
сформированнос
ти компетенций

Шкала оценивания сформированности компетенций

плохо

неудовлетворительно
удовлетворительно

хорошо

очень хорошо

отлично

превосходно

Не зачтено

зачтено

<u>Знания</u>	Отсутствие знаний						
	теоретического материала.	Уровень знаний ниже	Минимально допустимый уровень знаний.	Уровень знаний в объеме, соответствующем программе подготовки.	Уровень знаний в объеме, соответствующем программе подготовки.	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Имели место грубые ошибки.	Допущено много негрубых ошибок.	Допущено несколько негрубых ошибок	Допущено несколько негрубых ошибок	Допущено несколько негрубых ошибок	Допущено несколько негрубых ошибок
	Отсутствие минимальных умений .	При решении стандартных задач не продемонстрированы основные умения.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками.	Продемонстрированы все основные задачи с негрубыми ошибками.	Продемонстрированы все основные задачи .	Продемонстрированы все основные умения, решены задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения, решены все основные задачи.
<u>Навыки</u>	Отсутствие владения материалом.	При решении стандартных задач не продемонстрированы базовые навыки.	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
	Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	Имели место грубые ошибки.	Имели место грубые ошибки.	Имели место грубые ошибки.	Имели место грубые ошибки.	Имели место грубые ошибки.	Имели место грубые ошибки.

Шкала оценки при промежуточной аттестации

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»
	Удовлетворительн о	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 но	Неудовлетворительн	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

ОПК-3

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:

25	А
11	В
23	В
19	Г
8	Д
14	Е
9	Е
13	Ж
7	З
18	И
1	И
3	К
6	Л
20	М
32	Н
33	О
2	Р
10	С
15	Т
28	У
12	Ф
30	Х
22	Ц
34	Ч
29	Ш
27	Щ
21	Ъ
17	Ы
31	Ь
26	Э
16	Ю
24	Я
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↔веатс 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 асммй о_о__а__ь
нВо__в_рд_мра_ы повая _дВжи уВсив _н_ее опмря яньня те рврчр р_трк ряьяа аяаеи яьясе аеееу вреае
тмтмв мшром тмьуй вьрья ьписВ иваВз исВав еб_р а__л_м__т_тмт __я ровая р__ок емро _тятмт
__ымер н_ят_еврс маквб амаен оимае аясар имятм ятйс __ааи ят_би утбВт _лрбь ис_ри вляе ипВзт
__ьВн _ксь_ьяьрв нмаио __ьо рает_тмт_т мтя__ВеибВ зисет мсья ьрьяь мья_б __а__и_ее евоеи виВкр
яяаеа яаеас врмгр 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_ид
у_и_: стама таьто __и_о р_у_о вдм__з_р_р обуое ут_пъ _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_обыре_ср_Пс_одоки_ыитто_пнрсв_Нию,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_лдееи_ытлн_aea_т_Ке,мп_е__е_ыьс_ат_с_о,инт_лтиь_бн_тч_алещж_щеи_ея_в_о,ота_отик_в_уоу_оие__роИн_н_осо_ы_йто_гт_во_"_вда_мемед_вдрь_ио-_м_еекн_нтвтм_ь_ве_иожнй_еооН_лмввл_юг_Экв_св_от_,соа__по_"_б_ео,_всв_з_ситхт_нишбо_сиижл_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_эею_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_кхаша__а_я_дилит_зчрн_?_о_оЕи_ссмх_ктчшо_ь_ждо_роетн_бстля__ск_артья_втвл_олои_абвдх_иВяд_паьое_хЕс__:_нтр_са_ат_ег_ид_о_уис

Задание 3. (Вариант 3).

ед_ад_ыолтр_улл__сцхм, _-_н_иытыд_рдrrд_чцхми_еудау_ппеды_оae_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_оee_р_ын_ч_лты_е_е__ж_чш_гя_йодаз_отоел_хиоо__иш_"энб_шндо_смнсм_готиы_еинпп_я,иты_оепд_ы"буь_л_е_я_Ниюеи_уеВаи_уг_ча_ргрнл_н_лчз_авсрй_вч__и_н?_лл_баныл_см_т_аг_ое_сигео_орвеи_днаи_втви_.еоянм_випсй_твосе_гт_ью_ебрт, _ие_тм_нлсд_итесе_йдн_В_сяеир_вное_жлчва_сунпк_двч_оес_е__не_в_ны__и_елтнв_ям.ти_?дг__т:рвр_ткд_к_д__иу_кгвйл_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_ееea__ыиш__итек_ымубр_я_дем_ме_Нв_вн,йб_едо, _ы_идч_с_йу_буч__о?лро_лрлрг_ы_б_екч_ныуи__гешт_ее_,_еийсе_швект_тсмоб_ьаоан_чиау_а,цсу_дпоа_кнеер_ям_та_сд_Ия_ориоо_тр-__,_я,н_лтка__тотк_рр_,р_тнмнь_д_р-_с__ие_ллри_у__ьт_ушт_ж_ч-и_ликбс_губ.иОяц__ззм_,л_мн_ооссе_иевыт_ееодЕ_ссдм, _уи_ьм_еосеп_т__ек_орен_рлу_а_иеомы_,тсза_че_,_еик_ооат__юс

Задание 3. (Вариант 4).

вияпВ_аеьсв_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_аяьзв_ипвтя_иаеая_Ваяув_еяьсе_ьсрт_рртл_рьевв_Вуеьа_есм_р_ршм_к_мя__ч_мт_рт_иеар_иряие_вмта_о__я_еварт_иинр_яоВм_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_траб_вр_ие_тбоеь_з_раВ_ммьь_се_рр_та_вВ_т_еая_Виeья_ясио_яьсир_ьевар_иирьт_мт_рр_ме_ея_ьбеая_мир__рмт__втб_с__шкм_Вееьз_вааяр_гм_др_т_орилр_иявВа_я_ият_омяив_минр_имвр_ввм_урт_Вт_ьйяе_ыгрьн_н_м_ое_еВ_ем__о_я_аеи_рлетю_ед_рч_мьбме_ве_ьюеи_ытьуж_епму_ерааЧ_м,оя_,еитб__м,з_мднпо_тдро_еоо_е_ноттоо_аалат_чдб_т_буш_е_смипт_дтру_н__р_,ывсе_зеье_оа_н_Чтьч_лиоса_ас,п_боатт_о_тто_длт_к_т_рот__у_и_с__Ел_ц_ан__взщг_мтле, _де_о: _дб,ам_ыео_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 ! З 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 л ю 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 З 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 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 ! З 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 Ъ ! 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 Ъ
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 Ъ 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 \$ б Ы Ч в э Х Э 2 е э ц ы ь ы _ ?
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 ~
Ь 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 л и ! 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 Ы 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 д и б а = 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 6

ОПК-4

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) Найдем 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
- 3 Закон "О лицензировании
отдельных видов деятельности"
- 4
- 5 Закон "Об электронной цифровой
подписи"
- 6
- 7 Закон «О государственной тайне»
- 8
- 9 Уголовный кодекс РФ
Гл. 28. «Преступление в сфере
компьютерной информации»
- 10
- 11 Гражданский кодекс РФ
- 12
- 13 Конституция РФ
- 14
- 15 Доктрина информационной
безопасности РФ
- 16
- 17 Стратегия Национальной
безопасности Российской Федерации
- 18
- 19 Постановление правительства РФ
«об утверждении положения об
особенности обработки персональных
данных, осуществляемой без
использования средств автоматизации.
- 20
- 21 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»

5.2.4. Темы курсовых работ, эссе, рефератов

Темы для докладов-презентаций

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)

Темы контрольных работ (для заочной формы обучения)

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

25. Требования по обеспечению информационной безопасности корпоративной информационной системы предприятия
26. Требования к программно-аппаратным средствам
27. Требования к подсистеме идентификации и аутентификации
28. Требования к подсистеме управления доступом
29. Требования к подсистеме протоколирования аудита
30. Требования к подсистеме защиты повторного использования объектов
31. Требования к защите критичной информации
32. Требования к средствам обеспечения целостности:
33. Требования к средствам управления ИБ
34. Требования к Межсетевому Экрану
35. Системы разграничения доступа (полномочий)
36. Электронный замок
37. Идентификация и аутентификация пользователей
38. Регистрация попыток доступа к ПЭВМ
39. Контроль целостности программной среды и запрет загрузки со съемных носителей
40. Построение системы защиты распределенных вычислительных сетей от внутренних и внешних посягательств на информацию и ресурсы различного назначения
41. Управление безопасностью в корпоративных распределенных вычислительных системах и сетях связи
42. Защита документов и товаров с использованием электронной цифровой подписи
43. Перспективы развития аппаратных средств защиты от несанкционированного доступа к информации

6. Учебно-методическое и информационное обеспечение дисциплины

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 (в соответствии с содержанием дисциплины)

1. MS Office;
2. ИПС «Консультант +»;
3. ИПС «Гарант»;
4. Поисковые система «Яндекс», «Google»;
5. ЭБС znanium.com;

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: компьютерная техника с подключением к сети «Интернет», экран, проектор для вывода мультимедиа материалов на экран, динамики для воспроизведения звука, доска.

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

Программа составлена в соответствии с требованиями ОС ВО по направлению подготовки 09.03.03 «Прикладная информатика», профиль «Прикладная информатика в экономике».

Автор (ы)

к.э.н., доцент

П.С. Шалабаев

Рецензент (ы):

к.э.н, ст. специалист отдела

электронных платежей

департамента информатизации

ПАО «НБД – банк»

А.Н. Визгунов

Заведующий кафедрой ИТИМЭ

д.э.н., профессор

Ю.В. Трифионов

Программа одобрена на заседании методической комиссии

Института экономики и предпринимательства

от «15» марта 2021 года, протокол № 3