

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

---

УТВЕРЖДЕНО

решением Ученого совета ННГУ

протокол № 10 от 02.12.2024 г.

**Рабочая программа дисциплины**

Информатика

---

Уровень высшего образования

Специалитет

---

Направление подготовки / специальность

38.05.01 - Экономическая безопасность

---

Направленность образовательной программы

Экономико-правовое обеспечение экономической безопасности

---

Форма обучения

очная, заочная

---

г. Нижний Новгород

2025 год начала подготовки

## 1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.19 Информатика относится к обязательной части образовательной программы.

## 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	Для текущего контроля успеваемости	Для промежуточной аттестации
ОПК-6: Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.	ОПК-6.1: Осуществляет сбор и анализ данных для решения профессиональных задач с использованием информационных технологий и программных средств ОПК-6.2: Обрабатывает и анализирует данные с применением программных средств и с использованием современных информационных технологий при решении профессиональных задач	ОПК-6.1: Знать: порядок хранения, обработки и анализа информации для решения задач профессиональной деятельности. Уметь: применять методы обработки и анализа информации для решения задач профессиональной деятельности. Владеть: средствами поиска, хранения, обработки и анализа информации из различных источников и баз данных их для решения задач профессиональной деятельности.  ОПК-6.2: Знать: достижения современных информационных технологий для решения профессиональных задач. Уметь: применять достижения современных информационных технологий для решения профессиональных задач. Владеть: средствами достижения современных информационных технологий для решения профессиональных задач	Собеседование Практическое задание	Зачёт: Задания Тест
ОПК-7: Способен понимать принципы	ОПК-7.1: Демонстрирует понимание принципов	ОПК-7.1: Знать: порядок хранения,	Собеседование Практическое	Зачёт:

работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	работы современных информационных технологий для решения задач в профессиональной деятельности ОПК-7.2: Применяет принципы работы современных информационных технологий для решения задач в профессиональной деятельности	обработки и анализа информации для решения задач профессиональной деятельности. Уметь: применять методы обработки и анализа информации для решения задач профессиональной деятельности. Владеть: средствами поиска, хранения, обработки и анализа информации из различных источников и баз данных их для решения задач профессиональной деятельности.  ОПК-7.2: Знать: достижения современных информационных технологий для решения профессиональных задач. Уметь: применять достижения современных информационных технологий для решения профессиональных задач. Владеть: средствами достижения современных информационных технологий для решения профессиональных задач	задание	Задания Тест
---	--	--	---------	-----------------

### 3. Структура и содержание дисциплины

#### 3.1 Трудоемкость дисциплины

	очная	заочная
<b>Общая трудоемкость, з.е.</b>	<b>3</b>	<b>3</b>
<b>Часов по учебному плану</b>	<b>108</b>	<b>108</b>
в том числе		
<b>аудиторные занятия (контактная работа):</b>		
- занятия лекционного типа	16	6
- занятия семинарского типа (практические занятия / лабораторные работы)	32	6
- КСР	1	1
<b>самостоятельная работа</b>	<b>59</b>	<b>91</b>
<b>Промежуточная аттестация</b>	<b>0</b> Зачёт	<b>4</b> Зачёт

### 3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)		в том числе								
			Контактная работа (работа во взаимодействии с преподавателем), часы из них						Самостоятельная работа обучающегося, часы		
			Занятия лекционного типа		Занятия семинарского типа (практические занятия/лабораторные работы), часы		Всего				
	О Ф О	З Ф О	О Ф О	З Ф О	О Ф О	З Ф О	О Ф О	З Ф О	О Ф О	З Ф О	
Тема 1. Информатика, ее предмет и задачи. Основные понятия курса	22	10	2		10		12	0	10	10	
Тема 2. Особенности экономической информации	17	10	2		5		7	0	10	10	
Тема 3. Принципы работы компьютерной техники	17	22	2	1	5	1	7	2	10	20	
Тема 4. Программное обеспечение компьютерной техники	11	10	3	1	3	1	6	2	5	8	
Тема 5. Основы работы в среде глобальных компьютерных сетей	8	10	2	1	3	1	5	2	3	8	
Тема 6. Тенденции развития современных информационно-коммуникационных технологий (ИКТ)	14	10	2	1	2	1	4	2	10	8	
Тема 7. Основы информационной безопасности при использовании ИКТ	7	22	1	1	1	1	2	2	5	20	
Тема 8. И.И. Основы шифрования данных и их применение в экономической безопасности.	6	2	2		2		4	0	2	2	
В т.ч. текущий контроль	5	7	0	1	1	1	1	2	4	5	
Аттестация	0	4									
КСР	1	1						1	1		
Итого	108	108	16	6	32	6	49	13	59	91	

#### Содержание разделов и тем дисциплины

Тема 1. Информатика, ее предмет и задачи. Основные понятия курса

Тема 2. Особенности экономической информации

Тема 3. Принципы работы компьютерной техники

Тема 4. Программное обеспечение компьютерной техники

Тема 5. Основы работы в среде глобальных компьютерных сетей

Тема 6. Тенденции развития современных информационно-коммуникационных технологий (ИКТ)

Тема 7. Основы информационной безопасности при использовании ИКТ

#### 4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Для обеспечения самостоятельной работы обучающихся используются:  
Электронные курсы, созданные в системе электронного обучения ННГУ:

Информатика, <https://e-learning.unn.ru/course/view.php?id=4753>.

Открытые онлайн-курсы MOOC:

Информатика, <https://e-learning.unn.ru/course/view.php?id=4753>.

Иные учебно-методические материалы:

курс «Информатика», расположенный <https://e-learning.unn.ru/course/view.php?id=4753> в системе электронного обучения ННГУ - <https://e-learning.unn.ru/>.

## **5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)**

### **5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:**

#### **5.1.1 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ОПК-6:**

1. Информатизация и компьютеризация общества
2. Данные. Методы воспроизведения и обработки данных. Понятие информации
3. Информационные процессы. Особенности информационных процессов в вычислительной технике
4. Понятие информации. Свойства информации
5. Информатика, предмет и задачи
6. Понятие экономической информации, её особенности и виды
7. Структура экономической информации. Её простые структурные единицы
8. Составные структурные единицы экономической информации
9. Понятие экономической информационной системы
10. История развития ЭВМ
11. Классификации ЭВМ
12. Двоичный код. Единицы измерения двоичной информации
13. Кодирование текстовых и числовых данных в ЭВМ

14. Представление мультимедийных данных в ЭВМ
15. Общая структура современного компьютера
16. Процессоры для персональных компьютеров и смартфонов
17. Память компьютера и её виды
18. Устройства ввода-вывода информации в ЭВМ
19. Материнская плата. Системный блок персонального компьютера
20. Состав программного обеспечения компьютера
21. Системное программное обеспечение компьютера
22. Инструментальное и прикладное программное обеспечение компьютера
23. Базы данных. Основные понятия и классификации БД
24. Структурные элементы БД
25. Модели данных для БД
26. Иерархическая модель данных
27. Сетевая модель данных
28. Реляционная модель данных
29. Реляционная база данных
30. Связи и их типы для БД
31. Назначение и классификация компьютерных сетей. Основные понятия компьютерных сетей
32. Локальные компьютерные сети, их топологии
33. Глобальная сеть SWIFT
34. Глобальная сеть Интернет, её история и основные сервисы
35. Основные протоколы Интернета
36. Система доменных имён Интернета
37. Основы Всемирной Паутины: HTTP, HTML, URL
38. Интерактивный Интернет, основные тенденции развития

39. Облачные вычисления
40. Технологии искусственного интеллекта. Искусственные нейронные сети
41. Прогресс информационных технологий и необходимость обеспечения безопасности
42. Структура понятия ЗАЩИТА ИНФОРМАЦИИ (ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ)
43. Объекты информационной безопасности в организации
44. Виды защищаемой информации
45. Информационные угрозы и их классификация
46. Действия и события, нарушающие информационную безопасность
47. Основные виды каналов утечки информации
48. Вредоносные программы, их виды
49. Противодействие вредоносным программам. Антивирусное ПО
50. Защита от компьютерных преступлений (правовая, организационная, техническая)
51. Государственное регулирование информационной безопасности
52. Доктрина информационной безопасности РФ
53. Федеральный закон «Об информации, информационных технологиях и о защите информации»
54. Федеральный закон «Об электронной подписи»
55. Подходы к обеспечению информационной безопасности в организации
56. Принципы построения системы информационной безопасности
57. Методы и средства обеспечения ИБ
58. Сущность криптографических методов. Симметричные шифры
59. Сущность криптографических методов. Несимметричные шифры
60. Электронная цифровая подпись и особенности ее применения
61. Техническое обеспечение электронной подписи
62. Организационное обеспечение электронной подписи
63. Правовое обеспечение электронной подписи

64. Защита информации при работе в Интернете
65. Брандмауэры и прокси-серверы
66. Мероприятия по защите ценной компьютерной информации
67. Политика информационной безопасности в организации. Основные принципы
68. Организация системы защиты информации на предприятии
69. Процесс менеджмента риска ИБ
70. Аудит системы защиты информации в организации

1. «Применение искусственного интеллекта в анализе больших данных для выявления финансовых рисков».
2. «Модели искусственного интеллекта для прогнозирования экономических тенденций и их роль в обеспечении экономической безопасности».
3. «Автоматизация процессов с помощью искусственного интеллекта как метод снижения рисков в финансовых операциях».
4. «Этические и правовые аспекты использования искусственного интеллекта в экономической безопасности».
5. «Интеллектуальные системы обнаружения аномалий и предотвращения финансовых преступлений: технологии и перспективы».

#### **5.1.2 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ОПК-7:**

1. Информатизация и компьютеризация общества
2. Данные. Методы воспроизведения и обработки данных. Понятие информации
3. Информационные процессы. Особенности информационных процессов в вычислительной технике
4. Понятие информации. Свойства информации
5. Информатика, предмет и задачи
6. Понятие экономической информации, её особенности и виды
7. Структура экономической информации. Её простые структурные единицы
8. Составные структурные единицы экономической информации
9. Понятие экономической информационной системы
10. История развития ЭВМ



11. Классификации ЭВМ
12. Двоичный код. Единицы измерения двоичной информации
13. Кодирование текстовых и числовых данных в ЭВМ
14. Представление мультимедийных данных в ЭВМ
15. Общая структура современного компьютера
16. Процессоры для персональных компьютеров и смартфонов
17. Память компьютера и её виды
18. Устройства ввода-вывода информации в ЭВМ
19. Материнская плата. Системный блок персонального компьютера
20. Состав программного обеспечения компьютера
21. Системное программное обеспечение компьютера
22. Инструментальное и прикладное программное обеспечение компьютера
23. Базы данных. Основные понятия и классификации БД
24. Структурные элементы БД
25. Модели данных для БД
26. Иерархическая модель данных
27. Сетевая модель данных
28. Реляционная модель данных
29. Реляционная база данных
30. Связи и их типы для БД
31. Назначение и классификация компьютерных сетей. Основные понятия компьютерных сетей
32. Локальные компьютерные сети, их топологии
33. Глобальная сеть SWIFT
34. Глобальная сеть Интернет, её история и основные сервисы
35. Основные протоколы Интернета

36. Система доменных имён Интернета
37. Основы Всемирной Паутины: HTTP, HTML, URL
38. Интерактивный Интернет, основные тенденции развития
39. Облачные вычисления
40. Технологии искусственного интеллекта. Искусственные нейронные сети
41. Прогресс информационных технологий и необходимость обеспечения безопасности
42. Структура понятия ЗАЩИТА ИНФОРМАЦИИ (ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ)
43. Объекты информационной безопасности в организации
44. Виды защищаемой информации
45. Информационные угрозы и их классификация
46. Действия и события, нарушающие информационную безопасность
47. Основные виды каналов утечки информации
48. Вредоносные программы, их виды
49. Противодействие вредоносным программам. Антивирусное ПО
50. Защита от компьютерных преступлений (правовая, организационная, техническая)
51. Государственное регулирование информационной безопасности
52. Доктрина информационной безопасности РФ
53. Федеральный закон «Об информации, информационных технологиях и о защите информации»
54. Федеральный закон «Об электронной подписи»
55. Подходы к обеспечению информационной безопасности в организации
56. Принципы построения системы информационной безопасности
57. Методы и средства обеспечения ИБ
58. Сущность криптографических методов. Симметричные шифры
59. Сущность криптографических методов. Несимметричные шифры
60. Электронная цифровая подпись и особенности ее применения

61. Техническое обеспечение электронной подписи
62. Организационное обеспечение электронной подписи
63. Правовое обеспечение электронной подписи
64. Защита информации при работе в Интернете
65. Брандмауэры и прокси-серверы
66. Мероприятия по защите ценной компьютерной информации
67. Политика информационной безопасности в организации. Основные принципы
68. Организация системы защиты информации на предприятии
69. Процесс менеджмента риска ИБ
70. Аудит системы защиты информации в организации

1. «Применение искусственного интеллекта в анализе больших данных для выявления финансовых рисков».
2. «Модели искусственного интеллекта для прогнозирования экономических тенденций и их роль в обеспечении экономической безопасности».
3. «Автоматизация процессов с помощью искусственного интеллекта как метод снижения рисков в финансовых операциях».
4. «Этические и правовые аспекты использования искусственного интеллекта в экономической безопасности».
5. «Интеллектуальные системы обнаружения аномалий и предотвращения финансовых преступлений: технологии и перспективы».

#### **Критерии оценивания (оценочное средство - Собеседование)**

Оценка	Критерии оценивания
зачтено	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.
не зачтено	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа

#### **5.1.3 Типовые задания (оценочное средство - Практическое задание) для оценки сформированности компетенции ОПК-6:**

1. Символическое имя хоста называется:

- а) IP адрес,

- б) доменное имя,
- в) URL.

2. База данных, в которой все данные, доступные пользователю, организованы в виде таблиц, а все операции над данными сводятся к операциям над этими таблицами, называется:

- а) табличной,
- б) реляционной,
- в) операционной.

3. MS DOS относится к:

- а) прикладному ПО,
- б) инструментальному ПО,
- в) системному ПО.

4. К рунету относятся домены:

- а) РФ, su, ru,
- б) РФ, ru,
- в) su, edu.

5. Базовыми (элементарными) единицами экономической информации являются:

- а) экономические показатели,
- б) реквизиты-признаки,
- в) информационные сообщения.

6. Драйвер относится к:

- а) прикладному ПО,
- б) инструментальному ПО,
- в) системному ПО.

### **5.2.3. Типовые практические задания для оценки сформированности компетенции ОПК-6**

1. Создать в программе MS EXCEL автоматическую таблицу перевода двоичных чисел в десятичные. Примерный вид таблицы представлен ниже.

Число в двоичной системе счисления:	Здесь в одной или нескольких ячейках записывается двоичное число до 8 бит
Число в десятичной системе счисления:	Здесь выводится результат

2. Дешифровать защищенную информацию с использованием алгоритма блочного шифрования. Дано: шифротекст и ключ. Алфавит и алгоритм использовать стандартный, который использовался на практических занятиях в примерах.

#### Вариант 1

Ключ (2;4)                      Шифротекст: ЪРЦК

#### Вариант 2

Ключ (5;7)                      Шифротекст: ГЮЭЧ

### **1. Темы докладов, способствующих формированию знаний компетенции ОПК-6**

1. Микропроцессоры для персональных компьютеров и смартфонов.
2. Материнская плата персонального компьютера.
3. Накопители информации на жестких магнитных дисках.
4. Оперативная память персонального компьютера.
5. Постоянная память персонального компьютера.
6. Дисковые оптические накопители информации и их приводы.
7. Флэш-память для персональных компьютеров.
8. Обобщенная структура компьютера.
9. Мониторы для персональных компьютеров.
10. Принтеры для персональных компьютеров.
11. Устройства ввода информации в компьютер.
12. Устройства вывода информации из компьютера (кроме монитора и принтера).
13. Стандарты каналов связи Bluetooth и Wi-Fi.
14. Технологии искусственного интеллекта. Искусственные нейронные сети.
15. Технологии Big Data.

16. Вредоносные компьютерные программы.
17. Антивирусное программное обеспечение.
18. Виды компьютерного мошенничества и способы защиты от него.
19. Доктрина информационной безопасности РФ.
20. ФЗ «Об информации, информационных технологиях и защите информации».
21. ФЗ «О государственной тайне».
22. ФЗ «О коммерческой тайне».
23. ФЗ «О персональных данных».
24. Налоговая и банковская тайны (по НК РФ ст.102 и ФЗ о банках и банковской деятельности ст. 26).
25. Служебная информация ограниченного распространения (по Постановлению Правительства РФ от 3.11.1994 №1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»).
26. ФЗ «Об электронной подписи».
27. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

## **1. Кейс-задача для осуществления практической подготовки по компетенции ОПК-6**

1. Выбрать организацию (реальную или нет). Описать ее контекст (в соответствии с ГОСТ 27005), который будет необходим для организации процесса менеджмента рисков ИБ:

- цели и задачи организации;
- условия, в которых она работает;
- ограничения, с которыми она сталкивается (финансовые, правовые и другие – смотри ГОСТ);
- критерии оценки угроз, активов, уязвимостей и рисков ИБ в целом.

2. В соответствии с алгоритмом процесса менеджмента рисков ИБ идентифицировать для этой организации 5 рисков ИБ. Провести их анализ и оценку. В результате получить ранжированный список из 5 рисков.

3. Провести обработку рисков из итого списка, то есть для каждого риска предложить свой наиболее подходящий вариант обработки риска ИБ (название варианта обработки по ГОСТу и конкретное мероприятие).

*Методические указания для выполнения задания:*

А) общий объем текста ответа на задание не более 1 страницы (2400 знаков без пробелов);

Б) Риски, идентифицированные в задании, должны быть разноплановые, то есть активы в них должны быть как аппаратные, так и программные, и информационные; угрозы должны быть как естественные, так и обусловленные человеческим фактором (активные, пассивные, внутренние, внешние и прочие). Все риски должны быть идентифицированы для одной выбранной организации;

В) В контексте организации (в первой части) описывать только то, что будет востребовано и необходимо при выполнении пунктов 2 и 3, то есть при анализе, оценке и обработке 5 названных рисков. Буквально в нескольких словах описываем организацию, чем занимается, в каких условиях работает, какие информационные активы имеет, с какими проблемами с точки зрения ИБ может столкнуться и почему;

Г) Также в первом пункте необходимо пояснить критерии оценки активов, угроз, уязвимостей и рисков в целом, которые будут в дальнейшем применяться. Какой подход вы выбираете: качественный, количественный или комбинированный. Надо охарактеризовать шкалу, которую будете применять для оценки элементов риска. Например, для 5 рисков удобно использовать шкалу от 1 до 5, где 1 – самый низкий уровень опасности (вероятности) элемента риска, а 5 – самый высокий уровень. Вы можете использовать шкалу, которая вам подходит, только надо ее охарактеризовать, чтобы было понятно ее использование в дальнейшем в пункте 2;

Д) Что касается пункта 3, то здесь должны быть задействованы все варианты обработки риска (один вариант обработки для первого риска, другой – для второго, третий – для третьего, четвертый – для четвертого, а для пятого риска – любой вариант обработки или их комбинация). Соответственно, как уже отмечалось, риски должны быть разноплановые и должны предусматривать разные варианты обработки;

Е) Задание индивидуальное, если будут попадаться одинаковые ответы, то оценка будет делиться на количество одинаковых ответов.

1. Задание: создать запрос для нейросети, чтобы получить информацию о том, как работают основные алгоритмы шифрования данных и какие из них наиболее часто используются в сфере экономической безопасности.
2. Задание: разработать запрос для нейросети с целью получения данных о том, как применяются технологии машинного обучения для анализа финансовых транзакций и выявления мошеннических схем.
3. Задание: сформулировать вопрос для нейросети, чтобы узнать о методах защиты информационных систем от внешних угроз и атак, и привести примеры их применения в экономической сфере.

4. Задание: составить запрос для нейросети, чтобы получить данные о том, какие инструменты и программные решения используются для обеспечения кибербезопасности в экономических системах, и описать их основные функции.
5. Задание: разработать серию вопросов для нейросети, чтобы изучить принципы работы систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS) в контексте защиты экономических данных. Вопросы должны охватывать основные функции, механизмы работы и примеры применения этих систем.
6. Задание: сформулировать запрос для нейросети, чтобы получить информацию о том, как технологии блокчейн и распределённые реестры могут быть использованы для обеспечения прозрачности и надёжности финансовых операций, и какие риски связаны с их применением.
7. Задание: создать запрос для нейросети, чтобы узнать о методах аутентификации и авторизации пользователей в информационных системах, применяемых в сфере экономической безопасности, и привести примеры их реализации.
8. Задание: разработать серию вопросов для нейросети, чтобы изучить основы криптографии и её применение для защиты конфиденциальной экономической информации, включая примеры алгоритмов и их характеристики.
9. Задание: сформулировать запрос для нейросети, чтобы получить информацию о том, какие стандарты и протоколы используются для обеспечения безопасности передачи данных в экономических системах, и как они реализуются на практике.
10. Задание: создать запрос для нейросети, чтобы узнать о современных тенденциях и инновационных решениях в области кибербезопасности, которые могут быть применены для защиты экономических интересов организаций.

#### **5.1.4 Типовые задания (оценочное средство - Практическое задание) для оценки сформированности компетенции ОПК-7:**

1. Символическое имя хоста называется:

- а) IP адрес,
- б) доменное имя,
- в) URL.

2. База данных, в которой все данные, доступные пользователю, организованы в виде таблиц, а все операции над данными сводятся к операциям над этими таблицами, называется:

- а) табличной,
- б) реляционной,
- в) операционной.

3. MS DOS относится к:

- а) прикладному ПО,
- б) инструментальному ПО,
- в) системному ПО.

4. К рунету относятся домены:



а) РФ, su, ru.

б) РФ, ru,

в) su, edu.

5. Базовыми (элементарными) единицами экономической информации являются:

а) экономические показатели,

б) реквизиты-признаки,

в) информационные сообщения.

6. Драйвер относится к:

а) прикладному ПО,

б) инструментальному ПО,

в) системному ПО.

### 5.2.3. Типовые практические задания для оценки сформированности компетенции ОПК-6

1. Создать в программе MS EXCEL автоматическую таблицу перевода двоичных чисел в десятичные.  
Примерный вид таблицы представлен ниже.

Число в двоичной системе счисления:	Здесь в одной или нескольких ячейках записывается двоичное число до 8 бит
Число в десятичной системе счисления:	Здесь выводится результат

2. Дешифровать защищенную информацию с использованием алгоритма блочного шифрования. Дано: шифротекст и ключ. Алфавит и алгоритм использовать стандартный, который использовался на практических занятиях в примерах.

#### Вариант 1

Ключ (2;4)

Шифротекст: ЪРЦК

#### Вариант 2

Ключ (5;7)

Шифротекст: ГЮЭЧ

### 1. Темы докладов, способствующих формированию знаний компетенции ОПК-6

1. Микропроцессоры для персональных компьютеров и смартфонов.
2. Материнская плата персонального компьютера.
3. Накопители информации на жестких магнитных дисках.
4. Оперативная память персонального компьютера.
5. Постоянная память персонального компьютера.
6. Дисковые оптические накопители информации и их приводы.
7. Флэш-память для персональных компьютеров.
8. Обобщенная структура компьютера.
9. Мониторы для персональных компьютеров.
10. Принтеры для персональных компьютеров.
11. Устройства ввода информации в компьютер.
12. Устройства вывода информации из компьютера (кроме монитора и принтера).
13. Стандарты каналов связи Bluetooth и Wi-Fi.
14. Технологии искусственного интеллекта. Искусственные нейронные сети.
15. Технологии Big Data.
16. Вредоносные компьютерные программы.
17. Антивирусное программное обеспечение.
18. Виды компьютерного мошенничества и способы защиты от него.
19. Доктрина информационной безопасности РФ.
20. ФЗ «Об информации, информационных технологиях и защите информации».
21. ФЗ «О государственной тайне».
22. ФЗ «О коммерческой тайне».
23. ФЗ «О персональных данных».
24. Налоговая и банковская тайны (по НК РФ ст.102 и ФЗ о банках и банковской деятельности ст. 26).
25. Служебная информация ограниченного распространения (по Постановлению Правительства РФ от 3.11.1994 №1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»).
26. ФЗ «Об электронной подписи».
27. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

## **1. Кейс-задача для осуществления практической подготовки по компетенции ОПК-6**

1. Выбрать организацию (реальную или нет). Описать ее контекст (в соответствии с ГОСТ 27005), который будет необходим для организации процесса менеджмента рисков ИБ:

- цели и задачи организации;
- условия, в которых она работает;
- ограничения, с которыми она сталкивается (финансовые, правовые и другие – смотри ГОСТ);
- критерии оценки угроз, активов, уязвимостей и рисков ИБ в целом.

2. В соответствии с алгоритмом процесса менеджмента рисков ИБ идентифицировать для этой организации 5 рисков ИБ. Провести их анализ и оценку. В результате получить ранжированный список из 5 рисков.

3. Провести обработку рисков из итого списка, то есть для каждого риска предложить свой наиболее подходящий вариант обработки риска ИБ (название варианта обработки по ГОСТу и конкретное мероприятие).

*Методические указания для выполнения задания:*

А) общий объем текста ответа на задание не более 1 страницы (2400 знаков без пробелов);

Б) Риски, идентифицированные в задании, должны быть разноплановые, то есть активы в них должны быть как аппаратные, так и программные, и информационные; угрозы должны быть как естественные, так и обусловленные человеческим фактором (активные, пассивные, внутренние, внешние и прочие). Все риски должны быть идентифицированы для одной выбранной организации;

В) В контексте организации (в первой части) описывать только то, что будет востребовано и необходимо при выполнении пунктов 2 и 3, то есть при анализе, оценке и обработке 5 названных рисков. Буквально в нескольких словах описываем организацию, чем занимается, в каких условиях работает, какие информационные активы имеет, с какими проблемами с точки зрения ИБ может столкнуться и почему;

Г) Также в первом пункте необходимо пояснить критерии оценки активов, угроз, уязвимостей и рисков в целом, которые будут в дальнейшем применяться. Какой подход вы выбираете: качественный, количественный или комбинированный. Надо охарактеризовать шкалу, которую будете применять для оценки элементов риска. Например, для 5 рисков удобно использовать шкалу от 1 до 5, где 1 – самый низкий уровень опасности (вероятности) элемента риска, а 5 – самый высокий уровень. Вы можете использовать шкалу, которая вам подходит, только надо ее охарактеризовать, чтобы было понятно ее использование в дальнейшем в пункте 2;

Д) Что касается пункта 3, то здесь должны быть задействованы все варианты обработки риска (один вариант обработки для первого риска, другой – для второго, третий – для третьего, четвертый – для четвертого, а для пятого риска – любой вариант обработки или их комбинация). Соответственно, как уже отмечалось, риски должны быть разноплановые и должны предусматривать разные варианты обработки;

Е) Задание индивидуальное, если будут попадаться одинаковые ответы, то оценка будет делиться на количество одинаковых ответов.

1. Задание: создать запрос для нейросети, чтобы получить информацию о том, как работают основные алгоритмы шифрования данных и какие из них наиболее часто используются в сфере экономической безопасности.
2. Задание: разработать запрос для нейросети с целью получения данных о том, как применяются технологии машинного обучения для анализа финансовых транзакций и выявления мошеннических схем.
3. Задание: сформулировать вопрос для нейросети, чтобы узнать о методах защиты информационных систем от внешних угроз и атак, и привести примеры их применения в экономической сфере.
4. Задание: составить запрос для нейросети, чтобы получить данные о том, какие инструменты и программные решения используются для обеспечения кибербезопасности в экономических системах, и описать их основные функции.
5. Задание: разработать серию вопросов для нейросети, чтобы изучить принципы работы систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS) в контексте защиты экономических данных. Вопросы должны охватывать основные функции, механизмы работы и примеры применения этих систем.
6. Задание: сформулировать запрос для нейросети, чтобы получить информацию о том, как технологии блокчейн и распределённые реестры могут быть использованы для обеспечения прозрачности и надёжности финансовых операций, и какие риски связаны с их применением.
7. Задание: создать запрос для нейросети, чтобы узнать о методах аутентификации и авторизации пользователей в информационных системах, применяемых в сфере экономической безопасности, и привести примеры их реализации.
8. Задание: разработать серию вопросов для нейросети, чтобы изучить основы криптографии и её применение для защиты конфиденциальной экономической информации, включая примеры алгоритмов и их характеристики.

9. Задание: сформулировать запрос для нейросети, чтобы получить информацию о том, какие стандарты и протоколы используются для обеспечения безопасности передачи данных в экономических системах, и как они реализуются на практике.
10. Задание: создать запрос для нейросети, чтобы узнать о современных тенденциях и инновационных решениях в области кибербезопасности, которые могут быть применены для защиты экономических интересов организаций.

### Критерии оценивания (оценочное средство - Практическое задание)

Оценка	Критерии оценивания
превосходно	Уровень знаний в объеме, превышающем программу подготовки.
отлично	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
очень хорошо	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок
хорошо	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок
удовлетворительно	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.
неудовлетворительно	Уровень знаний ниже минимальных требований. Имели место грубые ошибки
плохо	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа

### 5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

#### Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено			зачтено			
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность	Уровень знаний ниже минимальных требований. Имели место	Минимально допустимый уровень знаний.	Уровень знаний в объеме, соответствующем	Уровень знаний в объеме, соответствующем	Уровень знаний в объеме, соответствующем	Уровень знаний в объеме, превышающем программу

	оценить полноту знаний вследствие отказа обучающегося от ответа	грубые ошибки	Допущено много негрубых ошибок	программе подготовки . Допущено несколько негрубых ошибок	программе подготовки . Допущено несколько несущественных ошибок	программе подготовки и. Ошибок нет.	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	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами .	Продемонстрированы все основные умения. Решены все основные задачи с отдельными и несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторым и недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторым и недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрирован творческий подход к решению нестандартных задач

### Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	<b>превосходно</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой
	<b>отлично</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	<b>очень хорошо</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	<b>хорошо</b>	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
	<b>удовлетворительно</b>	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	<b>неудовлетворительно</b>	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».

	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»
--	-------	---

### 5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

#### 5.3.1 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-6

1. Создать в программе MS EXCEL автоматическую таблицу перевода двоичных чисел в десятичные.
2. Дешифровать защищенную информацию с использованием алгоритма блочного шифрования. Дано: шифротекст и ключ. Алфавит и алгоритм использовать стандартный, который использовался на практических занятиях в примерах.
3. Составьте промт для разработки алгоритма ИИ для выявления финансовых рисков в больших данных. Укажите типы данных для анализа, методы и модели ИИ, а также метрики оценки эффективности.
4. Разработайте промт для исследования этических и правовых рисков ИИ в экономической безопасности. Укажите законодательные акты, этические принципы и меры по минимизации негативных последствий.

#### 5.3.2 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-7

1. Создать в программе MS EXCEL автоматическую таблицу перевода двоичных чисел в десятичные.
2. Дешифровать защищенную информацию с использованием алгоритма блочного шифрования. Дано: шифротекст и ключ. Алфавит и алгоритм использовать стандартный, который использовался на практических занятиях в примерах.
3. Составьте промт для разработки алгоритма ИИ для выявления финансовых рисков в больших данных. Укажите типы данных для анализа, методы и модели ИИ, а также метрики оценки эффективности.
4. Разработайте промт для исследования этических и правовых рисков ИИ в экономической безопасности. Укажите законодательные акты, этические принципы и меры по минимизации негативных последствий.

#### Критерии оценивания (оценочное средство - Задания)

Оценка	Критерии оценивания
зачтено	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
не зачтено	Уровень знаний ниже минимальных требований. Имели место грубые ошибки

#### 5.3.3 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-6

Прочитайте текст и выберите один/несколько правильный ответ

№	Вопрос
---	--------

1	<p><b>Что такое алгоритм?</b></p> <p>а) Последовательность математических операций.  б) Набор инструкций для выполнения определённой задачи.  в) Способ представления информации в виде кода.  г) Метод шифрования данных.</p>
2	<p><b>Какая система счисления используется в компьютерах для представления информации?</b></p> <p>а) Десятичная.  б) Двоичная.  в) Шестнадцатеричная.  г) Восьмеричная.</p>
3	<p><b>Что такое информационная система?</b></p> <p>а) Комплекс аппаратных средств для обработки информации.  б) Совокупность данных и методов их обработки.  в) Система, обеспечивающая сбор, хранение, обработку и передачу информации.  г) Программное обеспечение для работы с документами.</p>
4	<p><b>Какие основные типы данных используются в программировании?</b></p> <p>а) Целые и вещественные числа.  б) Строки и массивы.  в) Логические значения и указатели.  г) Все перечисленные варианты.</p>
5	<p><b>Что такое база данных?</b></p> <p>а) Файл с данными, хранящимися в виде таблиц.  б) Система управления данными, обеспечивающая их хранение и обработку.  в) Программа для работы с электронными таблицами.  г) Способ представления данных в виде графиков и диаграмм.</p>
6	<p><b>Какие существуют основные модели баз данных?</b></p> <p>а) Иерархическая, сетевая, реляционная.  б) Объектно-ориентированная, документальная, распределённая.  в) Централизованная, децентрализованная, гибридная.  г) Все перечисленные варианты.</p>
7	<p><b>Что такое компьютерная сеть?</b></p> <p>а) Группа компьютеров, соединённых для обмена информацией.  б) Система серверов для хранения данных.  в) Комплекс аппаратных и программных средств для работы в интернете.  г) Программа для удалённого доступа к компьютерам.</p>

8	<p><b>Какие основные типы компьютерных сетей существуют?</b></p> <p>а) Локальные, глобальные, региональные.  б) Корпоративные, частные, публичные.  в) Одноранговые, клиент-серверные.  г) Все перечисленные варианты.</p>
9	<p><b>Что такое защита информации?</b></p> <p>а) Процесс шифрования данных для обеспечения их конфиденциальности.  б) Комплекс мероприятий по обеспечению безопасности информации от несанкционированного доступа, изменения или уничтожения.  в) Система антивирусного программного обеспечения.  г) Метод контроля доступа к файлам и папкам.</p>
10	<p><b>Какие основные угрозы информационной безопасности существуют?</b></p> <p>а) Вирусы и трояны.  б) Хакерские атаки и несанкционированный доступ.  в) Сбои оборудования и ошибки программного обеспечения.  г) Все перечисленные варианты.</p>
11	<p><b>Что такое криптография?</b></p> <p>а) Наука о шифровании информации.  б) Метод сжатия данных.  в) Технология передачи данных по сети.  г) Система управления ключами.</p>
12	<p><b>Какие основные методы шифрования используются в криптографии?</b></p> <p>а) Симметричные и асимметричные.  б) Хеширование и цифровая подпись.  в) Шифрование с использованием паролей.  г) Все перечисленные варианты.</p>
13	<p><b>Что такое электронная подпись?</b></p> <p>а) Цифровой аналог рукописной подписи.  б) Шифрованный текст, используемый для аутентификации.  в) Код, подтверждающий авторство документа.  г) Всё перечисленное.</p>
14	<p><b>Какие основные функции выполняет операционная система?</b></p> <p>а) Управление ресурсами компьютера.  б) Обеспечение взаимодействия с устройствами.  в) Запуск и выполнение программ.  г) Все перечисленные варианты.</p>
15	<p><b>Что такое межсетевой экран (firewall)?</b></p> <p>а) Программа для защиты от вирусов.  б) Устройство или программа для контроля трафика между сетями.</p>



	<p>в) Система резервного копирования данных.</p> <p>г) Метод шифрования сетевого трафика.</p>
--	---

#### Ключи

№	Верный ответ	Критерии
1	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
2	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
3	Правильный ответ: в.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
4	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
5	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
6	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
7	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
8	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
9	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
10	Правильный ответ: г.	1 балл –полное правильное соответствие

		0 баллов – остальные случаи
11	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
12	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
13	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
14	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
15	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи

Второй Вариант

№	Вопрос
1	<p><b>1. Что такое программное обеспечение?</b></p> <p>а) Физические компоненты компьютера.  б) Инструкции и данные, которые используются для управления компьютером и выполнения задач.  в) Система кабелей и разъёмов в компьютере.  г) Аппаратные средства для обработки информации.</p>
2	<p><b>2. Какие существуют типы программного обеспечения?</b></p> <p>а) Системное и прикладное.  б) Операционные системы и игры.  в) Только антивирусные программы.  г) Только офисные приложения.</p>
3	<p><b>3. Что такое операционная система?</b></p> <p>а) Программа для работы с текстом.  б) Комплекс программ, управляющих работой компьютера и обеспечивающих взаимодействие между аппаратными средствами и пользователем.  в) Программа для создания презентаций.  г) Система управления базами данных.</p>
4	<p><b>4. Какие функции выполняет операционная система?</b></p> <p>а) Только управление файлами и папками.</p>

	б) Только запуск приложений. в) Управление ресурсами компьютера, обеспечение взаимодействия с устройствами, запуск и выполнение программ. г) Только обеспечение работы сетевых протоколов.
5	<b>5. Что такое файл?</b> а) Единица хранения информации на компьютере. б) Физическое устройство для хранения данных. в) Сетевой протокол для передачи данных. г) Метод шифрования информации.
6	<b>6. Какие типы файлов существуют?</b> а) Только текстовые файлы. б) Только исполняемые файлы. в) Только файлы с изображениями. г) Текстовые файлы, исполняемые файлы, файлы с изображениями, архивные файлы и другие.
7	<b>7. Что такое сеть Интернет?</b> а) Локальная сеть в пределах одного здания. б) Глобальная сеть, объединяющая компьютеры по всему миру. в) Система управления базами данных в сети. г) Комплекс аппаратных средств для работы в сети.
8	<b>8. Какие существуют протоколы передачи данных в сети Интернет?</b> а) Только HTTP. б) Только FTP. в) HTTP, FTP, SMTP, TCP/IP и другие. г) Только SMTP.
9	<b>9. Что такое URL?</b> а) Адрес веб-сайта в сети Интернет. б) Название файла на компьютере. в) Шифрованный ключ для доступа к данным. г) Протокол передачи данных.
10	<b>1. Какие существуют виды поиска информации в сети Интернет?</b> а) Только поиск по ключевым словам. б) Только поиск по заголовкам. в) Поиск по ключевым словам, поиск по заголовкам, поиск по содержимому и другие. г) Только поиск по ссылкам.
11	<b>11. Что такое кибербезопасность?</b> а) Защита компьютерных систем от несанкционированного доступа. б) Защита от вирусов и вредоносного ПО. в) Обеспечение безопасности информации в компьютерных системах.

	г) Всё перечисленное.
12	<p>1. <b>Какие угрозы кибербезопасности существуют?</b></p> <p>а) Только вирусы и трояны.</p> <p>б) Только хакерские атаки.</p> <p>в) Вирусы и трояны, хакерские атаки, фишинг, DDoS-атаки и другие.</p> <p>г) Только фишинг.</p>
13	<p>13. <b>Что такое антивирусная программа?</b></p> <p>а) Программа для шифрования данных.</p> <p>б) Программа для обнаружения и удаления вирусов и другого вредоносного ПО.</p> <p>в) Программа для сжатия файлов.</p> <p>г) Программа для резервного копирования данных.</p>
14	<p>14. <b>Какие существуют методы защиты от вирусов и вредоносного ПО?</b></p> <p>а) Только антивирусные программы.</p> <p>б) Только файрволлы.</p> <p>в) Антивирусные программы, файрволлы, обновление программного обеспечения, резервное копирование данных и другие.</p> <p>г) Только обновление программного обеспечения.</p>
15	<p>15.</p> <p><b>Что такое резервное копирование данных?</b></p> <p>а) Создание копий файлов для их последующего восстановления в случае потери или повреждения.</p> <p>б) Шифрование данных для их защиты.</p> <p>в) Передача данных по сети.</p> <p>г) Удаление ненужных файлов.</p>

#### Ключи

№	Верный ответ	Критерии
1	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
2	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
3	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие

		0 баллов – остальные случаи
4	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
5	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
6	<b>Правильный ответ: г.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
7	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
8	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
9	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
10	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
11	<b>Правильный ответ: г.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
12	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
13	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
14	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
15	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие

		0 баллов – остальные случаи
--	--	-----------------------------

Прочитайте текст и дайте ответ, соответствующий смысловому содержанию вопроса

№	Вопрос
1	Какие основные компоненты включает в себя структура сети для обеспечения информационной безопасности в экономических системах?
2	Какие принципы лежат в основе защиты персональных данных в экономических системах?
3	Каковы основные цели применения криптографических методов в экономической сфере?
4	Какие факторы следует учитывать при выборе системы защиты от DDoS-атак для экономических систем?
5	Какие преимущества предоставляет использование систем мониторинга и анализа логов для обеспечения информационной безопасности экономических систем?

#### Ключи

В качестве верных ответов приведены эталонные/идеальные варианты. Верный ответ – соответствие смысловому содержанию.

№	Верный ответ	Критерии
1	структура сети для обеспечения информационной безопасности в экономических системах включает в себя маршрутизаторы, коммутаторы, межсетевые экраны (firewalls), системы обнаружения и предотвращения вторжений (IDS/IPS), системы управления доступом (IAM) и другие элементы сетевой инфраструктуры.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
2	в основе защиты персональных данных в экономических системах лежат принципы	1 балл –полное или частичное (не менее 50%) смысловое соответствие

	конфиденциальности, целостности и доступности данных. Это включает в себя шифрование данных, ограничение доступа, регулярный аудит и мониторинг, а также наличие планов восстановления после сбоев.	0 баллов – остальные случаи
3	основные цели применения криптографических методов в экономической сфере включают обеспечение конфиденциальности финансовых транзакций, аутентификацию участников сделок, защиту от подделок документов и обеспечение целостности данных.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
4	При выборе системы защиты от DDoS-атак для экономических систем следует учитывать типы атак, которые могут быть направлены на систему, требуемую пропускную способность и ресурсы, бюджет, уровень масштабируемости системы защиты, а также интеграцию с существующей инфраструктурой	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
5	Использование систем мониторинга и анализа логов позволяет своевременно выявлять подозрительную активность, обнаруживать попытки несанкционированного доступа, анализировать тренды и паттерны поведения пользователей, а также оптимизировать процессы реагирования на инциденты.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи

#### Второй вариант

№	Вопрос
1	Какие компоненты включает в себя структура сети для обеспечения информационной безопасности в экономических системах и какие функции они выполняют?
2	Какие основные принципы защиты персональных данных применяются в

	экономических системах и почему они важны?
3	Какие цели преследует применение криптографических методов в экономической сфере и какие задачи они помогают решать?
4	Какие критерии следует учитывать при выборе системы защиты от DDoS-атак для экономических систем и почему это важно?
5	Какие преимущества предоставляет использование систем мониторинга и анализа логов для обеспечения информационной безопасности экономических систем и как это влияет на эффективность управления рисками?

№	Верный ответ	Критерии
1	Маршрутизаторы обеспечивают передачу данных между сетями, коммутаторы — между устройствами в одной сети, межсетевые экраны (firewalls) — фильтрацию трафика, системы обнаружения и предотвращения вторжений (IDS/IPS) — мониторинг и предотвращение атак, системы управления доступом (IAM) — контроль доступа пользователей к ресурсам.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
2	Основные принципы — конфиденциальность, целостность и доступность данных. Они важны для предотвращения утечек информации, обеспечения точности данных и гарантии того, что данные доступны для авторизованных пользователей в нужное время.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
3	Применение криптографических методов обеспечивает Конфиденциальность финансовых транзакций, аутентификацию участников сделок, защиту от подделок документов и целостность данных. Это	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи



	помогает предотвратить мошенничество, обеспечить надёжность сделок и защитить права участников экономических отношений.	
4	При выборе системы защиты от DDoS-атак следует учитывать типы атак, требуемую пропускную способность, бюджет, уровень масштабируемости и интеграцию с инфраструктурой. Это важно для обеспечения стабильной работы экономических систем и защиты от потенциальных финансовых потерь из-за атак.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
5	Использование систем мониторинга и анализа логов позволяет своевременно выявлять подозрительную активность, обнаруживать попытки несанкционированного доступа, анализировать тренды поведения пользователей и оптимизировать реагирование на инциденты. Это повышает эффективность управления рисками за счёт более быстрого выявления и устранения угроз.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи

### 5.3.4 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-7

Прочитайте текст и выберите один/несколько правильный ответ

№	Вопрос
1	<b>Что такое алгоритм?</b> а) Последовательность математических операций. б) Набор инструкций для выполнения определённой задачи. в) Способ представления информации в виде кода. г) Метод шифрования данных.
2	<b>Какая система счисления используется в компьютерах для представления информации?</b> а) Десятичная. б) Двоичная. в) Шестнадцатеричная. г) Восьмеричная.

3	<p><b>Что такое информационная система?</b></p> <p>а) Комплекс аппаратных средств для обработки информации.  б) Совокупность данных и методов их обработки.  в) Система, обеспечивающая сбор, хранение, обработку и передачу информации.  г) Программное обеспечение для работы с документами.</p>
4	<p><b>Какие основные типы данных используются в программировании?</b></p> <p>а) Целые и вещественные числа.  б) Строки и массивы.  в) Логические значения и указатели.  г) Все перечисленные варианты.</p>
5	<p><b>Что такое база данных?</b></p> <p>а) Файл с данными, хранящимися в виде таблиц.  б) Система управления данными, обеспечивающая их хранение и обработку.  в) Программа для работы с электронными таблицами.  г) Способ представления данных в виде графиков и диаграмм.</p>
6	<p><b>Какие существуют основные модели баз данных?</b></p> <p>а) Иерархическая, сетевая, реляционная.  б) Объектно-ориентированная, документальная, распределённая.  в) Централизованная, децентрализованная, гибридная.  г) Все перечисленные варианты.</p>
7	<p><b>Что такое компьютерная сеть?</b></p> <p>а) Группа компьютеров, соединённых для обмена информацией.  б) Система серверов для хранения данных.  в) Комплекс аппаратных и программных средств для работы в интернете.  г) Программа для удалённого доступа к компьютерам.</p>
8	<p><b>Какие основные типы компьютерных сетей существуют?</b></p> <p>а) Локальные, глобальные, региональные.  б) Корпоративные, частные, публичные.  в) Одноранговые, клиент-серверные.  г) Все перечисленные варианты.</p>
9	<p><b>Что такое защита информации?</b></p> <p>а) Процесс шифрования данных для обеспечения их конфиденциальности.  б) Комплекс мероприятий по обеспечению безопасности информации от несанкционированного доступа, изменения или уничтожения.  в) Система антивирусного программного обеспечения.  г) Метод контроля доступа к файлам и папкам.</p>
10	<p><b>Какие основные угрозы информационной безопасности существуют?</b></p> <p>а) Вирусы и трояны.</p>

	б) Хакерские атаки и несанкционированный доступ. в) Сбои оборудования и ошибки программного обеспечения. г) Все перечисленные варианты.
11	<b>Что такое криптография?</b> а) Наука о шифровании информации. б) Метод сжатия данных. в) Технология передачи данных по сети. г) Система управления ключами.
12	<b>Какие основные методы шифрования используются в криптографии?</b> а) Симметричные и асимметричные. б) Хеширование и цифровая подпись. в) Шифрование с использованием паролей. г) Все перечисленные варианты.
13	<b>Что такое электронная подпись?</b> а) Цифровой аналог рукописной подписи. б) Шифрованный текст, используемый для аутентификации. в) Код, подтверждающий авторство документа. г) Всё перечисленное.
14	<b>Какие основные функции выполняет операционная система?</b> а) Управление ресурсами компьютера. б) Обеспечение взаимодействия с устройствами. в) Запуск и выполнение программ. г) Все перечисленные варианты.
15	<b>Что такое межсетевой экран (firewall)?</b> а) Программа для защиты от вирусов. б) Устройство или программа для контроля трафика между сетями. в) Система резервного копирования данных. г) Метод шифрования сетевого трафика.

#### Ключи

№	Верный ответ	Критерии
1	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
2	Правильный ответ: б.	1 балл –полное правильное соответствие

		0 баллов – остальные случаи
3	Правильный ответ: в.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
4	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
5	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
6	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
7	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
8	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
9	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
10	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
11	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
12	Правильный ответ: а.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
13	Правильный ответ: г.	1 балл –полное правильное соответствие 0 баллов – остальные случаи
14	Правильный ответ: г.	1 балл –полное правильное соответствие

		0 баллов – остальные случаи
15	Правильный ответ: б.	1 балл –полное правильное соответствие 0 баллов – остальные случаи

Второй Вариант

№	Вопрос
1	<p><b>1. Что такое программное обеспечение?</b></p> <p>а) Физические компоненты компьютера.  б) Инструкции и данные, которые используются для управления компьютером и выполнения задач.  в) Система кабелей и разъёмов в компьютере.  г) Аппаратные средства для обработки информации.</p>
2	<p><b>2. Какие существуют типы программного обеспечения?</b></p> <p>а) Системное и прикладное.  б) Операционные системы и игры.  в) Только антивирусные программы.  г) Только офисные приложения.</p>
3	<p><b>3. Что такое операционная система?</b></p> <p>а) Программа для работы с текстом.  б) Комплекс программ, управляющих работой компьютера и обеспечивающих взаимодействие между аппаратными средствами и пользователем.  в) Программа для создания презентаций.  г) Система управления базами данных.</p>
4	<p><b>4. Какие функции выполняет операционная система?</b></p> <p>а) Только управление файлами и папками.  б) Только запуск приложений.  в) Управление ресурсами компьютера, обеспечение взаимодействия с устройствами, запуск и выполнение программ.  г) Только обеспечение работы сетевых протоколов.</p>
5	<p><b>5. Что такое файл?</b></p> <p>а) Единица хранения информации на компьютере.  б) Физическое устройство для хранения данных.  в) Сетевой протокол для передачи данных.  г) Метод шифрования информации.</p>

6	<p><b>6. Какие типы файлов существуют?</b></p> <p>а) Только текстовые файлы.  б) Только исполняемые файлы.  в) Только файлы с изображениями.  г) Текстовые файлы, исполняемые файлы, файлы с изображениями, архивные файлы и другие.</p>
7	<p><b>7. Что такое сеть Интернет?</b></p> <p>а) Локальная сеть в пределах одного здания.  б) Глобальная сеть, объединяющая компьютеры по всему миру.  в) Система управления базами данных в сети.  г) Комплекс аппаратных средств для работы в сети.</p>
8	<p><b>8. Какие существуют протоколы передачи данных в сети Интернет?</b></p> <p>а) Только HTTP.  б) Только FTP.  в) HTTP, FTP, SMTP, TCP/IP и другие.  г) Только SMTP.</p>
9	<p><b>9. Что такое URL?</b></p> <p>а) Адрес веб-сайта в сети Интернет.  б) Название файла на компьютере.  в) Шифрованный ключ для доступа к данным.  г) Протокол передачи данных.</p>
10	<p><b>1. Какие существуют виды поиска информации в сети Интернет?</b></p> <p>а) Только поиск по ключевым словам.  б) Только поиск по заголовкам.  в) Поиск по ключевым словам, поиск по заголовкам, поиск по содержимому и другие.  г) Только поиск по ссылкам.</p>
11	<p><b>11. Что такое кибербезопасность?</b></p> <p>а) Защита компьютерных систем от несанкционированного доступа.  б) Защита от вирусов и вредоносного ПО.  в) Обеспечение безопасности информации в компьютерных системах.  г) Всё перечисленное.</p>
12	<p><b>1. Какие угрозы кибербезопасности существуют?</b></p> <p>а) Только вирусы и трояны.  б) Только хакерские атаки.  в) Вирусы и трояны, хакерские атаки, фишинг, DDoS-атаки и другие.  г) Только фишинг.</p>
13	<p><b>13. Что такое антивирусная программа?</b></p> <p>а) Программа для шифрования данных.  б) Программа для обнаружения и удаления вирусов и другого вредоносного ПО.  в) Программа для сжатия файлов.</p>

	г) Программа для резервного копирования данных.
14	<p><b>14.Какие существуют методы защиты от вирусов и вредоносного ПО?</b></p> <p>а) Только антивирусные программы.</p> <p>б) Только фаерволлы.</p> <p>в) Антивирусные программы, фаерволлы, обновление программного обеспечения, резервное копирование данных и другие.</p> <p>г) Только обновление программного обеспечения.</p>
15	<p><b>15.</b></p> <p><b>Что такое резервное копирование данных?</b></p> <p>а) Создание копий файлов для их последующего восстановления в случае потери или повреждения.</p> <p>б) Шифрование данных для их защиты.</p> <p>в) Передача данных по сети.</p> <p>г) Удаление ненужных файлов.</p>

#### Ключи

№	Верный ответ	Критерии
1	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
2	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
3	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
4	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
5	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
6	<b>Правильный ответ: г.</b>	1 балл –полное правильное соответствие

		0 баллов – остальные случаи
7	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
8	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
9	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
10	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
11	<b>Правильный ответ: г.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
12	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
13	<b>Правильный ответ: б.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
14	<b>Правильный ответ: в.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи
15	<b>Правильный ответ: а.</b>	1 балл –полное правильное соответствие 0 баллов – остальные случаи

Прочитайте текст и дайте ответ, соответствующий смысловому содержанию вопроса

№	Вопрос
1	Какие основные компоненты включает в себя структура сети для обеспечения информационной безопасности в экономических системах?
2	Какие принципы лежат в основе защиты персональных данных в



	экономических системах?
3	Каковы основные цели применения криптографических методов в экономической сфере?
4	Какие факторы следует учитывать при выборе системы защиты от DDoS-атак для экономических систем?
5	Какие преимущества предоставляет использование систем мониторинга и анализа логов для обеспечения информационной безопасности экономических систем?

#### Ключи

В качестве верных ответов приведены эталонные/идеальные варианты. Верный ответ – соответствие смысловому содержанию.

№	Верный ответ	Критерии
1	структура сети для обеспечения информационной безопасности в экономических системах включает в себя маршрутизаторы, коммутаторы, межсетевые экраны (firewalls), системы обнаружения и предотвращения вторжений (IDS/IPS), системы управления доступом (IAM) и другие элементы сетевой инфраструктуры.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
2	в основе защиты персональных данных в экономических системах лежат принципы конфиденциальности, целостности и доступности данных. Это включает в себя шифрование данных, ограничение доступа, регулярный аудит и мониторинг, а также наличие планов восстановления после сбоев.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
3	основные цели применения криптографических методов в экономической сфере включают	1 балл –полное или частичное (не менее 50%) смысловое соответствие

	обеспечение конфиденциальности финансовых транзакций, аутентификацию участников сделок, защиту от подделок документов и обеспечение целостности данных.	0 баллов – остальные случаи
4	При выборе системы защиты от DDoS-атак для экономических систем следует учитывать типы атак, которые могут быть направлены на систему, требуемую пропускную способность и ресурсы, бюджет, уровень масштабируемости системы защиты, а также интеграцию с существующей инфраструктурой	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
5	Использование систем мониторинга и анализа логов позволяет своевременно выявлять подозрительную активность, обнаруживать попытки несанкционированного доступа, анализировать тренды и паттерны поведения пользователей, а также оптимизировать процессы реагирования на инциденты.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи

#### Второй вариант

№	Вопрос
1	Какие компоненты включает в себя структура сети для обеспечения информационной безопасности в экономических системах и какие функции они выполняют?
2	Какие основные принципы защиты персональных данных применяются в экономических системах и почему они важны?
3	Какие цели преследует применение криптографических методов в экономической сфере и какие задачи они помогают решать?
4	Какие критерии следует учитывать при выборе системы защиты от DDoS-атак для экономических систем и почему это важно?
5	Какие преимущества предоставляет использование систем мониторинга и анализа логов для обеспечения информационной безопасности экономических систем и как это влияет на эффективность управления

	рисками?
--	----------

№	Верный ответ	Критерии
1	Маршрутизаторы обеспечивают передачу данных между сетями, коммутаторы — между устройствами в одной сети, межсетевые экраны (firewalls) — фильтрацию трафика, системы обнаружения и предотвращения вторжений (IDS/IPS) — мониторинг и предотвращение атак, системы управления доступом (IAM) — контроль доступа пользователей к ресурсам.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
2	Основные принципы — конфиденциальность, целостность и доступность данных. Они важны для предотвращения утечек информации, обеспечения точности данных и гарантии того, что данные доступны для авторизованных пользователей в нужное время.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
3	Применение криптографических методов обеспечивает Конфиденциальность финансовых транзакций, аутентификацию участников сделок, защиту от подделок документов и целостность данных. Это помогает предотвратить мошенничество, обеспечить надёжность сделок и защитить права участников экономических отношений.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи
4	При выборе системы защиты от DDoS-атак следует учитывать типы атак, требуемую пропускную способность, бюджет, уровень масштабируемости и интеграцию с инфраструктурой. Это важно для обеспечения стабильной работы	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи

	экономических систем и защиты от потенциальных финансовых потерь из-за атак.	
5	Использование систем мониторинга и анализа логов позволяет своевременно выявлять подозрительную активность, обнаруживать попытки несанкционированного доступа, анализировать тренды поведения пользователей и оптимизировать реагирование на инциденты. Это повышает эффективность управления рисками за счёт более быстрого выявления и устранения угроз.	1 балл –полное или частичное (не менее 50%) смысловое соответствие 0 баллов – остальные случаи

#### Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
зачтено	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
не зачтено	Уровень знаний ниже минимальных требований. Имели место грубые ошибки

#### 6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Информатика для экономистов : Учебник для СПО / под ред. Полякова В.П. - Москва : Юрайт, 2020. - 524 с. - (Профессиональное образование). - ISBN 978-5-534-11165-1 : 959.00. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=589694&idb=0>.

Дополнительная литература:

1. Федотова Елена Леонидовна. Информатика : Курс лекций. Учебное пособие; Учебное пособие / Московский институт электронной техники. - Москва : Издательский Дом "ФОРУМ", 2018. - 480 с. - ВО - Бакалавриат. - ISBN 978-5-8199-0448-0. - ISBN 978-5-16-500255-7. - ISBN 978-5-16-004571-9., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=742105&idb=0>.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

Электронный управляемый курс ИНФОРМАТИКА <https://e-learning.unn.ru/course/view.php?id=4753>

2. Текстовый процессор MS WORD online <https://office.live.com/start/Word.aspx>

3. Табличный процессор MS EXCEL online <https://office.live.com/start/Excel.aspx>

4. Платформы Deductor Academic 5.3, Loginom на сайте компании Loginom Co (бывшая BaseGroup Labs) <https://basegroup.ru/deductor/download>
5. Официальный сайт компании «Intel» - [www.intel.ru](http://www.intel.ru)
6. Официальный сайт компании «Microsoft» - [www.microsoft.com](http://www.microsoft.com)
7. Электронный управляемый курс ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ <https://e-learning.unn.ru/course/view.php?id=4760>
8. [www.itsec.ru](http://www.itsec.ru) Интернет-журнал «Информационная безопасность».
9. Официальный сайт компании INFOTECs <https://infotecs.ru/>
- 10 Официальный сайт Яндекс GPT <https://ya.ru/ai/gpt>

#### **7. Материально-техническое обеспечение дисциплины (модуля)**

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

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 ННГУ по направлению подготовки/специальности 38.05.01 - Экономическая безопасность.

Автор(ы): Поляков Александр Сергеевич

Сочков Андрей Львович, кандидат технических наук, доцент.

Рецензент(ы): Трифонов Юрий Васильевич, доктор экономических наук.

Заведующий кафедрой: Трифонов Юрий Васильевич, доктор экономических наук.

Программа одобрена на заседании методической комиссии от 12.11.2024, протокол № №5.